Rapport d'activités 2021
Activiteitenverslag 2021

Comité Permanent R
Vast Comité I

Comité Permanent de Contrôle des
services de renseignement et de sécurité

Vast Comité van Toezicht op
de inlichtingen- en veiligheidsdiensten

RAPPORT D'ACTIVITÉS 2021
ACTIVITEITENVERSLAG 2021

Quis custodiet ipsos custodes ?

Quis custodiet ipsos custodes ? est une série de publications qui a pour objectif de stimuler une discussion approfondie sur le fonctionnement, les compétences et le contrôle des services de renseignement et de sécurité et sur le travail de renseignement. Dans cette série figurent notamment des études scientifiques, les rapports d'activités du Comité permanent R et des rapports de colloques.

Rédaction

Comité permanent de Contrôle des services de renseignement et de sécurité, rue de Louvain 48, boîte 4 à 1000 Bruxelles (02 286 29 88).

Déjà parus dans cette série

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Comité permanent R, *Rapport d'activités 2006,* 2007, 147 p.
3) Comité permanent R, *Rapport d'activités 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism - Fusion Centres throughout Europe*, 2010, 220 p.
5) Comité permanent R, *Rapport d'activités 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Comité permanent R, *Rapport d'activités 2009,* 2010, 127 p.
8) Comité permanent R, *Rapport d'activités 2010,* 2011, 119 p.
9) Comité permanent R, *Rapport d'activités 2011,* 2012, 134 p.
10) W. Van Laethem et J. Vanderborght, *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, 2013, 565 p.
11) Comité permanent R, *Rapport d'activités 2012*, 2013, 127 p.
12) Comité permanent R, *Rapport d'activités 2013*, 2014, 212 p.
13) Comité permanent R, *Rapport d'activités 2014*, 2015, 141 p.
14) Comité permanent R, *Rapport d'activités 2015*, 2016, 131 p.
15) Comité permanent R, *Rapport d'activités 2016*, 2017, 227 p.
16) Comité permanent R, *Rapport d'activités 2017*, 2018, 152 p.
17) Comité permanent R, *Rapport d'activités 2018*, 2019, 167 p.
18) J. Vanderborght (ed.), *Les méthodes particulières de renseignement : de l'ombre à la lumière*, 2019, 151 p.
19) Comité permanent R, *Rapport d'activités 2019*, 2020, 148 p.
20) Comité permanent R, *Rapport d'activités 2020*, 2021, 189 p.
21) Comité permanent R, *Rapport d'activités 2021*, 2022, 241 p.

RAPPORT D'ACTIVITÉS 2021

Comité permanent de Contrôle des services de renseignement et de sécurité

Comité permanent de Contrôle des services
de renseignement et de sécurité

Le présent Rapport d'activités 2021 a été approuvé par le Comité permanent de Contrôle des services de renseignement et de sécurité lors de la réunion du 25 mai 2022.

(soussignés)
Serge Lipszyc, président
Pieter-Alexander De Brock, conseiller
Thibaut Vandamme, conseiller
Frédéric Givron, greffier

Rapport d'activités 2021
Comité permanent de Contrôle des services de renseignement et de sécurité

Tous droits réservés. Sous réserve d'exceptions explicitement prévues par la loi, aucun élément de cette publication ne peut être reproduit, stocké dans une base de données automatisée ou publié, de quelque manière que ce soit, sans l'autorisation expresse préalable des éditeurs.

Malgré tout le soin apporté à la composition du texte, ni les auteurs ni l'éditeur ne sauraient être tenus pour responsables des dommages pouvant résulter d'une erreur éventuelle de cette publication.

TABLE DES MATIÈRES

Liste des abréviations ..... *xi*
Préface ..... **xvii**

CHAPITRE I. **1**
LES ENQUÊTES DE CONTRÔLE **1**
I.1. Les services d'appui de l'OCAM (suivi) 2
I.1.1. Suivi des recommandations par les Douanes et Accises 2
I.1.2. Suivi des recommandations par le SPF Mobilité et Transports 3
I.1.3. Conclusion 4
I.2. L'OCAM et les services d'appui 'supplémentaires' 4
I.2.1. Le flux d'informations 5
I.2.1.1. SPF Intérieur – Centre de crise 5
I.2.1.2. SPF Justice – Direction générale des Établissements Pénitentiaires 6
I.2.1.3. SPF Finances – Administration générale de la Trésorerie 7
I.2.1.4. SPF Justice – Direction générale de la Législation et des Libertés et Droits fondamentaux – Laïcité et Cultes 8
I.2.2. Constatations et conclusion 8
I.3. L'échange d'informations sur un collaborateur entre les services de renseignement et un employeur privé ou public 9
I.3.1. Le cadre général 9
I.3.2. L'employeur souhaite un screening de sécurité 10
I.3.2.1. La base légale pour les screenings de sécurité 10
I.3.2.2. Article 19, alinéa 1er, première partie de la phrase L.R&S 11
I.3.3. L'employeur fait l'objet d'une menace (présumée) 12
I.3.3.1. Article 19, alinéa 1er, dernière partie de la phrase L.R&S 12
I.3.3.2. Une élaboration plus poussée de cette réglementation dans une directive ? 12
I.3.3.3. Les limites posées par la Loi organique des services de renseignement et de sécurité 13
I.3.3.4. Qu'est ce qui peut ou doit être communiqué ? 15
I.3.4. Conclusions 17
I.4. Dysfonctionnements graves en matière de sécurité nationale 18
I.5. Le suivi des organisations sectaires nuisibles et des organisations criminelles par la Sûreté de l'État 19
I.5.1. Contextualisation 20
I.5.1.1. Les organisations sectaires nuisibles 20

I.5.1.2. Les organisations criminelles 21
I.5.2. La compétence matérielle 21
I.5.3. La compétence procédurale 22
I.5.4. Les priorités politiques 23
I.5.5. La marge de manœuvre autorisée 24
I.5.6. La traduction organisationnelle des priorités politiques 25
I.5.7. Besoin de renforts et d'un débat sociétal 26
I.6. L'attention des services de renseignement belges pour un collaborateur du SGRS et ses liens avec des citoyens russes 27
I.7. Le screening de sécurité des militaires et des civils à la Défense 27
I.7.1. Le screening des militaires et des civils de la Défense 28
I.7.2. Le screening de sécurité pour les étudiants (étrangers) de l'École Royale Militaire ? 29
I.8. Enquête de contrôle sur le suivi des mandataires politiques 30
I.8.1. Introduction 30
I.8.2. Constatations concernant l'exécution des recommandations formulées par le Comité permanent R 32
I.8.2.1. L'élaboration de directives quant au recueil, au traitement, à la consultation, au stockage et à l'archivage des données 32
I.8.2.2. Une attention particulière pour la position des mandataires politiques mentionnés 33
I.8.2.3. L'exécution de l'article 19 L.R&S. 34
I.8.3. La collecte, l'analyse et la diffusion des renseignements sur les mandataires politiques entre 2019 et 2020 34
I.8.3.1. Collecte et analyse 34
I.8.3.2. Diffusion des renseignements 35
I.8.4. Le respect des droits fondamentaux des mandataires politiques 35
I.9. Enquête sur la détection et le suivi de la radicalisation d'un militaire de la défense : l'affaire Jürgen Conings 36
I.9.1. Un aperçu du parcours professionnel de Jürgen Conings 37
I.9.2. Cadre juridique et politique 38
I.9.2.1. Les missions de renseignement de la VSSE et du SGRS 39
I.9.2.2. La réalisation de screenings de sécurité par les deux services de renseignement 40
I.9.2.3. La responsabilité du SGRS en matière de sécurité militaire 41
I.9.3. Les constatations de l'enquête 41
I.9.3.1. La position d'information de la VSSE 42
I.9.3.2. La position d'information du SGRS 42
I.9.3.3. Un manque de communication 44
I.9.3.4. La 'watchlist' extrême droite 46

I.9.3.5. Les habilitations de sécurité successives de Jürgen Conings 47
I.9.3.6. La mission d'officier de sécurité 48
I.9.3.7. Le dépôt d'armes et le rôle du SGRS 48
I.9.4. Conclusions 49
I.10. Enquête commune de contrôle sur le rôle de l'OCAM dans le suivi du militaire Jürgen Conings 49
I.10.1. Analyse du cadre légal 50
I.10.2. L'OCAM et les banques de données communes 51
I.10.2.1. La procédure d'inscription 52
I.10.2.2. L'échange d'informations avec les partenaires 53
I.10.3. Le rôle de l'OCAM dans le suivi de Jürgen Conings : l'inscription dans la banque de données commune 54
I.10.4. L'échange d'informations 54
I.10.5. Conclusions 56
I.11. Le suivi d'un commissaire du gouvernement par la VSSE 56
I.11.1. Une note de la Sûreté de l'État 57
I.11.2. Constatations de l'enquête 58
I.11.2.1. Une attention renouvelée pour les Frères musulmans (et Ihsane Haouach) ? 58
I.11.2.2. Le principe de précaution 58
I.11.2.3. Aucune autre constatation d'enquête ? 59
I.11.2.4. La fuite d'une note classifiée 59
I.11.2.5. Une 'entrave' ? 60
I.11.2.6. La nécessité d'un screening pour les fonctions revêtant un caractère public ? 60
I.12. Une attention renouvelée pour Frères musulmans 61
I.12.1. Les Frères musulmans : contextualisation 61
I.12.1.1. Genèse et internationalisation du mouvement 61
I.12.1.2. Quelle ampleur du phénomène en Belgique ? 62
I.12.1.3. Une mouvance considérée comme une menace à l'étranger ? 63
I.12.2. Constatations de l'enquête 63
I.12.2.1. La mouvance fait-elle l'objet d'un suivi par les services de renseignement ? 63
I.12.2.2. La mouvance est-elle identifiée comme une menace pour la Belgique ? 64
I.12.2.3. Collaboration entre partenaires 65
I.12.2.4. Quelles stratégies poursuivent les services de renseignement pour endiguer la menace identifiée? 66
I.13. Les technologies de l'information et de la communication dans le processus de renseignement au sein de la direction Cyber du SGRS et au sein de la VSSE 67
I.13.1. Le core business d'un service de renseignement 67
I.13.2. L'environnement et l'organisation ICT de la direction Cyber du SGRS 69

I.13.2.1. Contexte....69
I.13.2.2. Évaluation des risques....71
I.13.3. L'environnement et l'organisation ICT de la VSSE 72
I.13.3.1. Contexte....72
I.14. Enquêtes de contrôle pour lesquelles des devoirs d'enquête ont été effectués en 2021 et enquêtes qui ont débuté en 2021.... 75
I.14.1. L'application de nouvelles méthodes (particulières) de renseignement 75
I.14.2 Le suivi par la vsse des condamnés pour terrorisme qui ont été libérés 76
I.14.3. Le risque d'infiltration au sein des deux services de renseignement 77
I.14.4. Menaces éventuelles pour le potentiel économique et scientifique (PRISM/PES) : enquête de suivi 77
I.14.5. Espionnage via du matériel de cryptage : l'opération Rubicon 78
I.14.6. Capacités de renseignement (supplémentaires) pour les services de renseignement belge à l'étranger? 79
I.14.7. Contrôle des fonds spéciaux : enquête de suivi 80
I.14.8. Enquête de contrôle sur la détection et le suivi par les services de renseignement des organisations philosophiques à visées politiques contraires à l'ordre démocratique 81

CHAPITRE II....83
LE CONTRÔLE DES MÉTHODES PARTICULIÈRES ET DE CERTAINES MÉTHODES ORDINAIRES DE RENSEIGNEMENT 83
II.1. Les chiffres relatifs aux méthodes particulières et à certaines méthodes ordinaires 84
II.1.1. Tendances générales 84
II.1.1.1. Quant aux méthodes particulières de renseignement à la VSSE et au SGRS....84
II.1.1.2. Quant aux méthodes ordinaires plus, en particulier l'article 16/2 L.R&S....88
II.1.1.3. Les conséquences de l'annulation de la Loi sur la conservation des données ?....90
II.1.2. Méthodes utilisées par le SGRS 91
II.1.2.1. Méthodes ordinaires 'plus' 91
II.1.2.2. Les méthodes spécifiques....93
II.1.2.3. Les méthodes exceptionnelles....94
II.1.2.4. Les missions et les menaces justifiant le recours aux méthodes ordinaires et particulières 96
II.1.3. Les méthodes utilisées par la VSSE.... 99
II.1.3.1. Les méthodes ordinaires 'plus' 99
II.1.3.2. Les méthodes spécifiques 100
II.1.3.3. Les méthodes exceptionnelles....102

II.1.3.4. Les menaces et les intérêts justifiant le recours aux méthodes (ordinaires et) particulières 103
II.2. Les activités du Comité permanent R en sa qualité d'organe (juridictionnel) et d'auteur d'avis préjudiciels 105
II.2.1. Contrôle de certaines méthodes ordinaires 105
II.2.1.1. Généralités 105
II.2.2. Contrôle des méthodes particulières 106
II.2.2.1. Les chiffres 106
II.2.2.2. La jurisprudence 110
II.3. Constatations générales 116

CHAPITRE III. 119
LE CONTRÔLE DES INTERCEPTIONS À L'ÉTRANGER, DES PRISES D'IMAGES ET DES INTRUSIONS DANS DES SYSTÈMES INFORMATIQUES 119
III.1. Les compétences du SGRS et la mission de contrôle du Comité permanent R 119
III.2. Les contrôles effectués en 2021 121
III.2.1. Le contrôle préalable à l'interception, l'intrusion ou la prise d'images 121
III.2.2. Le contrôle pendant l'interception, l'intrusion ou la prise d'images 121
III.2.3. Le contrôle après l'exécution de la méthode 122

CHAPITRE IV. 123
LE COMITÉ PERMANENT R EN SA QUALITÉ D'AUTORITÉ DE CONTRÔLE COMPÉTENTE DANS LE CADRE DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL 123
IV.1. Introduction 123
IV.2. Le traitement des requêtes individuelles 124
IV.3. Les avis 127
IV.4. La notification d'une potentielle brèche de sécurité 127
IV.5. Évaluation de la loi relative à la protection des données 128

CHAPITRE V. 129
LE CONTRÔLE DES BANQUES DE DONNÉES COMMUNES 129
V.1. La mission de contrôle et l'objet du contrôle 129
V.2. Les constatations de l'enquête 130
V.2.1. L'absence d'accès de l'ANS 130
V.2.2. Le suivi des recommandations antérieures 131
V.2.2.1. Les recommandations suivies d'effet 131
V.2.2.2. Les recommandations non suivies d'effet 131
V.2.2.3. Les recommandations partiellement suivies d'effet 132
V.2.3. De nouvelles recommandations 133
V.3. La mission d'avis 134

CHAPITRE VI. 135
AVIS 135
VI.1. Avis relatif à la création d'une agence fédérale du renseignement 136
VI.2. Avis relatif à l'instauration d'une obligation de notification pour les services de renseignement 136
VI.2.1. La notification active 137
VI.2.2. La notification passive 139
VI.3. Avis relatif à la rétention des données 140
VI.3.1. Modifications à la loi organique des services de renseignement 141
VI.3.1.1. Conservation ciblée des données de trafic et de localisation 141
VI.3.1.2. Accès aux données de trafic et de localisation 141
VI.3.1.3. Conservation généralisée et indifférenciée des données de trafic et de localisation 142
VI.3.1.4. Notification obligatoire des décisions du Comité aux opérateurs 143
VI.3.2. Modifications à la Loi Télécom (LCE) 143
VI.4. Avis concernant l'avant-projet de loi modifiant la loi organique des services de renseignement 144
VI.4.1. Une réglementation trop complexe 144
VI.4.2. Cybersécurité - mission du SGRS 145
VI.4.3. La commission d'infractions d'appui 146
VI.4.3.1. Généralités 146
VI.4.3.2. Lacune dans la procédure pénale 146
VI.4.3.3. La commission d'infractions par des agents 147
VI.4.3.4. La commission d'infractions par des informateurs 147
VI.4.3.5. Dommages subis ou causés par une source humaine 148
VI.4.3.6. Protection juridique insuffisante de la source humaine 148
VI.4.4. Identité et qualité fictives comme mesure d'appui à une méthode de renseignement ou uniquement pour des raisons de sécurité 148
VI.4.5. Infiltration dans le monde réel et virtuel 149
VI.4.6. Méthodes ordinaires plus 149
VI.4.7. Réclamation de données financières 150
VI.4.8. Moyens en personnel et moyens financiers 150
VI.5. Avis sur des propositions de loi à propos d'incriminations visant à promouvoir la résilience démocratique 150
VI.5.1. Observation préalable 151
VI.5.2. Coopération et échange d'informations avec les acteurs judiciaires 151
VI.5.3. Coopération et échange d'informations avec les acteurs administratifs 152
VI.6. Avis commun sur l'avant-projet de loi modifiant la loi OCAM 153

VI.6.1. Extension de la liste des services d'appui 153
VI.6.2. Modification des conditions de nomination du directeur et du directeur adjoint 154
VI.6.3. Extension des missions de l'OCAM 155
VI.6.3.1. La coordination de l'approche globale des menaces 155
VI.6.3.2. De nouvelles missions confiées à l'OCAM par le Conseil national de sécurité ? 156
VI.6.4. Communication et consultation des évaluations 156
VI.6.5. Communication et consultation de renseignements de nature judiciaire sous embargo 157
VI.6.6. communication et consultation de renseignements visés à l'article 12, 1er alinéa L.OCAM 157

CHAPITRE VII. 159
LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES 159

CHAPITRE VIII. 161
EXPERTISE ET CONTACTS EXTERNES 161
VIII.1. Expert dans différents forums 161
VIII.2. Protocole de coopération avec les Médiateurs fédéraux 162
VIII.3. Collaboration avec l'Institut fédéral des 'droits de l'homme' 163
VIII.4. Une initiative multinationale en matière d'échange d'informations ... 163
VIII.5. Contacts avec des organes de contrôle étrangers 164

CHAPITRE IX. 165
L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ 165
IX.1. Le rapport d'activités de l'Organe de recours 165
IX.1.1. Introduction 165
IX.1.2. Le détail des chiffres 166
IX.2. Remarques et suggestions du président de l'Organe de recours 174
IX.2.1. Une procédure particulière et complexe 174
IX.2.2. Décision du conseil d'état 176
IX.2.3. Responsabilité de l'Organe de recours 177
IX.2.4. Deux questions au regard de l'article 6 de la Convention européenne des droits de l'homme (CEDH) 177
IX.2.4.1. La publication 178
IX.2.4.2. Les audiences publiques 179
IX.2.5. Effectivité des décisions de l'Organe de recours 181
IX.2.6. Perspective 182
CHAPITRE X. 183
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R 183
X.1. Composition du Comité permanent R 183
X.2. Un audit relatif au bien-être au Comité 184
X.3. Réunions avec la Commission de suivi 185
X.4. Réunions communes avec le Comité permanent P 186
X.5. Une attention médiatique importante 187
X.6. Le 'Data Protection Officer' au Comité 187

X.7. Moyens financiers et activités de gestion 188
X.8. Mise en œuvre des recommandations de l'audit de la Cour des comptes 190
X.9. Formations 191

CHAPITRE XI. 193
RECOMMANDATIONS 193
XI.1. Recommandations relatives à la protection des droits que la Constitution et la loi confèrent aux personnes 193
XI.1.1. Rédaction d'une proposition de directive sur la communication d'informations par la VSSE ou le SGRS aux employés et adaptation des directives existantes .. 193
XI.1.2. Directives en matière de suivi de mandataires politiques 194
XI.2. Recommandations relatives à la coordination et à l'efficacité des services de renseignement, de l'OCAM et des services d'appui 194
XI.2.1. Recommandations relatives à l'OCAM et ses (nouveaux) services d'appui 194
XI.2.2. Application conforme de la possibilité d'introduire des demandes de screenings de sécurité 195
XI.2.3. Signalement obligatoire auprès de l'employeur en cas de reprise dans une banque de données commune 196
XI.2.4. Un débat étendu sur les tâches et priorités des services de renseignement 196
XI.2.5. Plus de screenings de sécurité des militaires et des civils à la Défense 196
XI.2.6. La mise en place d'un ensemble cohérent 'renseignement' ... 198
XI.2.7. Stabilité dans la gestion du personnel au sein du SGRS 198
XI.2.8. La validation du Plan Directeur du Renseignement (et de sécurité) 198
XI.2.9. Une meilleure communication interne au SGRS 198
XI.2.10. Une meilleure communication entre le SGRS et les autres autorités en cas d'infractions judiciaires ou pénales ... 199
XI.2.11. Une meilleure communication interne du SGRS vers le commandement et le ministre de la Défense 199
XI.2.12. Suivi actif de l'extrémisme au sein de la Défense par le SGRS 199
XI.2.13. Évaluation du plan stratégique national du renseignement (PSNR) 200
XI.2.14. De meilleures règles et connaissances sur l'introduction des entités dans les banques de données communes (BDC) 200
XI.2.15. L'échange d'informations entre services de renseignement concernant le personnel de la Défense 201
XI.2.16. Respect des accords HUMINT 201
XI.2.17. Respect du transfert d'informations à l'OCAM 201

XI.2.18. Une politique de recrutement flexible et proactive pour les services de renseignement 201
XI.2.19. Un environnement digital de qualité 202
XI.2.20. Une méthologie uniforme en matière d'évaluation de la menace dans le domaine du renseignement 202
XI.2.21. L'importance de divers règlements 202
XI.2.22. Autorité disciplinaire sur le personnel civil de la Défense 203
XI.2.23. Utilisation des méthodes de recueil de données 203
XI.2.24. Recrutement de juristes 203
XI.2.25. Investir dans le management 203
XI.2.26. Clarification des missions de counterintelligence au sein du SGRS 204
XI.2.27. Fonctionnement des officiers de sécurité au sein du SGRS ... 204
XI.2.28. Identification d'indicateurs de radicalisation par le SGRS 204
XI.2.29. Visibilité des entités respectives à suivre par la VSSE et le SGRS 204
XI.2.30. Les moyens pour la lutte contre l'extrémisme 204
XI.2.31. Actualisation de directives existantes 205
XI.2.32. Cumul au sein de la Défense 205
XI.2.33. Le fonctionnement des banque de données communes au sein du SGRS 205
XI.2.34. Notification et suivi des incidents de sécurité au sein du SGRS 206
XI.2.35. Collaboration entre les bureaux de sécurité du SGRS et de la VSSE 206
XI.2.36. Utilisation cohérente des niveaux de la menace et communication des évaluations par l'OCAM 206
XI.2.37. Communication écrite en cas d'application de l'article 19 L.R&S 207
XI.2.38. Le traitement d'informations classifiées par des tiers 207
XI.2.39. Des screenings de sécurité pour des fonctions de confiance . 208
XI.2.40. Indication des destinataires sur les notes sortantes 208
XI.2.41. Communiquer les besoins du Conseil national de sécurité aux services de renseignement 209
XI.2.42. Collaboration dans le cadre de la problématique des Frères musulmans 209
XI.2.43. Analyse des moyens du SGRS dans le cadre de la problématique des Frères musulmans 210
XI.2.44. Sensibilisation générale dans le cadre de la problématique des Frères musulmans 210
XI.2.45. Sensibilisation des officiers de sécurité de la Défense dans le cadre de la problématique des Frères musulmans 210
XI.2.46. L'ICT dans le processus du renseignement au sein de la Direction cyber du SGRS 210
XI.3. Recommandation relative à l'efficacité du contrôle 211
XI.3.1. Signalement par le SGRS du suivi des mandataires politiques 211

ANNEXES **213**

Annexe A **213**
Aperçu des principales réglementations relatives aux compétences, au fonctionnement et au contrôle des services de renseignement et de sécurité et de l'OCAM (1er janvier 2021 au 31 décembre 2021) **213**

Annexe B 216
Aperçu des principales propositions de lois, des projets de lois, des résolutions, motions d'ordre et des débats parlementaires relatifs aux compétences, au fonctionnement et au contrôle des services de renseignement et de sécurité et de l'OCAM (1er janvier 2021 au 31 décembre 2021) 216

Annexe C 219
Aperçu des interpellations, des demandes d'explications et des questions orales et écrites relatives aux compétences, au fonctionnement et au contrôle des services de renseignement et de sécurité et de l'OCAM (1er janvier 2021 au 31 décembre 2021) 219

LISTE DES ABRÉVIATIONS

AC(C)	Autorité de contrôle (compétente)
AG	Administrateur général (VSSE)
AIVD	*Algemene Inlichtingen- en Veiligheidsdiensten*
A.M.	Arrêté ministériel
Ann. parl.	Annales parlementaires
ANS	Autorité nationale de sécurité
APD	Autorité de protection des données
A.R.	Arrêté royal
AR BDC	Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters et portant exécution de certaines dispositions de la section 1er*bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police
AR C&HS	Arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
AR FTF	Arrêté royal du 21 juillet 2016 relatif à la banque de données commune 'Foreign Terrorist Fighters' et portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police
AR OCAM	Arrêté royal du 28 novembre 2006 portant exécution de la Loi du 10 juillet 2006 relative à l'analyse de la menace
AR PH	Arrêté royal du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police
AR TF	Arrêté royal du 23 avril 2018 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters portant exécution de certaines dispositions de la section 1er*bis* 'de la gestion des informations' du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters

A-Rens	Autorité de surveillance indépendante des activités de renseignement
BCP	*Business continuity plan*
BDC	Banques de données communes
BDC PH	Banque de données commune ' Propagandistes de haine'
BDC TF	Banque de données commune ' Terrorist fighters'
BELPIU	*Belgian Passenger Information Unit* (Unité belge d'information des passagers)
BfV	*Bundesamt für Verfassungsschutz*
BINII	*Belgian Intelligence Network Information Infrastructure*
BNG	Banque de données nationale générale
CAC	Cellule administrative de coordination
CaMa	*Case Managers (*SGRS)
CCB	Centre pour la Cybersécurité Belgique
CCIRM	*Collection Coordination Information Requirement Management* (SGRS)
CCL	Conseil Central Laïque
CCRS	Comité de coordination du renseignement et de la sécurité
CE	Contre-extrémisme
CEDH	Convention européenne des droits de l'homme
CelEx	Cellule Extrémisme (SPF Justice)
CI	*Counterintelligence*
CIA (model)	Confidentiality, Integrity & Availability (model)
CIAOSN	Centre d'information et d'avis sur les organisations sectaires nuisibles
CJUE	Cour de justice de l'Union européenne
CM BDC	Circulaire du 22 mai 2018 du Ministre de la Sécurité et de l'Intérieur et du Ministre de la Justice relative à l'échange d'informations et au suivi des Terrorist Fighters et des Propagandistes de haine
CMDB	*Component Management DataBase* (base de données de gestion de configuration)
CMOJ	Commission de Modernisation de l'Ordre judiciaire
CNS	Conseil national de sécurité
Cour EDH	Cour européenne des droits de l'homme
C.O.C.	Organe de contrôle de l'information policière
CoMa	*Collection Managers* (SGRS)
Comité permanent P	Comité permanent de Contrôle des services de police
Comité permanent R	Comité permanent de Contrôle des services de renseignement et de sécurité

Commission BIM	Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité
CRABV	Compte Rendu Analytique – *Beknopt Verslag*
CRIV	Compte Rendu Intégral – *Integraal Verslag*
CSIL-R	Cellule de Sécurité Intégrale Locale - Radicalisme
CTIF	Cellule de Traitement des Informations Financières
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten*
DG EPI	Direction générale des Établissements Pénitentiaires (SPF Justice)
DGSP	Direction générale Sécurité & Prévention (SPF Intérieur)
DISCC	*Defense Intelligence and Security Coordination Centre* (SGRS)
DJSOC/Terro	Direction de la lutte contre la criminalité grave et organisée (section terrorisme) de la Police judiciaire fédérale
Doc. parl.	Documents parlementaires de la Chambre et du Sénat
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*
DRI	Direction de l'information policière et des moyens ICT (Police fédérale)
DRP	*Disaster recovery plan*
EPV	Extrémiste potentiellement violent
ERM	École Royale Militaire
FTF	*Foreign terrorist fighters*
GEOINT	*Geospacial intellingence*
HTF	*Homegrown terrorist fighters*
HUMINT	*Human intelligence*
ICM	*Incident & Crisis Management*
ICT	*Information and communications technology*
IEFH	Institut pour l'égalité entre les femmes et les hommes
IFDH	Institut fédéral pour la protection et la promotion des droits humains
IOWG	*Intelligence Oversight Working Group*
IPCO	*Investigatory Powers Commissioner's Office*
JDC	*Joint Decision Centre*
JIC	*Joint Intelligence Centre*
LCE	Loi du 13 juin 2005 relative aux communications électroniques
L.Contrôle	Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace

L.C&HS	Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
LFP	Loi du 5 août 1992 sur la fonction de police
L.OCAM	Loi du 10 juillet 2006 relative à l'analyse de la menace
Loi APD	Loi du 3 décembre 2017 portant création de l'Autorité de protection des données
Loi MRD	Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité
Loi PNR	Loi du 25 décembre 2016 relative au traitement des données des passagers
L.Org.recours	Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité
LPA	Loi du 11 avril 1994 relative à la publicité de l'administration
LPD	Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (Loi Protection des données)
L.R&S	Loi du 30 novembre 1998 organique des services de renseignement et de sécurité
LTF	*Local task force*
M.B.	Moniteur belge
MoU	*Memorandum of Understanding*
MPLUS	Méthodes ordinaires plus
MRD	Méthodes de recueil des données
NA	Note aux autorités
NTSU-CTIF	*National Technical & Tactical Support Unit – Central Technical Interception Facility* (Police intégrée)
OCAM	Organe de coordination pour l'analyse de la menace
OE	Office des étrangers
OSINT	*Open sources intelligence*
OTAN	Organisation du Traité de l'Atlantique Nord
PCT	Personnes condamnées pour terrorisme
PDT-IA	Cellule *Pre-Deployment Training for Individual Augmentees* (Défense)
PH	Propagandistes de haine
Plan R	Plan d'action Radicalisme
Plateforme CT	Plateforme commune contre-terrorisme
PROTEUS	Banque de données de l'OCAM
PSNR	Plan Stratégique National du Renseignement
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)

RFC	*Requests for Collect*
RFI	*Request for information*
RGPD	Règlement Général sur la Protection des Données
SARM	Service d'assistance religieuse et morale (Défense)
SGRS	Service Général du Renseignement et de la Sécurité
SIGINT	*Signal intelligence*
SOP	*Standard Operating Procedures*
SPF	Service public fédéral
TF	*Terrorist fighters*
VSSE	Sûreté de l'État

PRÉFACE

L'année 2021 nous a rappelé à quel point la planète était vulnérable, à quel point les sociétés étaient fragilisées, à quel point la démocratie était remise en question, à quel point les droits des citoyens étaient précaires.

Le phénomène des extrémistes potentiellement violents – religieux ou idéologiques – s'est amplifié par des attaques contre les institutions et a affaibli durablement celles-ci. L'assaut du Capitole à Washington est certainement l'exemple le plus révélateur du rejet des institutions démocratiques. Un tel scenario ne pourrait-il pas toucher nos institutions belges ?

Ce type de menace, loin de disparaître, a été, au contraire, renforcée par les médias sociaux. C'est ainsi que de nombreuses théories conspirationnistes autour de la COVID-19 ont été propagées. Même si le terreau était déjà présent, la pandémie s'est avérée être le parfait prétexte pour dresser davantage des groupes de population les uns contre les autres.

Aujourd'hui comme hier, les coups d'État, les renversements des 'pouvoirs en place' nous obligent à intervenir et à rapatrier si nécessaire nos compatriotes. Cette volonté de protéger nécessite le renforcement de l'engagement de nos services de renseignement et de sécurité à l'étranger.

Le procès à la suite des attentats de Paris, tout comme le procès d'Anvers suite à l'attentat déjoué de Villepinte, nous rappelle également la nécessité pour les services de renseignement de renforcer leur partenariat et de renforcer la lutte commune contre le terrorisme.

En Belgique, les problématiques liées aux mouvements djihadistes ont servi de terreau fertile à la polarisation croissante de la société. Le rapport d'enquête sur le suivi de l'extrême droite a lui aussi montré sa pertinence. À la suite de la traque d'un militaire armé, menaçant nos institutions, l'enquête du Comité a mis en évidence la fragilité de certaines de nos institutions face à ce phénomène qui ne touche plus seulement nos pays voisins.

En ce qui concerne nos services de renseignement, rappelons que notre pays est un carrefour pour de nombreuses institutions européennes et internationales ainsi que de nombreuses communautés et d'opposants. Cette situation particulière exige un investissement permanent dans le renforcement de la protection de ses acteurs et dans la lutte contre les ingérences étrangères.

Il faut encourager les services de la sécurité à agir de manière plus proactive et de mieux interagir entre eux, en visant ainsi une communauté belge du renseignement et de la sécurité consolidée et soudée. J'appuie Jaak Raes, l'Administrateur général de la Sûreté de l'Etat, dans sa volonté de voir dorénavant le « besoin de savoir » (need to know) se concilier avec le « besoin de partager » (need to share).

Je soutiens le projet de statut unique des personnels des services de renseignement et de sécurité. Il est assurément un pas indispensable dans le développement des synergies entre services. J'invite à l'optimisation des ressources ainsi qu'au renforcement de l'expertise disponible dans la lutte contre les menaces. Je pense que la question de la sécurité nécessite une vision stratégique plus claire et ambitieuse du Conseil national de sécurité sur les enjeux de sécurité qui nous sont imposés par l'évolution de notre société.

En raison des impacts du COVID-19, l'organisation quotidienne du Comité a été profondément bouleversée. Il n'a été possible de garantir la continuité du travail que grâce à la conscience professionnelle tenace de chacun.e. Nos collaborateurs ont d'autant plus de mérite qu'ils n'ont pu que très partiellement recourir au télétravail. Nous manquons toujours d'un indispensable réseau digitalisé sécurisé qui nous fait défaut dans nos tâches au quotidien. Et si les défis sont nombreux, le Comité entend y répondre avec pertinence.

Le chantier nécessaire des synergies ouvert par la Chambre permet enfin, aujourd'hui, d'en entrevoir les fondations. Il suscite encore logiquement bon nombre de questions, d'inquiétudes mais aussi d'espoirs. Le renforcement de l'institution du Comité reste d'actualité tout comme les questions soulevées par l'ouverture de dossiers relatifs à l'utilisation de logiciels espions, au suivi d'un imam, au suivi des condamnés terroristes, etc. Même s'il n'est pas le seul, le Comité permanent R est un rempart essentiel de notre Etat de droit.

Cette année fut aussi l'année du départ de plusieurs de nos collaborateurs Martine, Josiane, Wouter, Charles, Ludo, Frank, Jean-Philippe & Christophe que je souhaite remercier pour leur implication.

J'espère que la lecture de ce rapport contribuera à une meilleure perception de nos travaux et vous souhaite une lecture stimulante !

25 mai 2022,
Serge Lipszyc,
Président du Comité permanent de Contrôle
des services de renseignement et de sécurité

CHAPITRE I.
LES ENQUÊTES DE CONTRÔLE

En 2021, le Comité permanent R a finalisé dix enquêtes de contrôle, dont trois conjointement avec le Comité permanent de contrôle des services de police. En complément, trois dossiers d'information ont été présentés devant la Commission parlementaire de suivi et sont également repris dans le présent chapitre (I.4, I.6 et I.7).

Diverses instances et personnes peuvent 'saisir' le Comité permanent R d'une enquête de contrôle : la Commission parlementaire de suivi, les ministres compétents, toute personne (morale) qui souhaite introduire une plainte ou faire une dénonciation, etc. Le Comité peut lui aussi prendre l'initiative d'ouvrir une enquête de contrôle. Ce fut le cas pour cinq des dix enquêtes finalisées en 2021. Quatre enquêtes ont été initiées par la Commission parlementaire de suivi, et une enquête a été effectuée à la demande de la ministre de la Défense. Le Comité a par ailleurs poursuivi sept enquêtes ouvertes en 2021 ou antérieurement. Une description succincte des enquêtes en cours figure au chapitre I.14. Les recommandations émises à l'issue des enquêtes de contrôle ont été regroupées au Chapitre XI.

Le Comité permanent R a reçu, au total, 75 plaintes ou dénonciations en 2021.[1] Après une brève pré-enquête et la vérification de plusieurs données objectives, le Comité a rejeté 23 plaintes ou dénonciations parce qu'elles étaient manifestement non fondées[2] (art. 34 de Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (L.Contrôle)), ou dans 28 cas, parce que le Comité n'était pas compétent pour en traiter les griefs. Dans ce dernier cas de figure, les plaignants ont été renvoyés, si possible, vers les instances compétentes (en l'occurrence, le Procureur du Roi de Bruxelles, le Comité permanent P ou encore l'Autorité de protection des données (APD)). 14 des 24 plaintes traitées ont pu être clôturées en 2021, 10 plaintes étaient toujours en cours de traitement début 2022. En 2021, 16 des 24 plaintes traitées l'ont été en tant que plaintes *Data Protection Authority* (DPA).[3]

---

1 Dans un premier temps, la recevabilité de la plainte est examinée. Elle est ensuite classée dans une catégorie ('ordinaire', plainte APD, plainte MRD, etc.). Dans le cas d'une problématique générale, le Comité peut décider d'ouvrir une enquête de contrôle, sinon l'enquête reste limitée à la plainte (une enquête relative à une plainte).

2 Le Comité reçoit encore toute une série de plaintes et dénonciations fantaisistes.

3 Voir 'V.6. Traitement des requêtes individuelles'.

I.1. LES SERVICES D'APPUI DE L'OCAM (SUIVI)

En juin 2020, le Comité permanent R a, conjointement avec le Comité permanent P, finalisé un enquête de contrôle sur les services d'appui de l'Organe de coordination pour l'analyse de la menace (OCAM).[4] Cette enquête portait sur quatre services d'appui : le Service public fédéral (SPF) Intérieur (Office des étrangers), le SPF Affaires étrangères, le SPF Mobilité et Transports et le SPF Finances (Administration générale des Douanes et Accises).[5] L'enquête visait à examiner les relations entre les services d'appui précités et l'OCAM en ce qui concerne la coopération et l'échange d'informations. Une attention particulière a été accordée à la légalité, à l'efficacité et à la coordination de cette coopération et de cet échange d'informations.

Afin d'informer la Commission parlementaire de suivi de l'état d'avancement de la mise en œuvre des recommandations formulées dans le cadre de cette enquête, les Comités permanents R et P ont ouvert une enquête de suivi début juin 2020.[6]

L'enquête initiale avait ainsi notamment démontré le respect, par le SPF Affaires étrangères et le SPF Intérieur (Office des étrangers), des règles de traitement et de conservation des documents classifiés ainsi que la bonne circulation de l'information entre ces services et l'OCAM.

Dans leur rapport, les Comités permanents R et P formulaient des recommandations exclusivement à l'encontre du SPF Finances (Administration générale des Douanes et Accises) qui a élaboré un plan d'action afin de répondre aux exigences liées à son statut de service d'appui. En réponse aux conclusions et recommandations générales du rapport, le SPF Mobilité et Transport a toutefois également cherché à améliorer l'efficacité de sa collaboration avec l'OCAM. Le rapport de l'enquête de suivi se concentrait donc sur les mesures respectivement mises en place par ces deux administrations.

I.1.1. SUIVI DES RECOMMANDATIONS PAR LES DOUANES ET ACCISES

En réponse aux deux recommandations spécifiques formulées dans le rapport d'enquête en 2020, l'Administration générale des Douanes et Accises du SPF Finances a mis en place un plan d'action. Au moment de clôturer l'enquête de suivi (début 2021), la plupart des mesures prévues dans le plan d'action étaient

---

4 Voir COMITÉ PERMANENT R, *Rapport d'activités 2020*, 2-11 ('I.1. Les services d'appui de l'OCAM').

5 Les services de police et de renseignement ont déjà fait l'objet d'une enquête de contrôle commune portant sur les services d'appui de l'OCAM. Voir à ce propos : COMITÉ PERMANENT R, *Rapport d'activités 2010*, 45-46 ('II.12.6. Communication de renseignements à l'OCAM par les services d'appui') et plus en détail : COMITÉ PERMANENT R, *Rapport d'activités 2011*, 25-33 ('II.4. Les flux d'informations entre l'OCAM et ses services d'appui').

6 Les résultats de cette enquête ont été présentés à la Commission de suivi en avril 2021.

partiellement mises en œuvre. Certaines actions n'avaient toutefois pas encore pu être réalisées, notamment en raison de la crise sanitaire.

La première recommandation spécifique appelait à clarifier, en interne, les informations recueillies qui sont pertinentes pour l'OCAM. Une première mesure prévoit ainsi d'établir un plan de collecte d'informations sur la base d'indicateurs d'extrémisme et de terrorisme. Un travail de sensibilisation a également été entamé afin d'encourager le signalement et le partage d'informations. Des formations étaient prévues à cette fin, notamment sur les indices d'extrémisme et de terrorisme. L'administration des Douanes et Accises a également procédé à un inventaire des sources d'informations en interne (les informations recueillies lors des activités opérationnelles de l'Administration Opérations et de l'Administration Recherches ou enregistrées dans les bases de données internes). En mars 2021, l'administration n'avait toutefois toujours pas accès à la banque de données commune gérée par l'OCAM.

La seconde recommandation portait sur le respect des normes légales de conservation et de consultation des documents classifiés. Outre l'acquisition de nouveaux coffres-forts et la mise en place d'un registre complet des informations classifiées, un manuel sur le traitement des documents classifiés était préparé par l'officier de sécurité de l'administration. En outre, l'Administration Recherches a limité l'accès au local BINII (*Belgian Intelligence Network Information Infrastructure*, une plateforme de communication pour l'échange d'informations classifiées). Le plan d'action prévoit également une vérification périodique des habilitations de sécurité ainsi que l'organisation de briefings de sécurité pour les titulaires d'habilitations.

Les Comités permanents P et R concluaient ainsi que l'Administration des Douanes et Accises a pris un certain nombre d'actions et de mesures nécessaires pour répondre aux recommandations formulées dans le rapport d'enquête initial.

I.1.2. SUIVI DES RECOMMANDATIONS PAR LE SPF MOBILITÉ ET TRANSPORTS

Malgré l'absence de recommandation spécifique à son encontre lors de l'enquête initiale, le SPF Mobilité et Transports a élaboré, lui aussi, un plan d'action, accompagné d'un calendrier, afin d'améliorer l'efficacité de sa coopération avec l'OCAM. Ce plan d'action visait, d'abord, à sensibiliser les collaborateurs aux missions de l'OCAM et aux échanges avec ce service. En 2020, plusieurs réunions ont ainsi été organisées par la Cellule de Crise du SPF Mobilité et Transports, tant en interne pour rappeler le rôle de l'OCAM et les objectifs de cette coopération qu'avec l'OCAM afin d'identifier les points d'amélioration et pistes d'action. En parallèle, au moment de clôturer l'enquête de suivi, un nouvel outil informatique était en cours de développement au sein du SPF Mobilité et Transports. Un tel outil devrait faciliter les échanges entre le SPF et l'OCAM et leur gestion.

Ensuite, le plan d'action prévoyait le développement et la mise en place de canaux privilégiés de partage d'informations en interne et vers l'extérieur. Dans ce cadre, un manuel de procédures quant à la gestion des documents classifiés et du système BINII a notamment été validé en interne.

Les effets de ces mesures ne pourront être évalués qu'avec le temps. Pour sa part, la Cellule de Crise du SPF regrettait toutefois à la clôture de l'enquête de suivi toujours le nombre encore trop important d'évaluations et d'informations en provenance de l'OCAM.

I.1.3. CONCLUSION

Tant le SPF Finances (Administration des Douanes et Accises) que le SPF Mobilité et Transports ont mis en place des plans d'action permettant de rencontrer les conclusions et recommandations formulées. Les Comités concluaient que ces différentes mesures devraient permettre de mieux garantir la sécurité des informations transmises, de faciliter le flux d'informations et d'avoir une meilleure connaissance de l'OCAM et de ses missions au sein de ces services d'appui.

I.2. L'OCAM ET LES SERVICES D'APPUI 'SUPPLÉMENTAIRES'

L'Arrêté royal (A.R.) du 17 août 2018 a élargi la liste des services d'appui de l'OCAM à quatre autres services, que sont la Direction générale Centre de crise, l'Administration générale de la Trésorerie, la Direction générale des Établissements pénitentiaires et le Service des cultes et de la laïcité de la Direction générale de la Législation et des Libertés et Droits fondamentaux du SPF Justice. Bien que cette décision remonte à août 2018, la première enquête[7] ne portait pas encore sur ces services, car il était prématuré d'effectuer une analyse du flux d'informations et des processus mis en œuvre dans ce cadre. Une nouvelle enquête de contrôle, menée conjointement avec le Comité permanent P, s'imposait.[8]

---

7 Voir COMITÉ PERMANENT R, *Rapport d'activités 2020*, 2-11 ('I.1. Les services d'appui de l'OCAM').

8 Les résultats ont été présentés à la Commission parlementaire de suivi en avril 2021.

I.2.1. LE FLUX D'INFORMATIONS

L'enquête visait à examiner les relations entre l'OCAM et les quatre services d'appui supplémentaires au regard de la transmission d'informations, de la légalité, de l'efficacité et de la coordination.

Une analyse quantitative des échanges offre un premier aperçu du flux d'informations entre les services d'appui et l'OCAM.

	2019				
	TOTAL	IN	OUT	RFI IN	RFI OUT
SPF JUSTICE – LAÏCITÉ ET CULTES	**13**	8	5	8	0
SPF JUSTICE – ÉTABLISSEMENTS PÉNITENTIAIRES	**2273**	2223	50	224	2
SPF FINANCES – ADMINISTRATION GÉNÉRALE DE LA TRÉSORERIE	**17**	14	3	7	0
SPF INTERIEUR – CENTRE DE CRISE	**2940**	1334	1606	7	8

Tableau 1 : Chiffres fournis par l'OCAM. Les données « IN » renvoient aux données entrantes à l'OCAM venant du service d'appui et les données « OUT » renvoient aux données sortantes de l'OCAM vers le service d'appui (Requests for Information (RFI) inclues).

Le tableau rend compte des informations échangées entre l'OCAM et les quatre services d'appui pour l'année 2019 selon les chiffres fournis par l'OCAM.[9] Ces données n'incluent pas les évaluations envoyées par l'OCAM, excepté pour le Centre de crise, premier destinataire des évaluations.

I.2.1.1. SPF Intérieur – Centre de crise

De par ses missions, le Centre de crise (à travers sa direction *Incident & Crisis Management* – ICM) est en contact permanent avec l'OCAM. En effet, le service définit les mesures à prendre sur la base des évaluations de la menace réalisées par l'OCAM. À ce titre, des réunions de coordination et de sécurité ont lieu très

[9] Ces données sont extraites de PROTEUS, la banque de données de l'OCAM. Il ne s'agit que des flux d'informations jugés pertinents par l'OCAM. Ces chiffres ne reprennent donc pas les échanges non encodés dans PROTEUS, par exemple des RFI envoyées à l'OCAM sur des entités inconnues.

fréquemment, et cela avant même que le Centre de crise ne soit désigné service d'appui.

Le flux d'informations de l'OCAM vers le Centre de crise est le plus important des quatre services d'appui supplémentaires et concerne pour la grande majorité des évaluations. En revanche, le Centre de crise ne fournit que très peu d'informations à l'OCAM, si ce n'est sur la tenue d'événements ou la venue de personnalités étrangères (par exemple par des demandes d'évaluations de la menace). La désignation comme service d'appui se justifie toutefois par la mise sur pied, au sein du Centre de crise, de l'Unité d'Information des Passagers (ou *Belgian Passenger Information Unit* – BELPIU).[10]

Étant donné les contacts permanents et la proximité de leurs bureaux, il n'y a pas de membres du personnel du Centre de crise détaché à l'OCAM. Le flux d'informations est décrit comme très bon par la Direction ICM. Les procédures mises en place, notamment l'utilisation des boites fonctionnelles, donnent des garanties contre les risques de perte d'informations.

L'échange d'informations se fait via trois canaux différents : par e-mail pour les informations et évaluations non classifiées ou en diffusion restreinte, par BINII pour les documents classifiés et par les Banques de données communes (BDC) que le Centre de crise peut interroger directement (*hit/no hit*). Les mesures de sécurité relatives aux documents classifiés sont respectées et appliquées par l'officier de sécurité.

I.2.1.2. SPF Justice – Direction générale des Établissements Pénitentiaires

Au sein de la Direction générale des Établissements pénitentiaires du SPF Justice, le point de contact de l'OCAM est la Cellule Extrémisme (CelEx), chargée du suivi des détenus signalés comme radicalisés.

Deux collaborateurs de CelEx sont détachés à l'OCAM comme experts. Ils participent ainsi aux missions de l'OCAM, par exemple dans le cadre du suivi et de l'évaluation de combattants terroristes étrangers, au sein du groupe de travail Prisons ou encore des *Local Task Force* (LTF). Ils ne sont par contre pas tenus au courant des changements potentiels au sein de la Direction générale des Établissements Pénintentiaires (DG EPI). Si CelEx ne voit pas la plus-value de ce détachement, perçu surtout comme une perte de capacité, l'OCAM apprécie en revanche l'expertise du milieu carcéral qu'apportent ces deux collaborateurs.

---

[10] L'Unité d'Information des Passagers collecte, enregistre et traite les données des passagers utilisant un transport international depuis, vers ou via la Belgique, tant à l'intérieur qu'à l'extérieur de l'Union européenne. Les données des passagers arrivent en continu des transporteurs et sont analysées sur la base de critères préalablement définis et confrontées aux banques de données BDC (Banques de Données Communes - OCAM) et BNG (Banque de données Nationale Générale - Police). Lorsque qu'il y a un « hit » en BDC (identités correspondantes), les informations sont encodées et envoyées notamment à l'OCAM. En outre, les données peuvent également faire l'objet de recherches ciblées.

Le flux d'informations avec la DG EPI se fait en grande majorité à destination de l'OCAM. La DG EPI fournit en effet un nombre important d'informations issues du réseau pénitentiaire à l'OCAM et, en retour, reçoit les évaluations des détenus. C'est également le service qui fait le plus de demandes d'informations (RFI) à l'organe de coordination.

L'accès aux BDC et leur alimentation facilitent ce flux d'informations. En outre, les routines de communication et de transmission mises en place (par e-mail via les boites fonctionnelles ou par porteur pour les documents classifiés) garantissent un bon fonctionnement.

CelEx doit toutefois gérer un flux important d'informations qui lui arrivent du réseau pénitentiaire. S'il dit ne pas manquer de personnel, le service souligne en revanche le besoin d'outils informatiques en appui à une meilleure gestion et à une meilleure analyse de toutes les informations qu'il reçoit.

Une permanence officielle serait également une plus-value non négligeable pour la DG EPI et ses différents partenaires.

I.2.1.3. SPF Finances – Administration générale de la Trésorerie

La coopération entre l'OCAM et l'Administration générale de la Trésorerie du SPF Finances s'inscrit uniquement dans le cadre du gel des avoirs des personnes liées au terrorisme.[11] La section Sanctions Financières du service *Compliance* au sein de la Trésorerie a été désignée point de contact à cette fin.

Le flux d'informations entre ce service d'appui et l'OCAM est quantitativement faible, ce qui peut s'expliquer par la spécificité de leur collaboration. De plus, il est très rare que l'Administration générale de la Trésorerie recueille des informations jugées pertinentes pour l'OCAM.

Un membre du personnel est détaché à l'OCAM depuis février 2019. Les procédures liées au gel des avoirs ne représentent toutefois que 20% de son temps de travail. Rattaché au département 'Appui stratégique - Communication' de l'OCAM, ce membre du personnel est en outre chargé de tâches administratives.

Les informations échangées avec la Trésorerie sont non classifiées. L'échange se fait essentiellement par e-mail via les boites fonctionnelles et professionnelles. Depuis fin 2020, la Trésorerie a en outre un accès direct aux BDC et une obligation de les alimenter. Une procédure interne a été élaborée par l'officier de sécurité en ce qui concerne l'accès et l'encodage dans les BDC.

---

11 Circulaire du 7 septembre 2015 relative à la mise en œuvre des articles 3 et 5 de l'A.R. du 28 décembre 2006 relatif aux mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le financement du terrorisme – liste nationale.

I.2.1.4. SPF Justice – Direction générale de la Législation et des Libertés et Droits fondamentaux – Laïcité et Cultes

La désignation du Service des cultes et de la laïcité comme service d'appui de l'OCAM doit se lire au regard de ses compétences dans le cadre de la reconnaissance des cultes et organisations philosophiques non confessionnelles et de la gestion du statut des ministres du culte et représentants du Conseil Central Laïque (CCL). L'OCAM échange plus particulièrement avec la cellule « terrorisme et radicalisation » du service. Ce nouveau statut permet de légaliser le transfert d'informations, bien que le service ne récolte que peu d'informations pertinentes pour l'organe de coordination.

Une réunion a très vite été organisée entre l'OCAM et ce service d'appui supplémentaire afin de préciser les modalités de la coopération entre les deux services ainsi qu'entre le *Data Protection Officer* (DPO) et l'officier de sécurité du SPF Justice afin de mettre en place les accès ICT des BDC.

Le Service des cultes et de la laïcité a en effet accès aux BDC. Si le cadre légal prévoit uniquement un accès à la BDC Propagandistes de haine par interrogation directe (*hit/no hit*), il a été constaté que le service avait, en pratique, un accès complet aux BDC – qu'il juge utile et nécessaire. Le Comité a relevé l'importance de régulariser cet accès.[12]

Aucun membre du personnel n'a été détaché à l'OCAM, mais un collaborateur de l'organe de coordination a été désigné comme point de contact.

L'échange (restreint) d'informations se fait essentiellement par e-mail. Le service d'appui ne dispose toutefois pas d'une boite fonctionnelle : les e-mails sont par contre systématiquement adressés aux deux membres de la cellule « terrorisme et radicalisation » et au chef de service. Les documents classifiés seront transmis via le système BINII, désormais opérationnel au sein du SPF Justice, mais dans l'attente de l'élaboration de procédures internes pour son utilisation.

I.2.2. CONSTATATIONS ET CONCLUSION

Au terme de l'enquête, les Comités concluaient que les quatre services d'appui supplémentaires avaient identifié respectivement un point de contact pour leurs échanges avec l'OCAM qui centralise les informations échangées. Des membres du personnel sont détachés à l'OCAM pour la DG EPI (deux personnes) et la Trésorerie (une personne). Si la DG EPI y voit une perte de capacité, l'OCAM valorise l'expertise dont disposent ces collaborateurs.

12 Voir 'Chapitre V. Le contrôle des banques de données' ('V.2.3. de nouvelles recommndations').

L'échange d'informations est le plus important avec le Centre de crise et la DG EPI. En ce qui concerne la Trésorerie et le Services des cultes et de la laïcité, la collaboration avec l'OCAM reste très spécifique et restreinte à leurs compétences.

Tant L'OCAM que les services d'appui supplémentaires jugent l'échange d'informations entre eux comme étant très bon. Si des échanges avaient déjà lieu par le passé, la désignation comme service d'appui permet de légaliser cette collaboration, en particulier via les BDC. À travers son département gestion de dossiers/documentation, l'OCAM organise une permanence et dispose d'une boite fonctionnelle pour tous les échanges d'informations. À l'exception du Service des cultes et de la laïcité, ils disposent tous d'une boite fonctionnelle.

Les normes minimales de sécurité pour la conservation des documents classifiés sont respectées. La procédure pour l'utilisation du système BINII doit toutefois encore être finalisée pour le SPF Justice. Seule la Trésorerie n'échange pas d'informations classifiées avec l'OCAM.

I.3. L'ÉCHANGE D'INFORMATIONS SUR UN COLLABORATEUR ENTRE LES SERVICES DE RENSEIGNEMENT ET UN EMPLOYEUR PRIVÉ OU PUBLIC

En août 2019, le Comité permanent R a reçu une plainte d'une personne qui travaillait pour une institution publique. L'intéressé se plaignait que son employeur avait transmis et demandé des informations le concernant à un service de renseignement, et sur cette base, entendait entreprendre des démarches disciplinaires.

Afin de traiter cette plainte, le Comité a ouvert une enquête visant à déterminer les cas et les conditions dans lesquels une instance privée ou publique peut adresser une demande à l'un des deux services de renseignement sur un collaborateur (ou un candidat à un emploi) ainsi que les cas dans lesquels le service de renseignement concerné peut ou doit y répondre et, le cas échéant, à quelles exigences cette réponse doit satisfaire.[13]

I.3.1. LE CADRE GÉNÉRAL

Qu'un service de renseignement fournisse des informations sur un collaborateur (ou un candidat à un emploi) d'initiative ou à la demande d'un employeur constitue dans les deux cas une ingérence dans la vie privée et dans le droit à la protection

[13] Un avis juridique externe portant sur le respect du droit à la vie privée des travailleurs dans le cadre d'échanges éventuels entre des employeurs et les services de renseignement a été sollicité le 14 avril 2020.

des données à caractère personnel, et ce même s'il s'agit d'une relation de travail. Une telle ingérence n'est permise que s'il existe une base légale claire, si l'ingérence poursuit un objectif légitime et si elle est proportionnée (article 8 de la Convention européenne des droits de l'homme (CEDH), Convention 108 et 108+ et article 22 de la Constitution).

Dans ce cadre, il convient également de mentionner l'article 2 § 1er, alinéa 2, de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) qui dispose que les services de renseignement *'[d]ans l'exercice de leurs missions (…) veillent au respect et contribuent à la protection des droits et libertés individuels, ainsi qu'au développement démocratique de la société'*.

Aucune disposition de la L.R&S n'interdit qu'une instance privée ou publique adresse une demande à l'un des services de renseignement belges. Si un employeur s'adresse à un service de renseignement, il y a une ingérence dans la vie privée que seule une base légale claire rend possible. La L.R&S le permet dans la mesure où l'employeur croit raisonnablement que les informations qu'il communique peuvent être utiles pour l'exécution des missions du service de renseignement concerné (article 14 L.R&S pour les acteurs publics ; article 16 L.R&S pour les acteurs privés).

En ce qui concerne la réponse éventuelle à apporter par le service de renseignement interrogé, le législateur belge n'a prévu que deux cas dans lesquels un employeur (à son initiative ou à l'initiative du service de renseignement) peut obtenir directement ou indirectement des informations sur un collaborateur (ou un candidat à un emploi) : en cas de screening de sécurité ou en cas de menace. Même la simple question de savoir si un collaborateur (ou un candidat à un emploi) est 'connu' ou non d'un des deux services de renseignement belges, doit pouvoir être associée à l'un de ces deux cas de figure.

I.3.2. L'EMPLOYEUR SOUHAITE UN SCREENING DE SÉCURITÉ

I.3.2.1. La base légale pour les screenings de sécurité

Les screenings de sécurité font référence aux situations dans lesquelles un employeur, indépendamment d'un élément antérieur, souhaite que toutes les personnes qui ont besoin d'une autorisation ou d'un permis donné(e) soient soumises à un screening.[14] Un employeur privé ou public peut recourir à cette option dans les conditions prévues par la Loi du 11 décembre 1998 relative à la classification, aux

[14] Les exemples les plus classiques sont ceux d'une habilitation de sécurité en vue d'avoir accès à des informations classifiées, l'attestation de sécurité pour un accès à un lieu ou à un événement déterminé, ou encore un avis de sécurité qui peut être demandé pour des dizaines d'autorisations différentes.

habilitations, attestations et avis de sécurité (L.C&HS). En principe, l'employeur ne recevra que le résultat du screening.[15]

Dans certains cas (par ex. une habilitation de sécurité), le collaborateur est soumis à une forme de 'screening permanent'. En d'autres termes, pendant toute la durée de son habilitation, il devra répondre aux exigences pour disposer de cette habilitation. Si, à un moment donné, un employeur doute de cette condition, il peut consulter son officier de sécurité, qui, à son tour, peut saisir l'autorité de sécurité et/ou le service de renseignement ayant effectué l'enquête. Mais rien n'empêche l'employeur de prendre contact directement avec un service de renseignement s'il estime disposer d'informations utiles pour l'exercice de ses missions (articles 14 ou 16 L.R&S).

Il importe donc de souligner que le cadre légal détermine clairement quelles données à caractère personnel peuvent être transmises, sous quelle forme (par ex. un rapport d'enquête) et à quel destinataire (généralement une autorité de sécurité).

I.3.2.2. Article 19, alinéa 1er, première partie de la phrase L.R&S[16]

Le Comité a rappelé que l'article 19 L.R&S ne constitue pas une base pour la transmission systématique d'informations aux employeurs qui en font la demande dans le cadre des autorisations ou des permis qu'ils doivent accorder.

---

15 C'est l'officier de sécurité – personne désignée au sein d'une instance privée ou publique chargée de faire respecter les règles en matière de classification et personne de contact entre l'instance, l'intéressé et l'autorité de sécurité compétente – qui sera informé des éléments concrets du dossier. Mais cet officier de sécurité sera soumis à un secret professionnel spécifique et sanctionné pénalement (articles 23 et 24 de la Loi Classification) l'empêchant de communiquer tels quels à l'employeur les éléments dont il dispose.

16 Le premier paragraphe complet de l'article 19 L.R&S se lit comme suit: '*Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une [menace] visée aux articles 7 et 11.*'

I.3.3. L'EMPLOYEUR FAIT L'OBJET D'UNE MENACE (PRÉSUMÉE)

I.3.3.1. Article 19, alinéa 1er, dernière partie de la phrase L.R&S

L'article 19 L.R&S s'énonce comme suit : *'Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa (…) qu'aux instances et personnes qui font l'objet d'une [menace] visée aux articles 7 et 11.'*[17]

Cet article constitue une base légale claire pour un service de renseignement aux fins de communication de données (à caractère personnel) à des personnes ou à des instances publiques ou privées[18], et donc, le cas échéant, également à un employeur dont le collaborateur représente une des menaces que doivent suivre la Sûreté de l'État (VSSE) ou le Service Général du Renseignement et de la Sécurité (SGRS) en vertu de la loi.

Cette disposition constitue aussi, en combinaison avec l'article 14 ou 16 L.R&S, la base légale pour un employeur public ou privé inquiet qui interroge un service de renseignement sur son collaborateur parce qu'il estime qu'il représente une menace (potentielle) au sens de la L.R&S.[19] Ces articles sont également la base juridique permettant de communiquer, en réponse à cette question, des éléments concrets sur le collaborateur qui peuvent rendre la menace (présumée) plausible.[20]

I.3.3.2. Une élaboration plus poussée de cette réglementation dans une directive ?

Si la dernière partie de phrase de l'article 19, alinéa 1er L.R&S offre une base juridique suffisamment claire pour la communication d'informations à des

---

17 Le Comité s'est déjà penché sur l'application de la dernière partie de la phrase de l'article 19, alinéa 1er L.R&S dans le cadre de deux précédentes enquêtes : COMITÉ PERMANENT R, *Rapport d'activités 2015*, 41 et suiv. ('II.9. Plainte relative à la transmission d'informations à caractère personnel à un tiers par un agent de renseignement') ; COMITÉ PERMANENT R, *Rapport d'activités 2012*, 14 et suiv. ('II.2. Le suivi par certains services de renseignement étrangers de leur diaspora en Belgique').

18 La loi ne fait référence qu'à des 'instances et personnes'. Il n'y a aucune raison de croire que cette réglementation, hormis la première partie de phrase de l'article 19, alinéa 1er L.R&S, serait limitée aux personnes (morales) publiques.

19 Le fait que le cadre légal permette à un employeur d'un service public de communiquer des informations ou de poser des questions concernant l'un des membres de son personnel aux services de renseignement ne signifie pas que les services de renseignement peuvent ou doivent répondre à la question posée. Le fait que le service de renseignement ne peut (ou ne veut pas) répondre à une question ne rend pas illégal ou fautif le fait d'avoir posé la question.

20 Cette communication/question peut naturellement donner lieu, pour un service de renseignement, à l'ouverture d'une enquête de renseignement. D'un point de vue juridique, l'ouverture ou non d'une telle enquête, plus ou moins approfondie, est distincte de la question de savoir si et ce qu'un service de renseignement peut communiquer à un employeur. Il n'est évidemment pas légitime d'initier une enquête (par définition attentatoire à la vie privée) en l'absence de tout élément indiquant une menace potentielle ou concrète contre les intérêts fondamentaux de l'État.

instances publiques et privées, il existe une obligation de préciser les modalités de cette communication.

Conformément à l'article 20 § 3 L.R&S, le Conseil national de sécurité (CNS) doit définir, dans une directive, les conditions dans lesquelles des renseignements peuvent être communiqués à des instances ou à des personnes privées ou publiques.

Pour autant que le Comité ait pu le constater, cette obligation n'avait pas encore été remplie en ce qui concerne la situation des personnes et des instances qui font l'objet d'une menace.[21] Au terme de l'enquête, le Comité a souligné encore une fois l'importance pour le CNS d'émettre une telle directive offrant des points d'appui aux services de renseignement dans cette matière délicate, où la (non-) communication des informations peut avoir de graves répercussions sur l'intérêt général et sur les intérêts privés.

L'importance d'une telle directive a semblé d'autant plus grande aux yeux du Comité qu'il a pu constater qu'aucune réglementation n'avait été élaborée à cet égard au niveau des services de renseignement. En ce qui concerne la VSSE, il peut néanmoins être fait référence à deux directives. Il y a tout d'abord l'instruction du 10 octobre 2016 classifiée 'CONFIDENTIEL' qui traite de la manière dont le service doit réagir en cas de demande d'une autorité publique de vérifications concernant une personne déterminée. Le Comité a cependant pu constater que cette directive ne précise pas sur la base de quelle législation certaines réponses doivent être apportées et qu'elle ne semble pas s'appliquer à la situation prévue dans la dernière partie de phrase de l'article 19, alinéa 1er L.R&S. Du moins, elle ne règle pas les relations avec les acteurs privés. La légalité de certains passages de cette directive, qui semblent contraires à la réglementation sur les screenings de sécurité, pose par ailleurs question. La VSSE a également établi en 2018 une directive classifiée 'CONFIDENTIEL' sur les actions disruptives ou les entraves.[22] Si la communication d'informations à une personne ou à une instance faisant l'objet d'une menace peut parfaitement entrer dans cette définition, aucune référence n'est faite dans cette directive à l'article 19 L.R&S, ni à aucune autre disposition légale.

I.3.3.3. Les limites posées par la Loi organique des services de renseignement et de sécurité

Dans quels cas et dans quelles limites un service de renseignement peut-il actuellement faire usage de la possibilité d'informer un tiers (public ou privé) des informations dont il dispose ?

---

21 Dans le cadre d'une enquête portant sur la lutte contre le terrorisme et l'extrémisme, le Comité avait déjà insisté sur la nécessité d'une telle directive (COMITÉ PERMANENT R, *Rapport d'activités 2012*, 92).

22 Il s'agit d'entraver les menaces à un point tel qu'elles ne se produisent plus ou que leur nuisibilité s'en trouve considérablement réduite.

En ce qui concerne la VSSE, les menaces visées à l'article 19 L.R&S sont toutes les activités d'espionnage, d'ingérence, de terrorisme, d'extrémisme, de prolifération, ainsi que toutes activités menées par des organisations sectaires nuisibles ou des organisations criminelles susceptibles de mettre en péril la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'État, la sauvegarde du potentiel scientifique ou économique, tel que défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays (article 7 L.R&S). Il doit non seulement y avoir une activité bien définie dans le chef du collaborateur (par ex. l'extrémisme), mais celle-ci doit également représenter un danger pour un ou plusieurs intérêts fondamentaux de l'État. Dans le contexte de l'article 19 L.R&S, cette instance privée ou publique doit, en outre, faire l'objet d'une menace. Un employeur ne peut donc pas être informé, par exemple des activités extrémistes de son collaborateur, s'il ne fait nullement l'objet d'une menace.

Par ailleurs, l'article 19 L.R&S ne peut être appliqué que lorsque les intérêts fondamentaux de l'État sont en jeu, et donc pas s'il s'agit uniquement de porter atteinte à l'image d'une entreprise privée (sauf si cela signifie, par exemple, une perte de confiance dans certaines instances), d'une mauvaise ambiance de travail ou d'une perte financière (sauf si ces intérêts financiers dépassent les intérêts individuels de l'entreprise et peuvent être considérés comme fondamentaux pour le pays).

Les menaces qui peuvent amener le SGRS à avertir des instances ou personnes privées ou publiques figurent à l'article 11 L.R&S. Il s'agit, par exemple, de toute activité qui représente une menace pour l'intégrité du territoire national ou la population, les plans de défense militaires, le potentiel scientifique et économique dans les secteurs économiques et industriels liés à la défense, l'accomplissement des missions des Forces armées et/ou la sécurité militaire du personnel relevant du ministre de la Défense.

Étant donné que la communication de données sur la base de la dernière partie de phrase de l'article 19, alinéa 1er L.R&S a une finalité clairement définie (sauvegarde des intérêts fondamentaux de l'État contre certaines activités dont l'instance ou la personne concernée fait l'objet), cette communication doit également se limiter aux informations qui contribuent au suivi ou, si nécessaire, à la neutralisation de la menace.

La première obligation d'un service de renseignement qui se voit confronté à une demande d'informations est par conséquent de vérifier de quel problème, de quel incident, de quelle menace il pourrait s'agir. Dans ce cadre, le service de renseignement pourrait interroger ses banques de données.[23] Il apparaît aussi évident que le service de renseignement prenne contact avec l'employeur afin de bien contextualiser la demande. À cet effet, il conviendra de déterminer notamment

[23] C'est également ce que prescrit la directive de la VSSE du 10 octobre 2016 ('CONFIDENTIEL') dans le cadre d'une demande adressée par une autorité publique en vue de faire procéder à des vérifications sur une personne.

pourquoi l'employeur veut savoir si son collaborateur est connu des services de renseignement, quel est le problème et la menace, s'il y a eu un incident de sécurité ou autre, une urgence, etc.

Si ces données ne sont pas concluantes dans un sens ou dans l'autre, une enquête plus approfondie du service peut être indiquée. L'amplitude de cette dernière ne peut être déterminée *in abstracto*. Elle dépendra de la nature de la menace et des informations qui apparaîtront au cours de celle-ci. Dans le cadre d'une telle enquête, le service devra en tout cas tenir compte des principes de proportionnalité et de subsidiarité.

Les réponses à ces questions et les résultats de l'enquête complémentaire doivent permettre au service de renseignement d'évaluer s'il est compétent en la matière et, le cas échéant, s'il peut appliquer l'article 19 L.R&S. Ces réponses doivent également permettre au service de renseignement de déterminer ce qu'il peut ou non communiquer à l'employeur compte tenu de la menace.

I.3.3.4. Qu'est ce qui peut ou doit être communiqué ?

Dans ce qui suit, on part du principe qu'il existe effectivement une menace. La question se pose alors de ce qui peut être communiqué de quelle manière.[24]

I.3.3.4.1. Les principes de proportionnalité et de subsidiarité

Compte tenu des exigences de proportionnalité et de subsidiarité, la première question doit être de savoir si l'employeur peut être informé. Si la menace est très vague et peu grave, ou si le service peut lui-même suivre l'évaluation de la menace ou encore si la menace peut être contrée d'une autre manière (par ex. en s'adressant au collaborateur de sorte qu'il soit conscient d'être suivi), il se peut que la communication de données à caractère personnel à un employeur soit disproportionnée et non subsidiaire.

Si cela ne suffit pas et que la menace est suffisamment grave, la possibilité se présente alors d'en informer l'employeur. Ici aussi, il faut tenir compte de la quantité et du type d'informations qui sont données. Une fois encore, la règle est que, compte tenu de la nature et de la gravité de la menace et de la nécessité et

[24] Tout d'abord, l'hypothèse brièvement évoquée est celle du service de renseignement qui n'identifie absolument aucune menace dans le chef du collaborateur au sens de la L.R&S (éventuellement après avoir questionné une première fois ledit collaborateur ou après une enquête plus approfondie). À ce moment-là, l'employeur ne fait, par définition, pas l'objet d'une menace et *sensu stricto* l'article 19 L.R&S ne peut être appliqué. Le Comité estime cependant que dans ces cas, le service de renseignement doit avoir la possibilité d'informer l'employeur qu'il n'y a pas de menace au sens de la L.R&S (ce qui ne signifie évidemment pas que l'employeur ne peut pas faire l'objet d'une autre menace). Le Comité s'est déjà prononcé en ce sens dans une enquête précédente (COMITÉ PERMANENT R, *Rapport d'activités 2015*, 41 et suiv. ('II.9. Plainte relative à la transmission d'informations à caractère personnel à un tiers par un agent de renseignement')).

des options disponibles pour la contrer, l'objectif doit être une ingérence minimale dans la vie privée.

Cependant, si la menace est si grave qu'elle ne peut être contrée que par l'intervention de l'employeur, davantage d'informations et des informations plus concrètes peuvent être communiquées. Ces informations peuvent, par exemple, servir à motiver une décision administrative ou privée (une sanction disciplinaire, une mutation, un licenciement, etc.). De toute évidence, l'objectif ultime du service de renseignement doit être dans ce cas-ci de neutraliser ou d'atténuer une menace.

Dans le prolongement de la question de la communication proportionnée des informations, un service de renseignement peut-il, dans le cadre de sa communication, lui-même proposer une solution à l'instance publique ou privée qui est menacée, voire participer à la prise de décision de l'instance ou de la personne menacée sur la manière de traiter cette menace (par ex. suggérer un licenciement) ? Le Comité a estimé que ceci n'est pas illégal dans la mesure où la solution qui est suggérée est elle-même légale et proportionnée.

Enfin, la question s'est posée de savoir si l'article 19 L.R&S prévoit une obligation de répondre à une question ou de fournir des informations d'initiative. La disposition prévoit que les services de renseignement et de sécurité 'ne communiquent' leurs renseignements 'qu'aux' instances et personnes qui font l'objet d'une menace. Même si la disposition dans ce domaine n'est pas très claire, le Comité a estimé qu'un service de renseignement est tenu de communiquer des données s'il s'agit du seul moyen d'empêcher la concrétisation d'une menace grave contre les intérêts fondamentaux de l'État. Dans les autres cas, le service définit la meilleure stratégie en toute autonomie, en fonction de la menace. Le Comité a recommandé de pallier ce manque de clarté, soit via une initiative législative, soit via une clarification en la matière dans la directive que doit émettre le CNS.

Dans la foulée, le Comité a suggéré d'examiner s'il serait utile de prévoir une notification obligatoire à l'employeur pour chaque collaborateur (ou candidat à un emploi) figurant dans la Banque de données commune *Terrorist Fighters* ou Prédicateurs de haine.

I.3.3.4.2. Autres points d'attention : précaution, classification, communication écrite

Dans un contexte de renseignement, il y a peu de certitudes, et ce fait doit influencer la décision d'informer ou non un employeur ainsi que la manière de le faire. Pour pouvoir être considérée comme légale, la communication d'informations doit être

suffisamment étayée par des informations fiables. Elle doit également être formulée avec précaution.[25]

Par ailleurs, toutes les instances privées et publiques ne disposent pas d'une habilitation de sécurité, ce qui signifie que les informations classifiées devront être déclassifiées. Ceci est d'autant plus vrai si les informations doivent servir à étayer une décision de l'employeur.

Enfin, l'article 19 L.R&S ne précise pas comment informer une autorité qui est menacée. Le Comité a estimé que, pour des raisons de sécurité juridique, cette notification devrait se faire par écrit, sauf en cas d'urgence, afin d'éviter les discussions *a posteriori* et de permettre un contrôle parlementaire, et même judiciaire.

I.3.4. CONCLUSIONS

Des règles strictes s'appliquent, à raison, à la communication d'informations par les services de renseignement à un employeur privé ou public. En effet, la communication d'informations peut avoir des conséquences non négligeables pour les personnes concernées. À tout le moins, cela signifie une atteinte à la vie privée et, dans les cas extrêmes, cela peut constituer la base de mesures intrusives pouvant affecter la situation juridique des intéressés.

Si la VSSE et le SGRS fournissent des informations à un employeur public ou privé, que ce soit d'initiative ou sur demande (en ce compris le fait de simplement informer que la personne est 'connue' ou non), ils doivent respecter toutes les exigences légales :

1. Une base légale spécifique doit exister ;
2. Il faut faire preuve de vigilance dans la production interne des données à fournir et dans leur communication au destinataire ;
3. La communication doit répondre aux exigences de nécessité ;
4. La communication doit être proportionnée.

En ce qui concerne la base légale, le Comité a souligné qu'en dehors des deux situations évoquées (c.-à-d. l'employeur veut un screening de sécurité ou l'employeur fait l'objet d'une menace), il n'est pas permis de fournir des informations sur un collaborateur à un employeur public ou privé. Du point de vue de l'agent de

[25] Par exemple, aucune image sans nuance ne peut être donnée des renseignements sous-jacents, ou un élément particulier ne peut être présenté comme étant une 'vision de' ou une 'impression de'. En ce sens, les informations fournies doivent également être 'justes' en offrant une image objective de la façon dont le service de renseignement perçoit la menace et le rôle de la personne concernée, sans être 'manipulatrices' au sens où elles viseraient à orienter les décisions des employeurs privés ou publics.

renseignement, ce genre de communication peut même être punissable en fonction de la situation concrète.

Le Comité a souligné également que rien n'empêche un employeur du secteur public ou privé de communiquer des informations ou d'interroger un service de renseignement belge concernant une éventuelle menace, au sens de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S), dont l'un des collaborateurs serait l''auteur'.

Au terme de l'enquête, le Comité invitait cependant les acteurs des secteurs publics et privés à examiner si certaines menaces potentielles ne peuvent pas être évitées en recourant, pour certaines fonctions, autorisations ou permis, au système de screening de sécurité prévu dans la Loi Classification, en ayant un recours judicieux à ce système.

Le Comité estimait que la VSSE et le SGRS, dans les six mois suivant la conclusion de cette étude, devaient rédiger une directive visant à mettre en œuvre la dernière partie de phrase de l'article 19, alinéa 1er L.R&S et l'adresser aux ministres de la Justice et de la Défense pour soumission au Conseil national de sécurité invité à l'approuver.

I.4. DYSFONCTIONNEMENTS GRAVES EN MATIÈRE DE SÉCURITÉ NATIONALE

Début juillet 2020, le président du Comité permanent R adressait un courrier classifié au ministre des Affaires étrangères et de la Défense (de l'époque), compétent notamment de l'Autorité nationale de sécurité (ANS) et du SGRS. En sa qualité de président de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité[26], de graves dysfonctionnements en matière de sécurité nationale avaient été constatés.

Était en cause un dossier de renouvellement en janvier 2020 d'un avis de sécurité par une travailleuse qui avait reçu un avis positif en 2015. Ce dernier lui donnait le droit d'accéder aux zones de l'aéroport de Bruxelles National dont les accès sont limités pour des raisons de sécurité. Il ressortait cependant d'un rapport classifié que le partenaire de l'intéressée était un des co-auteurs présumés des attentats de Paris et Bruxelles, et qu'elle entretenait avec lui des contacts réguliers lors de visites en prison dans une pièce sans surveillance.

[26] L'organe de recours est une juridiction administrative compétente pour connaitre des recours relatifs aux habilitations, attestations et avis de sécurité dans le cadre de la Loi du 11 décembre 1998. Le président de l'Organe de recours est également le président du Comité permanent R. À ce propos, voir 'Chapitre IX. L'organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité'.

Nonobstant le risque sécuritaire indéniable, la décision de retrait de l'avis ou de l'habilitation de l'intéressée ne fût prise qu'à l'introduction de la demande de renouvellement.[27]

Le Comité permanent R a interpellé le gouvernement soulignant que cela mettait en évidence le 'dysfonctionnement' des administrations et services publics dans le domaine de la sécurité, le travail en silo empêchant de garantir la sécurité du citoyen. Le Comité permanent R a souligné la récurrence de ce problème qui avait déjà été mis en exergue par les travaux de la Commission parlementaire 'Attentats terroristes' du 22 mars 2016.[28]

S'en est suivi, entre juillet 2020 et février 2021, un échange de lettres entre le Comité permanent R, le ministre des Affaires étrangères et de la Défense (de l'époque), le président de l'ANS et le président du Collège des procureurs généraux. Il a notamment été demandé qu'un groupe de travail soit mis en place pour analyser les dysfonctionnements identifiés.

Le Comité permanent R a dû constater que peu d'attention était accordée aux problèmes de sécurité nationale qui avaient été soulevés.[29] Ayant atteint les limites de ses prérogatives, le Comité a confié la situation à la Chambre des représentants pour suite utile. Les remarques du Comité permanent R auraient été intégrées dans les travaux des différents groupes de travail mis en place au sein de l'ANS se penchant notamment sur une réforme structurelle de l'ANS.

I.5. LE SUIVI DES ORGANISATIONS SECTAIRES NUISIBLES ET DES ORGANISATIONS CRIMINELLES PAR LA SÛRETÉ DE L'ÉTAT

À la demande de la Commission de suivi, le Comité permanent R a ouvert une enquête visant à analyser la manière dont la VSSE exécutait deux de ses missions

---

27 L'enquête de contrôle sur la manière dont les services de renseignement réalisent les screenings de sécurité a également accordé une attention particulière à cette problématique. Voir COMITÉ PERMANENT R, *Rapport d'activités 2019*, 2-14 ('I.1. La réalisation de screenings de sécurité par les services de renseignement').

28 CHAMBRE DES REPRÉSENTANTS DE BELGIQUE, *Commission d'enquête Attentats terroristes 22 mars 2016. Résumé des travaux et recommmandations*, 2018.

29 Le sujet a fait l'objet de questions parlementaires (cf. Question de C. Thibaut à la ministre des Affaires étrangères sur 'l'absence de réponses de l'ANS au Comité R en matière d'habilitations de sécurité' (*Q.R.*, Chambre 2020-2021, 15 juillet 2021, n°59, p.108, Q. n°601) et d'articles de presse (par ex. L. BOVÉ, *De Tijd*, 6 mai 2021 ('Kamer slaat alarm over veiligheidsscreenings').

légales, à savoir le suivi des menaces que constituent les organisations sectaires nuisibles[30] et les organisations criminelles.[31]

I.5.1. CONTEXTUALISATION

I.5.1.1. Les organisations sectaires nuisibles

Longtemps, les autorités belges ont traité les mouvements réputés sectaires avec une réserve toute particulière. Cette attitude était dictée par la difficulté à prendre position dans un domaine touchant aux libertés fondamentales de religion, de pensée, d'expression et d'association.

Au cours des années 1980, plusieurs événements tragiques et très médiatisés ont attiré l'attention de la population et des autorités sur ce phénomène, ce qui a conduit à plusieurs initiatives en Belgique dans les années 1990. C'est ainsi qu'a été mise sur pied, en 1996, une commission d'enquête parlementaire 'sectes'.[32] Le Centre d'information et d'avis sur les organisations sectaires nuisibles (CIAOSN) ainsi que la cellule administrative de coordination (CAC) ont été institués par la Loi du 2 juin 1998.[33] Le secrétariat de la CAC a été attribué à la Sûreté de l'État.[34]

---

30 Le Comité entend par « secte », « organisation sectaire nuisible » ou « groupement sectaire nuisible », tout groupement à vocation philosophique ou religieuse, ou se prétendant tel, considéré comme nuisible et susceptible, à ce titre, de faire l'objet d'un intérêt quelconque de la part de la VSSE.

31 Le Comité avait déjà, dans le passé, pu se pencher sur plusieurs aspects de cette problématique.
Concernant les organisations sectaires : COMITÉ PERMANENT R, *Rapport d'activités 1996*, 86-96 ("Chapitre II. Enquête sur l'efficacité des services de renseignements relative à l'activité des sectes en Belgique") ; *Rapport d'activités 2006*, 60-61 ("II.6.2. Les organisations sectaires nuisibles et la compétence de la Sûreté de l'État") ; *Rapport d'activités 2007*, 40 ("II.10.9. Organisations sectaires nuisibles") ; *Rapport d'activités 2010*, 13-23 ("II.2. Le suivi des organisations sectaires nuisibles") ; *Rapport d'activités 2014*, 52-55 ("II.5. Une plainte de l'église de Scientologie contre la Sûreté de l'État ")
Concernant les organisations criminelles : COMITÉ PERMANENT R, *Rapport d'activités 2002*, 19-20 (« Chapitre II.2.6 Enquête de contrôle sur les renseignements dont dispose la Sûreté de l'État à propos d'une affaire de fraude aux visas évoquée au Sénat » ; *Rapport d'activités 2004*, 12-18 (IV.2.2 « Enquête sur la manière dont les services de renseignement belges fonctionnent et collaborent dans le cadre de leur nouvelle mission légale concernant les menaces des organisations criminelles ».

32 *Doc. parl.*, Chambre, 1995-1996, n° 313/008.

33 La Loi du 2 juin 1998 portant création d'un Centre d'information et d'avis sur les organisations sectaires nuisibles et d'une Cellule administrative de coordination de la lutte contre les organisations sectaires nuisibles (*M.B.* 25 novembre 1998). Celle-ci prévoit une collaboration active entre le CIAOSN, la CAC et les autres services publics impliqués dans la lutte contre les sectes nuisibles dont le Parquet fédéral, les Parquets généraux, les Parquets, la Police, la Sûreté de l'État et les autorités locales.

34 Arrêté royal du 8 novembre 1998 fixant la composition, le fonctionnement et l'organisation de la Cellule administrative de coordination de la lutte contre les organisations sectaires nuisibles (*M.B.* 9 décembre 1998).

I.5.1.2. Les organisations criminelles

En 2019, la Police Judiciaire Fédérale a réalisé une étude sur les organisations criminelles dans le cadre de laquelle plus de 600 organisations criminelles, associations de malfaiteurs ou groupes d'auteurs ont été renseignés en Belgique.[35]

Dans son rapport de 2020[36], la Cellule de Traitement des Informations Financières (CTIF) mentionne à son tour que 31.605 déclarations lui ont été adressées en 2020. Elle ajoute que 1.228 nouveaux dossiers ont été transmis en 2020 aux autorités judiciaires et que des informations issues de 2.765 déclarations de soupçon ont été utilisées dans une transmission aux Parquets et Parquet fédéral pour un montant total de 1.885,31 millions d'euros. Le rapport précise également que « *2020 a été marquée par un nombre important de dossiers transmis par la CTIF en lien avec la criminalité organisée* ».[37]

I.5.2. LA COMPÉTENCE MATÉRIELLE

La mission de la VSSE en matière de suivi des sectes nuisibles et des organisations criminelles se situe dans le cadre de sa mission de renseignement. Conformément à l'article 7, 1° L.R&S, la VSSE a pour mission *'de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, la sûreté extérieure de l'État et les relations internationales, le potentiel scientifique ou économique défini par le Conseil national de sécurité, ou tout autre intérêt fondamental du pays défini par le Roi sur proposition du Conseil national de sécurité'*.

Le législateur a choisi de dresser une liste limitative des menaces pour la sécurité qui relèvent du domaine de compétence de la VSSE (c'est-à-dire le terrorisme, l'extrémisme, l'espionnage, l'ingérence, la prolifération, les organisations sectaires nuisibles et les organisations criminelles).

Les *'organisations sectaires nuisibles'* sont décrites comme étant *'tout groupement à vocation philosophique ou religieuse, ou se prétendant tel, qui, dans son organisation ou sa pratique, se livre à des activités illégales dommageables, nuit aux individus ou à la société ou porte atteinte à la dignité humaine'* (art. 8, 1°, alinéa 2, L.R&S).

Le législateur a, en outre, désigné les *'organisations criminelles'* comme étant une menace pour la sécurité nationale qui doit relever de la sphère d'intérêt de la VSSE. Cette notion est décrite comme suit dans la Loi organique des services de renseignement et de sécurité : *'toute association structurée de plus de deux*

---

35 Police fédérale belge, 'Diagnostic- Vers une première approche des organisations criminelles', Avril 2020, 4. La PJF souligne que 'la problématique du terrorisme ou de son financement y est citée 20 fois'.

36 https://www.ctif-cfi.be/images/documents/French/Rapports_annuels/ra2020.pdf, 10.

37 https://www.ctif-cfi.be/images/documents/French/Rapports_annuels/ra2020.pdf, 22.

personnes, établie dans le temps, en vue de commettre de façon concertée des crimes et délits, pour obtenir, directement ou indirectement, des avantages patrimoniaux, en utilisant l'intimidation, la menace, la violence, des manœuvres frauduleuses ou la corruption ou en recourant à des structures commerciales ou autres pour dissimuler ou faciliter la réalisation des infractions.' (art. 8, 1°, alinéa 2, f) L.R&S).[38]

La VSSE n'est compétente que pour le suivi des organisations criminelles '*qui se rapportent intrinsèquement aux activités visées à l'article 8, 1°, a) à e) et g)*' – c'est-à-dire les activités de terrorisme, d'extrémisme, d'espionnage, d'ingérence, de prolifération et de sectes nuisibles – *'ou qui peuvent avoir des conséquences déstabilisantes sur le plan politique ou socio-économique*'.

Toutes les organisations sectaires nuisibles et toutes les organisations criminelles ne font donc pas partie de la sphère d'intérêt légale de la VSSE. La Loi organique des services de renseignement et de sécurité prévoit, en outre, que ces organisations ne relèvent de la compétence de la VSSE que si leurs activités sont susceptibles de représenter une menace pour la sécurité intérieure ou extérieure de l'État et/ou pour le potentiel économique ou scientifique du pays.

Le Comité relevait en 2015 l'exception que constituait la Belgique en attribuant à son service de renseignement civil la mission de suivi des organisations sectaires nuisibles : « *aucun autre service de renseignement étranger n'a pour mission officielle de surveiller les sectes nuisibles. Cette mission spécifique de la Sûreté de l'État belge constitue donc une exception dans le monde des services de renseignement.*[39] *La plupart des pays démocratiques refusent même d'impliquer ces services dans la surveillance des mouvements religieux. Parce que cette mesure pourrait être considérée comme une atteinte à la liberté religieuse* ».

I.5.3. LA COMPÉTENCE PROCÉDURALE

La compétence procédurale dans le cadre de la mission de renseignement est déterminée en premier lieu par les activités énumérées à l'article 7, 1° L.R&S : *'(de) rechercher, (d') analyser et (de) traiter le renseignement*'. Il en ressort que la VSSE est chargée de lutter contre les sectes nuisibles et les organisations criminelles en recueillant des informations et en analysant les renseignements, puis en transmettant à d'autres instances (par ex. les autorités policières ou judiciaires) les renseignements obtenus (c'est-à-dire les informations enrichies). Ces instances prendront finalement les contre-mesures qui s'imposent pour protéger la sécurité nationale.

---

38 Le législateur a voulu établir une distinction entre une organisation criminelle comme menace pour la sécurité nationale et une organisation criminelle comme infraction pénale (art. 324*bis* CP).

39 A laquelle la VSSE ajoute (14 avril 2021): "*et le service, au surplus, se trouve privée d'échanges fructueux en la matière avec ses correspondents étrangers*".

Pour réaliser ces missions, la VSSE y affectait, au pic de son activité en ces matières, le personnel suivant :

– *Organisations sectaires nuisibles (1999-2000)* : 6 personnes en 'Section Analyse' (dont 3 niveaux A) et 9 personnes en 'Section Opérationnelle' ;
– *Organisations criminelles* (*années 2000*) : 2 personnes en 'Section Analyse' et 2 personnes en 'Section Opérationnelle'.

I.5.4. LES PRIORITÉS POLITIQUES

Si l'article 7, 1° L.R&S établit une obligation légale d'agir dans le chef de la VSSE, cela ne signifie pas pour autant qu'aucune priorité ne peut être fixée dans le cadre de ses activités. En effet, le service ne dispose pas (et ne pourrait jamais disposer) de capacités et de ressources suffisantes pour détecter, surveiller et contrôler toutes les menaces pour la sécurité nationale relevant de sa compétence. La hiérarchisation des priorités est donc une nécessité, voire une obligation.

Cette lecture est confirmée dans diverses dispositions légales et réglementaires. Tout d'abord, l'article 4 L.R&S stipule que la VSSE accomplit ses missions à l'intervention du ministre de la Justice, mais *'conformément aux directives du Conseil national de sécurité'*.

La mission du CNS est définie à l'article 3 de l'Arrêté royal du 22 décembre 2020 'portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité'. Celui-ci établit que le CNS, *'(e)n tant qu'organe de coordination', 'est chargé de la définition des priorités des services de renseignement et de sécurité'*.

En juillet 2015, ce même Conseil national de sécurité a décidé que la VSSE n'assurerait plus un suivi actif des organisations sectaires nuisibles et des organisations criminelles. Cette décision a été prise sous l'impulsion des ministres de la Justice et de la Défense souhaitant, suite à la vague d'attentats et de tentatives d'attentats en Belgique et à l'étranger, redéfinir la priorité des missions des services de renseignement belges et la réaffectation de leurs moyens en personnel et matériel.

Le 25 août 2015, le ministre de la Justice de l'époque explique que « *De Staatsveiligheid reoganiseert vanaf 1 september haar buitendienst met een ongeziene focus op het radicalisme en het terrorisme* ». Dans ce cadre, la Sûreté de l'État communiquera encore que « *Le plan d'action 2015 de la Sûreté de l'État a été approuvé par le Conseil national de sécurité. Sur la base de ce plan, des décisions ont été prises par la direction de la Sûreté de l'État concernant son organisation* », ajoutant encore « *Conséquence de ce recentrage : les autres menaces telles que les*

sectes et l'espionnage industriel se retrouveront à l'arrière-plan ».[40] En 2020, la VSSE l'a également confirmé en indiquant que le '*suivi actif des organisations sectaires nuisibles a été mis en suspens, sauf au cas où une menace d'ingérence, d'espionnage, de prolifération, d'extrémisme ou de terrorisme y serait liée*'. Le même constat vaut pour les organisations criminelles.

L'article 2 de l'Arrêté royal du 5 décembre 2006 relatif à l'administration générale et à la cellule d'appui de la Sûreté de l'État dispose que la direction générale de la VSSE (c'est-à-dire l'Administrateur général et l'Administrateur général adjoint) est '*responsable de l'élaboration et de la mise en œuvre d'un plan stratégique quadriennal qui détermine les priorités de la Sûreté de l'État et les stratégies opérationnelles pour mettre en œuvre ces priorités*'. L'article 3 stipule que '*les administrateurs généraux de la VSSE soumettent conjointement chaque année au Ministre de la Justice un plan d'action*' lié à la réalisation des priorités du plan stratégique. Ce plan d'action comprend, entre autres, les objectifs stratégiques et les moyens de les concrétiser. L'analyse de ces plans montre que depuis les attentats de Verviers (janvier 2015), Paris (novembre 2015) et Bruxelles (mars 2016), le terrorisme et l'extrémisme (islamiste, de droite et de gauche), ainsi que l'espionnage, constituent les trois fers de lance de la politique de la VSSE et, en tant que tels, sont considérés comme les menaces les plus importantes. Ni les organisations sectaires nuisibles ni les organisations criminelles ne figurent dans la liste des priorités.

I.5.5. LA MARGE DE MANŒUVRE AUTORISÉE

Lorsqu'ils fixent les priorités politiques, le Conseil national de sécurité et le ministre de la Justice sont soumis à des contraintes juridiques. Les priorités doivent d'abord se situer dans la sphère de compétence définie par le législateur, c'est-à-dire dans le cadre des intérêts à protéger et des menaces pour la sécurité qu'il convient de contrer.

En outre, ni le Conseil national de sécurité, ni le ministre de la Justice, pas plus que la VSSE, ne sont compétents pour décider qu'une menace pour la sécurité, dans son intégralité, pour tous les types d'activités de renseignement et en tout temps, ne doit pas faire l'objet d'un suivi. Une telle mesure équivaut à une suspension par le pouvoir exécutif de l'article 7, 1° *p.o.* article 8, 1° L.R&S. L'établissement de priorités dans le cadre des missions de renseignement de la VSSE consiste à déterminer les questions pour lesquelles le service de renseignement doit constituer activement

[40] Le ministre de la Justice confirmera en 2016 encore ce changement d'orientation dans sa réponse à une question parlementaire et précisera qu'un projet modificatif est en cours de rédaction visant à décharger la Sûreté de l'État du secrétariat de la Cellule administrative de coordination, et à la confier au secrétariat du CIAOSN. (Question de K. JADIN au ministre de l'Intérieur sur la « surveillance des sectes » (*C.R.I.*, Chambre 2016-2017, 9 novembre 2016, COM 529, p.14, Q. n° 14723).

une position d'information. Cela ne signifie en aucun cas que si la VSSE reçoit passivement des informations d'un tiers contenant des indications concrètes (*leads*) d'éventuelles activités problématiques[41], la VSSE n'aurait pas le devoir de procéder à une évaluation approfondie et, si nécessaire, d'enquêter activement.[42]

I.5.6. LA TRADUCTION ORGANISATIONNELLE DES PRIORITÉS POLITIQUES

Il convient par ailleurs de se demander dans quelle mesure cette marge de manœuvre juridiquement limitée impacte la traduction organisationnelle des priorités politiques. En d'autres termes : qu'est-ce qui est et qu'est-ce qui n'est pas possible dans le cadre de la création et de la dissolution de services et de sections ? Et faut-il prévoir une capacité réservée ?

Le ministre de la Justice (*cf*. art. 5, § 3 L.R&S) et, à titre subsidiaire, la direction générale de la VSSE (*cf*. art. 2 A.R. 5 décembre 2006) ont, dans le cadre des règles définies par le législateur et le Roi, la responsabilité de définir la structure organisationnelle de la VSSE.[43]

Dans ce cadre législatif et réglementaire, il est laissé à la discrétion du pouvoir exécutif de créer ou non un service (d'analyse) ou une section (opérationnelle) pour une menace de sécurité particulière. La suppression du service d'analyse Sectes et, auparavant, de la section opérationnelle Sectes au sein de la VSSE, relève donc de l'autonomie des décideurs politiques susmentionnés.

Cependant, la VSSE doit s'organiser de manière à pouvoir remplir son obligation légale d'agir lorsqu'elle reçoit passivement des informations d'un tiers contenant des indications concrètes d'éventuelles activités problématiques de sectes nuisibles ou d'organisations criminelles. Une capacité réservée (par ex., x analystes et x agents de collecte) chargée d'examiner ces informations obtenues passivement et, le cas échéant, de recueillir des informations supplémentaires

---

41 Par ex. d'organisations sectaires nuisibles ou d'organisations criminelles telles que définies par la loi.

42 La VSSE a certes la compétence de procéder à une évaluation d'opportunité dans le cadre de ses enquêtes, mais elle a également l'obligation d'enquêter sur les menaces pour la sécurité énumérées par le législateur. Compte tenu du principe de précaution, l'évaluation de *leads* et la décision subséquente de les poursuivre activement ou non, doivent être prises sur la base de critères objectifs préétablis. Compte tenu du principe de légalité, ces critères ne doivent pas conduire à une situation où une menace pour la sécurité définie légalement ne fait jamais l'objet d'une enquête approfondie dans la pratique.

43 Au niveau gouvernemental, l'Arrêté royal du 5 décembre 2006 (*supra*) stipule que la VSSE est composée d'une direction des opérations, d'une direction de l'analyse et d'une direction d'encadrement. Au niveau législatif, la Loi relative à la classification stipule, par exemple, que la VSSE doit disposer d'un officier de sécurité, tandis que la Loi relative à la protection des données stipule que le service doit disposer d'un délégué à la protection des données.

pourrait ainsi être prévue.[44] Ces agents de la VSSE pourraient encore être chargés d'autres tâches définies par le responsable de la VSSE, mais ils jouraient un rôle de première ligne lorsque des informations problématiques sur les sectes ou les organisations criminelles sont transmises à la VSSE.

I.5.7. BESOIN DE RENFORTS ET D'UN DÉBAT SOCIÉTAL

Au terme de l'enquête, le Comité a pu établir que la priorisation des missions du service était conforme au cadre légal et réglementaire.

Après avoir constaté qu'en 2021 la VSSE n'était à même de suivre qu'une partie assez faible de dossiers ouverts – et qu'il en résultait indéniablement pour cette administration (en manque d'effectifs) l'obligation d'effectuer des choix – le Comité a rappelé les demandes pressantes de la VSSE quant à l'augmentation de ses moyens en personnel, financiers et quant à la détermination exacte de ses missions légales.

Enfin, dans ses conclusions, le Comité posait le constat qu'un débat sociétal plus large (lisez : parlementaire ?[45]) s'imposait sur les missions dévolues au service de renseignement civil dans la Loi organique des services de renseignement et de sécurité de 1998 et l'établissement des priorités qui y sont associées. Et par conséquent, l'attribution de capacités et de ressources suffisantes pour détecter, surveiller et contrôler l'ensemble des menaces pour la sécurité nationale relevant de la compétence de la VSSE devrait faire l'objet d'une discussion approfondie.

---

44 La VSSE précise à cet égard (14 avril 2021): *"La Sûreté de l'État applique déjà la recommandation de constituer une 'capacité réservée', à la fois opérationnelle et d'analyse, mobilisable le cas échéant pour assurer un traitement adéquat des informations reçues relatives aux organisations sectaires nuisibles et aux organisations criminelles, au cas où elles intéresseraient la Sûreté de l'État ou le potential scientifique ou économique de la Belgique*".

45 La VSSE réfléchit dans le même sens (14 april 2021): "*C'est au Parlement, tant dans sa fonction de législation que de controle du pouvoir exécutif, qu'il appartiendra d'apprécier (considérant les moyens humains et matériels limités dont la VSSE dispose et la gravité parfois extrême des nombreuses menaces liées à l'extrémisme, au terrorisme, à l'ingérence, à l'espionnage et à la prolifération auxquelles elle est confrontée in concreto) si il est opportun ou bien d'exiger de la Sûreté de l'État qu'elle assure à nouveau le suivi actif des organisations sectaires nuisibles, ou bien de l'en décharger, ou bien de valider la décision du Conseil national de sécurité du 13 juillet 2015 approuvant la mise en suspens du suivi actif des organisations sectaires nuisibles.*"

I.6. L'ATTENTION DES SERVICES DE RENSEIGNEMENT BELGES POUR UN COLLABORATEUR DU SGRS ET SES LIENS AVEC DES CITOYENS RUSSES[46]

En 2014-2015, la VSSE et le SGRS ont conjointement mené une enquête sur un officier de réserve de la Direction I (Renseignement) (de l'époque) du SGRS.

L'auteur des faits entrait déjà en 2008 dans la ligne de mire de la VSSE suite au signalement d'un partenaire étranger. En 2012, son nom est à nouveau mentionné. L'intéressé est situé comme 'cible périphérique' d'un oligarque russe. Deux ans plus tard, la VSSE prendra connaissance de sa qualité d'officier de réserve au SGRS. Une collaboration est alors lancée avec le SGRS. Les éléments en possession des deux services de renseignement semblent mettre en évidence des faits d'espionnage. En février 2015, le SGRS lui retire son habilitation de sécurité. La décision de retrait est confirmée par l'Organe de recours qui a été saisi de l'affaire. Le dossier est clôturé début juillet 2015 par la VSSE. L'intéressé semblait informé de l'enquête menée sur sa personne.

Sur la base des éléments récoltés par le SGRS et la VSSE et lui ayant été communiqués, le Comité permanent R n'a pas pu conclure en l'existence ou non de faits d'espionnage dans le chef de l'intéressé. Depuis la décision de l'Organe de recours, l'auteur des faits a quitté la Défense.

I.7. LE SCREENING DE SÉCURITÉ DES MILITAIRES ET DES CIVILS À LA DÉFENSE

Chaque année, la VSSE et le SGRS passent au crible plusieurs milliers de personnes qui veulent obtenir l'une ou l'autre licence ou autorisation, ou qui souhaitent exercer une fonction déterminée. Ce faisant, ils entendent vérifier si les intéressés offrent des garanties suffisantes en termes de fiabilité et de sécurité. Précédemment, le Comité a ouvert une enquête de contrôle plus large sur la manière dont les services de renseignement réalisent les screenings de sécurité.[47] [48]

---

[46] Cette brève enquête avait pour but d'informer la Commission de suivi suite à la demande d'information adressée par un membre de ladite Commission au Comité permanent R le 6 juin 2019.

[47] Par screening de sécurité, on entend « *une évaluation imposée par la loi et conforme à celle-ci, effectuée par une autorité administrative sur la base des données (à caractère personnel) dont elle dispose déjà ou qui lui ont été communiquées, par laquelle elle décide si le profil d'une personne (morale) privée présente ou peut présenter un risque d'usage non approprié d'une autorisation déterminée susceptible de mettre en péril certains intérêts fondamentaux (de l'État), de sorte que cette même autorité ou une autre autorité (étrangère) qui en est informée peut décider de l'octroi, du retrait ou de la limitation de cette autorisation.* ».

[48] COMITÉ PERMANENT R, *Rapport d'activités 2019*, 2 et suiv. ('La réalisation des screenings de sécurité par les services de renseignement').

Suite à cette enquête, il a été constaté que certains membres du personnel de la Défense n'ont jamais été soumis à un tel screening de sécurité au moment de leur candidature, de leur recrutement ou au cours de leur carrière, ou seulement une fois. Par conséquent, le Comité permanent R s'est penché sur le screening du personnel militaire et civil de la Défense (I.7.1.), ainsi que sur le screening des étudiants de l'École Royale Militaire (I.7.2.).

I.7.1. LE SCREENING DES MILITAIRES ET DES CIVILS DE LA DÉFENSE

La Loi du 28 février 2007 fixant le statut des militaires et candidats militaires du cadre actif des Forces armées décrit notamment la procédure de recrutement.

Les candidats militaires doivent satisfaire à diverses conditions : ils doivent jouir de leurs droits civils et politiques, et disposer des qualités morales indispensables (artt. 8 et 9). Enfin, ils ne peuvent pas avoir reçu un avis de sécurité négatif après une vérification de sécurité ou avoir refusé celle-ci. Cela signifie que, sauf à considérer que la carrière de l'intéressé impose une modification du niveau de sécurité, un militaire du département de la Défense ne subit qu'un seul *screening* de sécurité durant l'entièreté de sa carrière militaire. Le Comité était d'avis qu'il y avait lieu de se demander si une vérification de sécurité ne devrait pas se répéter périodiquement durant la carrière du personnel militaire.[49]

La situation est différente pour les (candidats) civils auprès de la Défense.[50] La grande majorité du personnel civil, soit 1.100 personnes, est statutaire ; ces fonctionnaires ayant été nommés et ayant prêté serment. Un deuxième groupe de civils est constitué par les contractuels qui sont engagés sur la base d'un contrat de travail, exactement comme dans le secteur privé. Par ailleurs, il y a encore des civils qui ne sont pas considérés comme du personnel de la Défense (p. ex. des chercheurs engagés par le Patrimoine, des professeurs détachés des Communautés à l'École Royale des Sous-Officiers…). Tout recrutement civil, à l'exception des contrats Rosetta[51], passe obligatoirement par le SELOR.

À de rares exceptions près[52], les civils du Département de la Défense ne font l'objet d'aucune vérification de sécurité. Le Comité était d'avis que cette différence

---

49 Il apparaît que l'intégrité de certains militaires peut effectivement poser problème. Cela signifie que ces militaires ne seront connus comme tels que lorsqu'ils représenteront une menace qui aura été détectée par le SGRS.

50 En ce compris les membres du service d'assistance religieuse et morale (SARM).

51 Les contrats Rosetta, ou 'Conventions de premier emploi', sont des contrats d'un an proposés à des jeunes de moins de 26 ans. La Défense organise elle-même les interviews de recrutement en fonction de ses besoins.

52 Par exemple, ceux qui sont recrutés ou détachés auprès du SGRS, étant donné que disposer d'une habilitation de sécurité constitue une des conditions essentielles pour pouvoir y travailler.

de traitement ne peut se justifier que si l'usage inapproprié de la fonction qu'ils occupent n'est pas susceptible de menacer les intérêts fondamentaux de l'État.

Le Comité permanent R soulignait également, à cet égard, les conséquences de l'évolution de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité. En effet, outre une menace potentielle ou concrète dans un bâtiment ou un lieu, certains sites peuvent par nature (et en permanence) être sensibles aux menaces : le tarmac d'un aéroport, une base de la Défense, etc. L'utilisation inappropriée de la possibilité d'accéder à un tel lieu peut porter sérieusement atteinte aux intérêts fondamentaux de l'État. Il en va de même pour les personnes qui exercent une fonction ou mission particulière ou qui souhaitent obtenir une autorisation spécifique. Initialement, la loi permettait à « toute autorité administrative » d'exiger de tels avis (positifs).[53]

La Loi du 23 février 2018 et l'AR du 8 mai 2018[54] ont réformé la procédure d'avis de sécurité, que ce soit au niveau de la décision réglementaire de l'autorité administrative ou du mécanisme de décision individuelle.

I.7.2. LE SCREENING DE SÉCURITÉ POUR LES ÉTUDIANTS (ÉTRANGERS) DE L'ÉCOLE ROYALE MILITAIRE ?

L'École Royale Militaire (ERM) est une institution militaire d'enseignement universitaire destinée à la formation académique, militaire, et physique des futurs officiers, ainsi qu'à la formation continue d'officiers pendant leur carrière à la Défense.[55]

L'ERM ouvre également ses portes à des élèves étrangers. La Sûreté de l'État relevait que « *les universités sont en général ouvertes à la coopération internationale, ce qui constitue indéniablement une valeur ajoutée. Toutefois, cette ouverture n'est pas sans risque. D'autres acteurs savent que nos universités sont une véritable mine d'or. […] Des étudiants d'instituts de recherche militaire (tels que la Chinese National*

---

53 La décision (de nature réglementaire) de requérir un avis de sécurité (individuel) pouvait être prise « *lorsque l'exercice d'une profession, d'une fonction, d'une mission, d'un mandat ou l'accès à des locaux, des bâtiments, des sites, ou la détention d'un permis, d'une licence ou d'une autorisation pouvait, par un usage inapproprié, porter atteinte à la défense de l'intégrité du territoire national et des plans de défense militaire, à l'accomplissement des missions des forces armées, à la sûreté intérieure de l'État, y compris dans le domaine de l'énergie nucléaire, à la pérennité de l'ordre démocratique et constitutionnel, à la sûreté extérieure de l'État et aux relations internationales de la Belgique, au potentiel scientifique et économique du pays, à la sécurité des ressortissants belges à l'étranger ou au fonctionnement des Organes décisionnels de l'État* ».

54 Loi du 23 février 2018 portant modification de la loi L.C.&HS (*M.B.*, 1er juin 2018, p. 45591) et Arrêté royal du 8 mai 2018 modifiant l'arrêté royal du 24 mars 2000 portant exécution de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (*M.B.*, 1er juin 2018, p. 45632).

55 L'ERM propose, entre autres, une formation de base (FBEM, anciennement appelée 'premier cycle'), une formation pour Candidat Officier supérieur (FCOS) ainsi qu'un Cours supérieur d'État-major (CSEM). Voir : www.rma.ac.be

University of Defense Technology) sont envoyés dans plusieurs pays d'Europe occidentale, dont la Belgique, pour y acquérir des connaissances essentielles à certains développements militaires. Ces étudiants et chercheurs emportent ensuite toutes les connaissances engrangées au sein des universités belges pour les mettre à disposition de l'armée de leur pays. À l'heure actuelle, quelques dizaines de ces étudiants militaires sont actifs dans des universités belges »[56].

Le Comité permanent R a également estimé que la Défense présentait une fragilité dans son accueil des élèves étrangers. Il existe en effet un risque non négligeable d'espionnage et d'ingérence dans le chef de certaines personnes qui, de surcroit, se voient offrir un accès à des informations de la Défense.

Par conséquent, l'admission d'étudiants étrangers nécessite, selon le Comité, une analyse de risque systématique et préalable au cas par cas (autrement dit de chaque candidat-élève) par le SGRS.

I.8. ENQUÊTE DE CONTRÔLE SUR LE SUIVI DES MANDATAIRES POLITIQUES

I.8.1. INTRODUCTION

Lors de débats (parlementaires) [57], une question est posée à maintes reprises, à savoir si et dans quelle mesure les services de renseignement belges suivent (ou sont autorisés à suivre) des mandataires politiques, et quelles règles doivent être observées à cet égard.[58] Depuis début janvier 2018, une note de service classifiée 'CONFIDENTIEL' est d'application au sein de la VSSE. Conformément à cette note, actualisée en juin 2020[59], le service envoie deux types de rapports au ministre de la Justice et au Premier ministre, avec copie au Comité permanent R. Il s'agit, d'une part, de rapports ponctuels sur des mandataires politiques qui contribueraient à l'apparition d'une menace et, d'autre part, d'un aperçu trimestriel de l'ensemble

---

56 https://www.vsse.be/sites/default/files/paragraphs/1-ra2020-fr-version10-single-light.pdf

57 Voir Question de S. Creyelman au ministre de la Justice sur les 'dossiers politiques à la VSSE' (*Q.R.* Chambre 2019-20, 16 juillet 2020, QRVA 23, 33, Q. n° 351).

58 COMITÉ PERMANENT R, *Rapport d'activités 2019*, 71-72 ('IV.3. Contrôle du suivi des mandataires politiques').

59 Cette note de service du 13 décembre 2017 a été actualisée en juin 2020 en vue d'améliorer les rapports destinés à la direction sur les activités disruptives. Malgré ses demandes répétées, le Comité n'a reçu, en 2019, aucune information du SGRS. Le Comité avait pourtant exhorté le SGRS, comme la VSSE d'ailleurs, à adopter une directive uniforme, assortie de règles claires et univoques quant au recueil, au traitement, à la consultation, au stockage et à l'archivage des informations relatives aux mandataires politiques. Le SGRS ne dispose pas d'une procédure spécifique pour traiter cette thématique, pas plus qu'il n'a défini de procédure pour informer le Comité permanent R.

des documents dans lesquels des mandataires politiques sont mentionnés.[60] Le ministre de la Justice avait marqué son accord sur le *« principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991 »*.[61]

Étant donné qu'il n'est mentionné nulle part ce que le Comité permanent R est censé faire des informations précitées, il a pris l'initiative de développer une méthodologie autour de cette problématique et de son rôle de contrôle. Cette méthodologie a été approuvée par la Commission parlementaire de suivi en 2020. Sur la base de cette méthodologie, une enquête de contrôle a été initiée en 2020 et finalisée en 2021.[62] L'enquête se penchait sur la fréquence avec laquelle, pendant la période de référence (du 1er septembre 2019[63] au 31 août 2020), des informations concernant un mandataire ont été recueillies, traitées et ont fait l'objet d'un rapport. Il s'agissait également de vérifier si la collecte d'informations était légale et non disproportionnée et si les recommandations formulées dans le passé par le Comité permanent R ont été exécutées. [64]

À cette fin, le Comité permanent R a établi une liste des (543) personnes ayant occupé, pendant la période de référence, un mandat politique au niveau européen, fédéral, régional et communautaire.[65]

Cette liste a été transmise fin octobre 2020 respectivement à la VSSE et au SGRS. En réponse, la VSSE a remis au Comité permanent R les listes des documents pertinents établis par ses services extérieurs et le service d'analyse. De son côté, le

---

60 Les mandataires politiques visés sont les ministres des différents gouvernements, le Commissaire belge siégeant à la Commission européenne et les membres des différents parlements et assemblées, y compris les membres belges du Parlement européen. Les autres élus ou mandataires désignés ne sont pas concernés (par ex. les échevins au niveau communal ou les gouverneurs au niveau provincial).

61 Voir le courrier du ministre de la Justice daté du 26 juillet 2018 et adressé au Comité permanent R sur 'le recueil d'informations par un service de renseignement concernant une personne exerçant un mandat politique'.

62 Le Comité permanent R a déjà mené des enquêtes sur ce sujet ou des matières connexes. Voir COMITÉ PERMANENT R, *Rapport d'activités 1998*, 60 et suiv. ; *Rapport d'activités 1999*, 13 et suiv. ; *Rapport d'activités 2008*, 20-21 et suiv. ; *Rapport d'activités 2013*, 3 ('I.I.3. Une nouvelle note de service de la VSSE sur le suivi des parlementaires').

63 Début de la législature fédérale parlementaire 55 (2019- 2024).

64 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 37- 47 ('II.4. Le suivi de mandataires politiques par les services de renseignement').

65 Concrètement, il s'agissait : a) des ministres du Gouvernement flamand, du Gouvernement de la Fédération Wallonie-Bruxelles, du Gouvernement de la Région wallonne, du Gouvernement de la communauté germanophone, du Gouvernement bruxellois, du Gouvernement fédéral et des commissaires belges au sein de la Commission européenne ; b) des membres des parlements communautaires et régionaux (Fédération Wallonie-Bruxelles, Région wallonne, Région de Bruxelles-Capitale, Parlement flamand et communauté germanophone), du Parlement fédéral (Chambre et Sénat) et des membres belges du Parlement européen ; et c) à l'exception des présidents de partis politiques qui ne sont pas membres d'un parlement et n'ont pas de mandat exécutif à l'un des niveaux susmentionnés, des membres de la famille royale, des ministres d'État, des mandataires locaux (bourgmestres, échevins, conseillers communaux, membres d'intercommunales) pour autant qu'ils ne revêtent aucun mandat régional/communautaire/fédéral/européen, des gouverneurs et anciens mandataires sans mandat actuel.

SGRS a signalé au Comité que le service n'avait suivi ni examiné aucun mandataire politique belge pendant la période de référence.

I.8.2. CONSTATATIONS CONCERNANT L'EXÉCUTION DES RECOMMANDATIONS FORMULÉES PAR LE COMITÉ PERMANENT R

I.8.2.1. L'élaboration de directives quant au recueil, au traitement, à la consultation, au stockage et à l'archivage des données

En 2008, le Comité permanent R avait recommandé l'élaboration de directives claires et non équivoques quant au recueil, au traitement, à la consultation (y compris le cloisonnement interne éventuel), au stockage et à l'archivage des données de certaines catégories de personnes qui assument ou ont assumé des responsabilités particulières.[66]

En juin 2020, la VSSE a produit une note de service[67] qui définit de nouvelles directives internes et actualise les procédures, en remplacement de trois notes de services antérieures.[68] Cette note prévoit notamment « *l'obligation de notification de la VSSE au ministre de la Justice dès que certains mandataires politiques apparaissent dans les documents de la VSSE* ». Début décembre 2020, la VSSE a en outre envoyé une note aux partis politiques représentés au sein du Parlement fédéral expliquant la procédure suivie lorsque les noms de mandataires politiques apparaissent dans le cadre d'enquêtes de la VSSE.[69]

Malgré les recommandations formulées en 2013[70], le Comité permanent R n'a reçu du SGRS aucune information selon laquelle il prévoyait une procédure

---

66 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 110 et suiv. (VIII.1.2. Des directives pour le traitement de données concernant certaines catégories de personnes.)

67 VSSE, Note de service du 11 juin 2020.

68 La note de service du 4 juillet 2013 ayant pour objet « *Modifications pour l'établissement de documents sauvegardés dans VESTA* », la note de service du 25 juillet 2013 intitulée « *Note de service concernant les liens de parlementaires et mandataires politiques dans les documents de la VSSE* » et la note de service du 13 décembre 2017 concernant « *l'obligation de notification de la VSSE au ministre de la Justice dès que certains mandataires politiques apparaissent dans les documents de la VSSE* ».

69 Procédure mandataires politiques concernant : *'la mention d'un mandataire politique dans la base de données de la VSSE', 'si le mandataire politique est la victime d'une menace', 'l'implication présumée ou avérée d'un mandataire politique dans l'apparition d'une menace'*.

70 COMITÉ PERMANENT R, *Rapport d'activités 2013*, 112 ('IX.1.2. Une directive sur le travail de renseignement à l'égard de personnes exerçant des responsabilités particulières et de partis politiques' et 'IX.1.3. « Directives univoques concernant l'information sur le suivi des responsables politiques').

spécifique pour la gestion de ces informations, et aucune procédure n'a été déterminée pour informer le Comité permanent R.[71]

I.8.2.2. Une attention particulière pour la position des mandataires politiques mentionnés

Une recommandation antérieure du Comité portait sur l'attention nécessaire à accorder à la position, vis-à-vis de la menace (victime, acteur, passant, etc.), des mandataires politiques mentionnés dans les rapports des services de renseignement. Les mandataires politiques peuvent, par exemple, apparaitre dans le radar des services de renseignement via des informations récoltées dans le cadre de l'exercice de leur mandat ou en marge d'une menace : ils peuvent être cités par des sources humaines, apparaître dans des messages de services partenaires, figurer dans des listes créées suite à l'application de ressources techniques (par ex. listes de téléphonie). Dans de tels cas, le mandataire politique entre fortuitement dans le champ de vision des services de renseignement.

Ainsi, la note de service de la VSSE stipule que les mandataires politiques qui apparaissent dans des documents de la VSSE ne peuvent être « reliés » à la menace que s'ils apparaissent comme victimes ou auteurs au sens de la L.R&S.

---

[71] Le 30 novembre 2017, le SGRS signalait au Comité permanent R que depuis les recommandations de 2013, la Loi organique de 1998 avait été modifiée à plusieurs reprises, constatant qu'aucune autorité politique ou législative n'avait admis avoir connaissance du fait que de telles règles devaient être établies concernant le suivi des responsables politiques. Le suivi de responsables politiques par le SGRS n'avait, selon lui, pas porté préjudice à la liberté d'association ou d'expression et, si cela avait été le cas, il y aurait été procédé sur la base de la Loi organique qui est en conformité avec la Déclaration universelle des droits de l'homme et avec les arrêts de la Cour européenne des droits de l'homme, dans le sens où il est prévu que dans certaines situations correctement décrites, il est possible d'aller à l'encontre de l'un ou l'autre droit fondamental. En dépit de cette constatation, le SGRS estimait que toutes les initiatives capables de consolider les contrôles démocratiques sur les services de renseignement devaient être encouragées et que le SGRS pouvait lui aussi jouer un rôle crucial dans cette consolidation. Dans cette optique, le SGRS a pris l'initiative de contacter la VSSE pour réfléchir à la (aux) recommandation(s) prise(s). Le SGRS a également signalé en date du 6 décembre 2017 au Comité permanent R qu'il avait l'intention d'élaborer dans le courant de 2018 des procédures similaires à celles de la VSSE pour informer les organes de contrôle démocratiques, dans le sens où l'élaboration de telles procédures devait également être liée à l'élaboration de procédures internes concernant la sauvegarde et l'archivage d'informations concernant les mandataires et organisations politiques concernés. L'élaboration de ces procédures devait s'inscrire dans le cadre d'un projet plus vaste qui prévoit la rédaction de plusieurs directives internes pour le fonctionnement du personnel(-cadre) du SGRS. L'audit du Comité permanent R sur le fonctionnement de la Direction CI et du SGRS, réalisé en février et mars 2018, et la publication des résultats de cet audit le 15 mai 2018, contrariaient les plans du SGRS pour l'élaboration desdites procédures. Le SGRS a cependant estimé qu'il était judicieux d'attendre les conclusions du Business Process Re-engineering (BPR), le processus de réforme interne du SGRS mis en place à l'issue de l'audit du Comité permanent R. Le 6 janvier 2020, le SGRS mettait en place sa nouvelle structure.

Il ressort toutefois de l'examen des documents visés que le rôle joué (victime, acteur, passant, etc.) par les mandataires politiques mentionnés n'était pas décrit de manière suffisamment claire.

I.8.2.3. L'exécution de l'article 19 L.R&S.[72]

La note de service susmentionnée précise qu'un aperçu de tous les documents dans lesquels figurent des mandataires politiques est transmis tous les trois mois par la VSSE au Comité permanent R (voir *infra*). L'aperçu reprend les références des documents qui contiennent des informations brutes ainsi que les références des documents d'analyse. L'aperçu indique également quelles notes ont été transmises au ministre de la Justice et au Premier ministre.[73]

En ce qui concerne le SGRS, le Comité permanent R recommande au service de lui remettre tous les trois mois un aperçu de tous les documents dans lesquels des mandataires politiques sont mentionnés.

I.8.3. LA COLLECTE, L'ANALYSE ET LA DIFFUSION DES RENSEIGNEMENTS SUR LES MANDATAIRES POLITIQUES ENTRE 2019 ET 2020

I.8.3.1. Collecte et analyse

Pendant la période de référence, sur les 543 mandataires politiques :
- 49 % (267) n'étaient pas repris dans la base de données de la VSSE ;
- 23 % (124) étaient repris dans la base de données de la VSSE, mais sans lien avec une menace ;
- 28 % (152) étaient repris dans la base de données de la VSSE, avec mention dans des documents d'analyse (828) produits par la VSSE à propos d'une menace.

Sur ces 828 documents d'analyse, 53 % (439) sont des rapports d'enquête, 25 % (206) des documents transmis par un partenaire (inter)national externe, 6 % (53)

---

72 « Art. 19 L.R&S : *Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11.*
Dans le respect de la vie privée des personnes, et pour autant que l'information du public ou l'intérêt général l'exige, l'administrateur général de la Sûreté de l'État et le chef du Service général du renseignement et de la sécurité, ou la personne qu'ils désignent chacun, peuvent communiquer des informations à la presse. »

73 Le ministre de la Justice et le Premier ministre ne sont pas informés d'une mention purement accidentelle de mandataires politiques dans des documents de la VSSE.

des notes aux autorités belges et 16 % (130) des documents divers (essentiellement des procès-verbaux de réunions et des fiches de synthèse élaborées dans le cadre de l'analyse interne d'un dossier).

I.8.3.2. Diffusion des renseignements

La VSSE remet chaque trimestre au Premier ministre et au ministre de la Justice, avec copie au Comité permanent R, un aperçu de tous les documents dans lesquels apparaissent des mandataires politiques.

En outre, dès que, sur la base des informations disponibles, il y a une présomption d'implication d'un mandataire politique dans l'apparition d'une menace, le ministre de la Justice et le Premier ministre, avec notification au Comité permanent R, en sont informés via des fiches de notification. Ces fiches sont éventuellement complétées par le détail des informations analysées et vérifiées qui justifient la notification des autorités. Pendant la période de référence, cinq fiches de notification de ce genre ont été établies pour autant de mandataires.

La VSSE partage en outre les informations à propos des mandataires politiques dont le nom apparait dans certains documents sans toutefois pouvoir être reliés à une menace. Dans des notes aux autorités, la VSSE fournit ainsi une description de la manière dont le mandataire politique contribue à l'apparition d'une menace, une évaluation des possibles conséquences que peut ou a pu avoir cette implication (pour autant qu'elles soient connues) et la manière dont le dossier sera traité.

Pendant la période de référence, 17 des 543 mandataires politiques (3,13 %) ont fait l'objet de 53 notes aux autorités (21 concernant l'extrémisme, 25 pour espionnage et ingérence, 7 autres tels que organisations criminelles ou corruption).[74]

I.8.4. LE RESPECT DES DROITS FONDAMENTAUX DES MANDATAIRES POLITIQUES

La légalité du recueil des informations repose sur la(es) mission(s) des services de renseignement telle(s) que précisée(s) à l'article 7 L.R&S.

Le Comité permanent R n'a trouvé aucune indication selon laquelle la VSSE visait des mandataires politiques pour des raisons étrangères aux intérêts et menaces énumérés dans la loi, ni qu'ils étaient traités différemment des autres groupes professionnels.

---

[74] L'examen des 53 notes aux autorités belges (NA) susmentionnées indique qu'elles étaient également adressées à l'une ou plusieurs des personnes/institutions suivantes selon le principe du '*need to know*' : Comité permanent R (28), OCAM (13), Police fédérale (13), SGRS (12), ministre de la Justice (9), Parquet fédéral (9), Direction générale du centre de crise (6), Procureur du Roi (5), Premier ministre (5), autres (24 – par exemple, Direction générale des Établissements pénitentiaires, Cellule de traitement des informations financières, SPF Intérieur ou Police locale).

De l'examen des notes aux autorités, il ne ressort pas que les droits fondamentaux des mandataires politiques n'ont pas été respectés dans le recueil, l'analyse et la diffusion d'informations.

Sur la base des critères repris dans la méthodologie approuvée par la Commission de suivi, il ne ressort pas de l'enquête que des mandataires politiques apparaissent de manière disproportionnée dans les documents de la VSSE.

I.9. ENQUÊTE SUR LA DÉTECTION ET LE SUIVI DE LA RADICALISATION D'UN MILITAIRE DE LA DÉFENSE : L'AFFAIRE JÜRGEN CONINGS

En mai 2021, Jürgen Conings, fiché comme 'extrémiste potentiellement violent' (EPV)[75] par l'OCAM, a quitté la caserne de Bourg-Léopold et a pris la fuite en emportant des armes. Au moment de sa disparition, l'intéressé était employé comme Caporal-chef à la Défense. Il est apparu rapidement que l'intéressé était connu des services de police et des services de renseignement et de sécurité (voir *infra*). L'affaire a ému l'opinion publique et a soulevé, à juste titre, de très nombreuses questions (parlementaires).[76]

Sur demande de la ministre de la Défense, le Comité permanent R a ouvert une *'enquête de contrôle concernant, d'une part la détection et le suivi de la radicalisation d'un militaire de la Défense par les deux services de renseignement, et d'autre part, leur collaboration portant notamment sur l'échange d'informations avec leurs partenaires, y compris avec la Défense'*. À travers cette enquête, la ministre de la Défense a assigné trois missions au Comité : (a) vérifier la fiabilité des informations relatives aux personnes suspectées de radicalisation au sein de la Défense, (b) coopérer avec l'inspecteur général de la Défense chargé de réaliser un audit portant notamment sur les aspects de la gestion du personnel et (c) formuler des recommandations en vue de garantir le bon fonctionnement du SGRS, mais aussi de la Défense dans son ensemble.

En ce qui concerne le rôle de l'OCAM dans cette affaire, une '*enquête de contrôle commune sur le rôle de l'OCAM et ses services d'appui, dans le suivi de Jürgen Conings, notamment dans sa mise en « pré-enquête », de son évaluation au*

---

75 Les EPV sont l'une des catégories de la banque de données commune *Terrorist Fighters* dont l'OCAM est le gestionnaire opérationnel. Les entités inscrites comme EPV doivent remplir une série de critères définis dans l'A.R. du 20 décembre 2019 modifiant l'A.R. du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters et l'A.R. du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er*bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police, *M.B.* 27 janvier 2020. Voir COMITÉ PERMANENT R, *Rapport d'activités 2020*, 128 ('VI.1.1. L'ajout des extrémistes potentiellement violents (EPV) dans la BDC TF').

76 Voir, par exemple, le Débat d'actualité sur le militaire en fuite (Commission de la Défense nationale), *C.R.I.* Chambre 2020-21, 26 mai 2021, COM 490 et les débats autour du rapport de l'Inspecteur général, *C.R.I.* Chambre, 2020-2021, 16 juin 2021, COM 519.

niveau 3 de la menace et de ses conséquences, et sur l'échange d'informations relatif à cette personne' a été initiée conjointement avec le Comité permanent P.[77]

Les rapports d'enquête ont été discutés début juillet 2021 avec la Commission parlementaire de suivi.

I.9.1. UN APERÇU DU PARCOURS PROFESSIONNEL DE JÜRGEN CONINGS

Le parcours professionnel de Jürgen Conings est fait d'un enchevêtrement d'affectations, de mutations, de missions à l'étranger[78], de formations en tous genres[79] au sein de la Défense ainsi que de petits boulots dans le secteur de la sécurité privée. Démarrée en 1992, la carrière du militaire est ainsi ponctuée par plusieurs changements d'affectation jusqu'à sa mutation, à sa demande, en juin 2020 au sein de la Cellule *Pre-Deployment Training for Individual Augmentees* (PDT-IA[80]) en tant que collaborateur logistique, réparateur d'armes et instructeur auxiliaire.

S'il apparait dans les radars de la Sûreté de l'État pour la première fois en 2015, l'intéressé obtient toujours de 'bonnes' évaluations au sein de la Défense, et ce malgré une sanction (un arrêt simple de quatre jours) pour propos racistes tenus sur Facebook en novembre 2019. [81] Le rapport de l'Inspection générale de la Défense fait également mention de facteurs psychosociaux.[82]

En mars 2020, il postule à la Police fédérale pour une fonction d'agent de sécurité mais sera recalé sur la base de son test de personnalité. En parallèle de ses affectations au sein de la Défense, il continue néanmoins son parcours dans le secteur de la sécurité privée en tant qu'agent de gardiennage.

Le 31 août 2020, son habilitation de sécurité n'est pas prolongée. Le même jour, il est inscrit par l'OCAM en pré-enquête EPV. Le 17 février 2021, il se voit

---

77 Voir 'I.10 Enquête commune de contrôle sur le rôle de l'OCAM dans le suivi du militaire Jürgen Conings'. Dans un souci d'exhaustivité, ces deux rapports d'enquête doivent être lus conjointement.

78 Entre autres, en ex-Yougoslavie (BELBAT), en Afghanistan (Resolute Support Mission) et en Jordanie (Operation Desert Falcon).

79 Entre autres, des formations au matériel roulant, des formations techniques (gestion d'entrepôt, réparation de radios, etc.) et des cours d'armement.

80 Cette cellule de la Composante Terre est responsable de la préparation des militaires de l'ensemble de la Défense qui, en tant qu'individu, participeront à des opérations (par exemple, les militaires impliqués dans certaines missions, indépendamment d'un grand détachement lié à leur propre unité, voire à leur composante).

81 Le motif avancé est le suivant : *"Betrokkene heeft op sociale media een mening geuit die niet strookt met de waarden van Defensie en schade toebrengt aan het imago van Defensie"*. L'intéressé a exprimé dans les médias sociaux une opinion qui n'est pas conforme aux valeurs de la Défense et qui porte atteinte à son image (traduction libre).

82 Inspectoraat-generaal, Eindrapport E2103. Intern onderzoek PDT-IA, Beperkte verspreiding.

attribuer le *full* statut d'EPV niveau 3[83] (art. 6, § 1er, 1°/2 AR TF). Le 3 mars 2021, sa promotion sociale est annulée. Le 17 mai 2021, il quitte la caserne en possession d'armes avant que sa disparition soit signalée le lendemain. Le 21 mai 2021, un juge d'instruction a été désigné pour 'tentative d'assassinat dans un contexte terroriste' et 'possession illégale d'armes dans un contexte terroriste'. Une procédure de suppression d'emploi a été lancée. Le 20 juin 2021, soit cinq semaines après sa disparition, il a été retrouvé sans vie.

Jürgen Conings faisait ainsi partie des quelque 30[84] militaires suivis par le service de renseignement militaire pour leur proximité avec les milieux d'extrême droite.[85] À sa disparition, il a d'ailleurs reçu le soutien de Tomas Boutens, ancien militaire et leader du groupe néo-nazi *Bloed, Bodem, Eer & Trouw*.[86] Sur un de ses profils Facebook, Jürgen Conings avait fait référence au 'Siegrune', un symbole runique utilisé dans l'Allemagne nazie. Plus encore que les contacts sporadiques avec Boutens, il avait été remarqué dans les milieux de la *Vlaams Legioen*[87], où il aurait donné un entraînement au combat. Jürgen Conings faisait également partie du groupe Facebook des *Knights of Flanders*, un groupe d'extrême droite.

I.9.2. CADRE JURIDIQUE ET POLITIQUE

Avant d'évaluer la position d'information des services de renseignement concernant Jürgen Conings, il importait de clarifier les compétences de la VSSE et du SGRS dans le cadre de la détection, du suivi et de la lutte contre le terrorisme, l'extrémisme et le radicalisme.

---

83 Conformément à l'article 11 de l'A.R. du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace, l'OCAM travaille à partir d'une échelle de quatre niveaux de la menace (du niveau 1 'faible' au niveau 4 'très grave'). Le niveau 3 rend compte d'une menace 'grave'.

84 À titre de comparaison, les services de police suivent environ 2500 personnes dans les milieux d'extrême droite.

85 L'influence exercée par l'extrême droite dans les rangs militaires n'est pas un phénomène uniquement belge, pas plus qu'il n'est nouveau. Au sein de l'unité d'élite allemande *Kommando Spezialkräft* (KSK), cinquante militaires sont suspectés depuis 2017 de mener des activités d'extrême droite. Récemment, un coup d'État mené par un ancien général issu des cercles de la droite (extrême) a suscité des craintes. Aux Pays-Bas aussi, plusieurs militaires ont quitté les forces armées ces cinq dernières années après avoir tenu des propos ou adopté un comportement d'extrême droite. Fin des années 90, l'ancien ministre de la Défense avait déjà prévenu qu'un bataillon de paras près d'Anvers ne devait pas être affecté par des tendances fascistes et racistes.

86 Condamné à cinq ans de prison pour avoir planifié, avec seize autres personnes appartenant pour la plupart à l'Armée belge des actes terroristes et diffusé une idéologie faisant l'apologie de la violence (deux tiers des individus arrêtés à l'époque étaient des militaires de carrière), Tomas Boutens a été l'un des premiers à avoir affiché son soutien au fugitif sur Facebook.

87 Un groupuscule d'extrême droite qui 'lutte pour le peuple flamand et pour la Flandre'.

I.9.2.1. Les missions de renseignement de la VSSE et du SGRS

L'assignation des tâches de la VSSE dans la lutte contre le terrorisme, l'extrémisme et le radicalisme se situe à titre principal dans le cadre de sa mission de renseignement (art. 7, 1° L.R&S). Le législateur a choisi d'établir une liste limitative des menaces contre la sécurité qui relèvent du domaine de compétence de la VSSE. L'article 8, 1°, alinéas 2, b et c L.R&S définit les menaces visées par l'enquête de contrôle, à savoir le terrorisme et l'extrémisme (en ce compris le processus de radicalisation).

Les activités du SGRS en matière de terrorisme, d'extrémisme et de radicalisme se situent elles aussi à titre principal dans le cadre de sa mission de renseignement telle que définie à l'article 11, § 1er, 1° L.R&S. À l'instar de la VSSE, le SGRS doit sauvegarder certains intérêts fondamentaux du pays au moyen de la détection, du suivi et de la lutte contre certaines menaces pesant sur ces intérêts. La principale différence réside dans la présence requise d'un aspect militaire, soit dans l'intérêt à protéger (par ex. les plans de défense militaires, l'exercice des missions militaires), soit la manière dont les intérêts à protéger peuvent être affectés, c'est-à-dire par des moyens de nature militaire (par ex. des armes militaires, du personnel de la Défense).

Les renseignements obtenus par les deux services, c'est-à-dire les informations collectées et analysées, sont ensuite tranmises à d'autres instances, en temps utile et de manière ciblée.[88] Ces instances (principalement politiques, administratives, judiciaires, policières, diplomatiques et militaires) prennent *in fine* les contre-mesures nécessaires pour protéger la sécurité nationale.

Cette vaste mission légale de renseignement impose aux services et à leurs responsables politiques de définir des priorités dans le cadre de leurs activités. En effet, la VSSE et le SGRS ne disposent pas des capacités et des moyens suffisants pour détecter, suivre et maîtriser (ni n'auraient jamais pu) toutes les menaces nationales en matière de sécurité relevant de leur compétence. Cette mission de priorisation incombe au Conseil national de sécurité (CNS).[89]

Le CNS est également chargé de définir les modalités de coopération effective entre les différents services de sécurité. A cette fin, le Plan Stratégique National du Renseignement (PSNR), établi conjointement par la VSSE et le SGRS et validé par le CNS en 2018, *'entend'*, entre autres, *'optimiser la coopération entre les services*

---

88 En vertu de l'article 19 L.R&S, les destinataires des renseignements sont les '(…) *ministres et autorités administratives et judiciaires concernés, (…) services de police et (…) toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi que (…) instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11*'. Les destinataires des informations des services de renseignement sont donc certaines instances publiques politiques, administratives, judiciaires, policières, diplomatiques et militaires. Des informations utiles peuvent également être portées à la connaissance de personnes ou d'instances menacées (par ex. un employeur).

89 Tel que confirmé à la lecture des articles 4 et 10 L.R&S et de l'article 2 de l'A.R. du 22 décembre 2020 portant création du Conseil national de sécurité, du Comité stratégique du renseignement et de la sécurité et du Comité de coordination du renseignement et de la sécurité, *M.B.* 29 décembre 2020.

de renseignement afin de mettre en oeuvre une politique de renseignement la plus efficiente possible en faveur des autorités compétentes et de la population.'.[90] Dans la section (classifiée) « Répartition des tâches », le PSNR détaille les compétences respectives de la VSSE et du SGRS en matière de lutte contre le terrorisme, l'extrémisme et le radicalisme.

I.9.2.2. La réalisation de screenings de sécurité par les deux services de renseignement

Outre leurs missions de renseignement, la VSSE et le SGRS ont également des missions de sécurité, au premier rang desquelles il convient de citer la réalisation de screenings de sécurité.
Les deux services mènent en effet des enquêtes de sécurité, c'est-à-dire les enquêtes effectuées au service d'une autorité de sécurité (principalement l'ANS) afin de vérifier si une personne satisfait aux conditions en matière de secret, loyauté et intégrité. Ces conditions sont nécessaires pour obtenir ou conserver une habilitation de sécurité.[91] Les services de renseignement sont en outre chargés de réaliser les vérifications de sécurité en vue de l'octroi d'une attestation ou d'un avis de sécurité.
Au sein des Forces armées, le SGRS remplit également la fonction d'autorité de sécurité. Ceci signifie qu'il est aussi chargé, en plus de la réalisation des enquêtes et des vérifications de sécurité, de l'octroi des habilitations et des avis de sécurité. Le Comité constate toutefois qu'au sein des Forces armées, il n'existe aucune instruction générale énumérant de manière exhaustive les fonctions à la Défense qui requièrent une habilitation de sécurité.
En vertu de la Loi du 28 février 2007 fixant le statut des militaires du cadre actif des Forces armées, un avis de sécurité positif est par contre exigé pour tout candidat-militaire (cf. art. 9, 9°). La loi n'impose cependant pas de screening de sécurité périodique pour les militaires.[92]

---

90 Plan Stratégique National du Renseignement, 4.

91 Les enquêtes de sécurité sont effectuées conformément aux directives (datées et peu adaptées) du 16 février 2000 du Comité ministériel du renseignement et de la sécurité (devenu le Conseil national de sécurité). Le Comité rappelle l'urgence d'actualiser les directives du Comité ministériel du renseignement et de la sécurité portant sur toutes sortes de règles de sécurité (portée des enquêtes de sécurité, règles de classification, conservation des pièces classifiées, infosec, missions des officiers de sécurité). Les directives en question remontent toutes à 2001 et nécessitent une adaptation.

92 Voir 'I.7. Les screenings de sécurité des militaires et et des civils à la Défense'.

I.9.2.3. La responsabilité du SGRS en matière de sécurité militaire[93]

Outre la réalisation d'enquêtes et de vérifications de sécurité, le SGRS est également chargé *'de veiller au maintien de la sécurité militaire du personnel relevant du Ministre de la Défense nationale, et des installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires'* (art. 11, § 1er, 2° L.R&S). La notion de sécurité militaire englobe donc, en plus de la sécurité des renseignements, *'la sécurité des personnes, du matériel et des installations'*.[94]

Ainsi, plusieurs directives ont été établies et diffusées par le SGRS en la matière et réglementent, par exemple, le stockage des armes et des munitions (les règlements IF5 et IF5(bis)).[95] Les compétences du SGRS consistent ici à conseiller le commandement militaire sur les mesures de protections adéquates, à vérifier leur mise en œuvre, à constater les éventuelles lacunes, à informer le commandement militaire précité des défaillances constatées et à formuler les recommandations requises pour y remédier.

I.9.3. LES CONSTATATIONS DE L'ENQUÊTE

L'affaire Conings illustre les constatations du Comité permanent R au fil des enquêtes de contrôle qu'il a effectuées ces dernières années. Cette affaire apparait comme étant le point d'intersection de toutes les constatations antérieures, en particulier en ce qui concerne le service de renseignement militaire. Les recommandations qui y sont associées conservent elles aussi toute leur valeur d'actualité,[96] tout

---

93 Le Comité rappelle qu'en 1999 et 2003 déjà – chaque fois à la suite d'un vol conséquent d'armes et/ou de munitions sur un site militaire – il avait fait état d'une enquête de contrôle ouverte en rapport avec ces incidents. Ces enquêtes étaient relatives respectivement à *'l'efficacité du SGR et à la collaboration des deux services de renseignement concernant le vol d'armes commis à Houthulst en 1997'* (COMITÉ PERMANENT R, *Rapport d'activités* 1999, 74 et suiv.) et à *'la sécurité et à la surveillance d'un dépôt militaire d'armes (Thuin)'* (COMITÉ PERMANENT R, *Rapport d'activités 2003*, 192 et suiv.).

94 Projet de loi organique des services de renseignement et de sécurité, *Doc. parl.*, Chambre 1995-1996, n°49-638/001, 11-12.

95 Le SGRS a informé le Comité permanent R à plusieurs reprises ces dernières années que le Règlement IF5(bis) serait actualisé. La version la plus récente du Règlement qui a été transmise au Comité est celle de 2016. Le Comité n'a pas connaissance d'une version plus actuelle.

96 Voir par exemple COMITÉ PERMANENT R, *Rapport d'activités 2020*, 38-53 ('Le suivi de l'extrême droite par les services de renseignement belges' ; *Rapport d'activités 2019,* 2-13 ('La réalisation de screenings de sécurité par les services de renseignement') ; *Rapport d'activités 2016,* 70-73 ('Évaluations individuelles de la menace par l'OCAM') ; *Rapport d'activités 2011,* 7-14 ('Un audit au sein du service de renseignement militaire') et 25-33 ('Les flux d'informations entre l'OCAM et ses services d'appui').

comme celles qui ont été formulées par la Commission d'enquête parlementaire 'Attentats'.[97]

I.9.3.1. La position d'information de la VSSE

Jürgen Conings est entré pour la première fois dans les radars de la Sûreté de l'État en septembre 2015 dans le cadre d'une récolte de fonds sur Facebook pour Dwekh Nawsha, une organisation paramilitaire chrétienne créée en soutien à la communauté assyrienne en Irak contre l'État islamique.[98] Il a attiré une seconde fois l'attention de la VSSE en octobre 2018.

Dans les deux documents de 2015 et 2018, il est mentionné que l'intéressé est un militaire. Le Comité permanent R a constaté que la VSSE n'avait pas partagé l'information de 2015 avec le SGRS, ne la considérant pas assez pertinente. L'information de 2018 a été communiquée au SGRS lors d'une réunion du Groupe de travail Extrême droite (Plan d'action Radicalisme ou Plan R)[99], au cours de laquelle les noms de l'organisation et des principaux protagonistes ont été mentionnés en termes généraux. Cette information a été communiquée à l'OCAM en 2020.

Entre juillet 2020 et mai 2021, la VSSE a rédigé plusieurs rapports d'information, dans lesquels étaient mentionnés la participation de Conings à des activités des groupements d'extrême droite *Knights of Flanders* et *Vlaams Legioen*. La VSSE a en outre constaté que Conings était en contact avec Tomas Boutens, l'ancien militaire et leader du groupuscule néo-nazi *Bloed, Bodem, Eer en Trouw* condamné en 2014 pour des faits de terrorisme.

Fin juin 2020, la VSSE a transmis une note à l'OCAM, au Parquet fédéral et au SGRS, entre autres, dans laquelle elle faisait mention d'un profil Facebook extrémiste de Conings et des menaces proférées par ce dernier à l'encontre du virologue Marc Van Ranst. En août 2020, la VSSE pose une série de questions spécifiques au SGRS. Pour autant que le Comité permanent R a pu le vérifier, le SGRS n'a jamais répondu officiellement à ces questions de la VSSE.

I.9.3.2. La position d'information du SGRS

Dès juillet 2020, peu après que des informations policières ont relié Conings aux possibles menaces à l'encontre de Marc Van Ranst, il a été signalé au sein du SGRS que l'intéressé devait retenir davantage l'attention. Le SGRS n'a pas communiqué ces informations à l'OCAM à ce moment-là, bien qu'une pré-enquête était en

97 *Doc. parl.*, Chambre, 2016-17, 54-1752/008 (15 juin 2017).

98 Selon des sources ouvertes, des *foreign fighters*, provenant, entre autres, des États-Unis, de France, du Royaume-Uni et d'Australie auraient rallié Dwekh Nawsha.

99 Devenu Stratégie Extrémisme et Terrorisme' (Stratégie TER) en septembre 2021.

cours concernant Conings dans le cadre de sa potentielle inscription comme EPV dans la BDC TF.

En février 2021, le SGRS valide une opération de renseignement avec Conings parmi les cibles, c'est-à-dire la mise en œuvre de méthodes de recueil de données (MRD). L'enquête du Comité permanent R a cependant montré qu'aucune MRD n'avait été mise en oeuvre jusqu'au 17 mai 2021. Le SGRS explique ce retard par une charge de travail élevée et l'absence de collaborateurs responsables de la gestion des MRD.[100]

L'intervention de la VSSE n'a pas été sollicitée en la matière, vu qu'il s'agissait d'un militaire.

Au cours des entretiens menés par le Comité, il est également apparu que les collaborateurs du SGRS ne sont pas, ou à peine, familiarisés avec l'utilisation et la finalité de la BDC TF.[101]

En outre, malgré la cinquantaine de collaborateurs du SGRS ayant un accès direct à la BDC TF, une trentaine de loggings enregistrés entre novembre 2020 et avril 2021 ont été effectués par seulement quelques collaborateurs.[102] Concernant Jürgen Conings plus spécifiquement, la fiche de renseignements de l'intéressé a été consultée le 15 janvier et le 19 février 2021 (le 17 février, il est passé en niveau 3). L'opération susmentionnée validée en février 2021 concernant Conings n'est toutefois pas liée à son évaluation au niveau 3 de la menace par l'OCAM.

L'enquête montre que l'existence du Plan R et de la BDC TF ne sont pas pris en considération au sein du SGRS. Il ressort de l'examen du dossier que ni la pré-enquête EPV, ni l'inscription comme EPV dans le BDC TF, ni l'évaluation au niveau de menace à 3 par l'OCAM n'ont eu d'impact sur le suivi de l'intéressé par le service de renseignement militaire.

Le SGRS a également manqué à ses obligations vis-à-vis du fonctionnement de la LTF.[103] Après la mise en pré-enquête de l'intéressé dans la BDC, le SGRS n'a fourni aucune information complémentaire et n'a pas joué son rôle d'initiateur

---

100 Lorsque des collaborateurs sont absents ou empêchés, leur remplacement n'est pas automatiquement prévu. Ainsi, il pouvait arriver que l'opération autour de Conings accuse un retard en raison, entre autres, d'une absence pour maladie du *case manager* qui devait gérer l'opération, et que personne au SGRS n'était présent à une réunion cruciale de la LTF compétente le 24 février 2021 au cours de laquelle ont été communiquées l'inscription de Conings comme EPV dans la BDC TF et l'attibution du niveau 3 de la menace par l'OCAM.

101 Ils ne sont pas au courant de la signification et des conséquences de l'inscription d'une entité dans une des catégories de la BDC TF et du niveau de menace attribué à une telle entité. Pour eux, l'inscription d'une entité ne change rien au suivi de celle-ci au niveau du travail de renseignement.

102 Il ressort néamoins des entretiens que personne de l'analyse, de la collecte ni de la hiérarchie n'était au courant que Jürgen Conings était repris dans la BDC TF, donc pas non plus du fait qu'à la fin février 2021, Jürgen Conings était fiché comme EPV avec une mention du niveau 3.

103 Autre problème : les réunions de la LTF compétente au début de la pandémie de COVID 19 ont été suspendues pendant un certain temps (mars et avril 2020) et se sont tenues par la suite en mode 'hybride' (certains services étaient physiquement présents aux réunions, tandis que d'autres services participaient par vidéoconférence). Compte tenu de la communication non sécurisée via les vidéoconférences, aucune information classifiée ne peut être échangée entre les participants.

(pourtant attendu compte tenu de la qualité de militaire de l'intéressé) dans un débat sur d'éventuelles mesures à prendre. À la réunion du 24 février 2021 de la LTF compétente, lors de laquelle l'inscription de Conings dans la BDC TF et le niveau 3 ont été communiqués, le SGRS n'était pas réprésenté.

I.9.3.3. Un manque de communication

Outre certains dysfonctionnements dans la communication avec la VSSE[104] et l'OCAM[105] abordés dans le rapport d'enquête, l'affaire Jürgen Conings a mis en lumière la persistance de problèmes de communication au sein même du SGRS. Ces défis en matière de communication interne avaient déjà été identifiés lors d'enquêtes de contrôle antérieures ainsi que par la Commission d'enquête parlementaire 'Attentats'. Ils avaient fait l'objet de recommandations.

La nouvelle structure du SGRS, élaborée en janvier 2020 en réponse à ces recommandations, n'a pas (encore) permis de résoudre les problèmes du passé. L'enquête a montré que les collaborateurs des échelons hiérarchiques inférieurs du SGRS perçoivent la structure actuelle du service comme complexe et peu claire. Le flou règne en ce qui concerne les compétences et la chaine de communication.

En outre, le Comité a pu observer qu'au sein de la plateforme PF6, en charge du suivi de l'extrême droite, des problèmes parmi les membres du personnel étaient survenus entre juillet 2020, alors que Jürgen Conings fait l'objet d'une attention particulière en raison des menaces qu'il a proférées à l'encontre du virologue Marc Van Ranst, et février 2021, au moment où l'intéressé a été repris dans la BDC TF.

Il y a également beaucoup d'incertitudes autour du fonctionnement précis du *Defence Intelligence & Security Command and Control* (DISCC), responsable de la direction opérationnelle du travail de renseignement et qui est placé sous les ordres du Chef du SGRS. Une autre section importante du DISCC est le *Collection Coordination Intelligence Requirements Management* (CCIRM), qui joue un rôle crucial dans la coordination et le traitement de toutes les informations entrantes (*Requests for Information* (RFI), rapports HUMINT) et sortantes (*Requests for Collect* (RFC), notes aux autorités).

---

104 En 2018, la VSSE a communiqué les informations dont elle disposait sur Jürgen Conings lors d'une réunion du Groupe de travail Extrême droite (Plan R). Le SGRS n'a pas non plus répondu formellement à une note du 8 janvier 2021, dans laquelle la VSSE faisait part de ses préoccupations concernant Jürgen Conings. Le SGRS aurait toutefois évoqué la question lors d'une réunion bilérale qui a eu lieu le 15 janvier 2021.

105 Voir à ce propos *in extenso* le rapport commun des Comités permanents R et P ('I.10 Enquête commune de contrôle sur le rôle de l'OCAM dans le suivi du militaire Jürgen Conings'). Les collaborateurs du SGRS soulignent que le niveau 3 de la menace n'a pas été transmis au SGRS dans une évaluation de la menace distincte de l'OCAM. L'OCAM fait cependant remarquer que les évaluations de la menace portant sur des personnes mentionnées dans la BDC TF ne peuvent être consultées que via ce canal.

Plusieurs collaborateurs expriment leurs doutes sur la connaissance du fonctionnement du service et de l'expérience en matière de travail de renseignement des collaborateurs qui font partie du DISCC (plus particulièrement le CCIRM). Ce manque de connaissances et d'expérience expliquerait l'orientation souvent lente et erronée des informations. Les doutes que nourrissent certains collaborateurs sur son bon fonctionnement font que les informations circulent en dehors du DISCC, d'où l'apparition de flux d'informations parallèles.

Dans ce dossier, les collaborateurs de la plateforme d'analyse PF6 ont expliqué qu'une note importante de la VSSE de janvier 2021, dans laquelle ce service se dit préoccupé par Jürgen Conings et pose une série de questions au SGRS, n'est jamais parvenue à la PF6, et est dès lors restée sans réponse. Selon la PF6, le DISCC n'a pas introduit la note en question dans le système *Request for Information Management*, normalement utilisé pour les questions entrantes des services externes.

Au sein du DISCC, les membres du *Steering Comittee*, censés prendre des décisions opérationnelles, ne sont pas suffisamment informés du contenu des dossiers. Ces décisions sont en outre rarement consignées officiellement, ce qui génère de la confusion.

Une troisième section essentielle du DISCC est constituée par ce que l'on appelle les *Case Managers* (CaMa) et les *Collection Managers* (CoMa), chargés de traduire les besoins en informations des plateformes d'analyse dans la mise en oeuvre de moyens de collecte, lorsqu'il faut recourir aux méthodes particulières de renseignement/méthodes de recueil de données (MRD). Toutefois, les CaMa et CoMa ne relèvent pas des mêmes structures (Directions) que les plateformes d'analyse et les services de collecte. Ces Directions ont quant à elles leur propre structure et leur propre hiérarchie, ce qui donne lieu à des controverses sur les compétences et les priorités. Par exemple, dans la structure actuelle, le chef de la section C6/Investigations (qui fait partie de la Direction Collecte) n'est pas compétent pour décider de l'affectation de ses collaborateurs.

L'enquête a également démontré la trop faible valorisation des détachements provinciaux[106], impliqués dans les LTF et en contact avec les commandants de corps et les officiers de sécurité des unités. Le Comité constate que cette 'proximité' est trop peu utilisée par les services centraux d'Evere. Plus précisément, les détachements provinciaux sont trop peu guidés.[107]

En outre, il est apparu qu'il y a peu de concertation entre les détachements provinciaux et le quartier général, ce qui fait que les collaborateurs dans les détachements provinciaux se sentent quelque peu abandonnés à leur sort et doivent

---

106 Les détachements provinciaux constituent une sorte d'antenne du SGRS dans chacune des provinces et sont donc plus proches des unités militaires que des services centraux à Evere. Leur position leur permet donc de détecter rapidement certains développements ou de suivre de près certaines affaires/événements. Mais ils sont aussi souvent les mieux placés pour répondre aux questions des service centraux, étant donné qu'ils ont des contacts sur place et connaissent l'environnement.

107 Le Comité permanent R avait déjà attiré l'attention sur ce point-là aussi à plusieurs reprises.

établir eux-mêmes leurs priorités. Il n'y a ainsi eu aucune concertation à propos de l'inscription de Conings dans la BDC TF entre la plateforme d'analyse compétente et le collaborateur du détachement provincial du Limbourg, qui représentait le SGRS à la LTF compétente.

C'est le détachement du Limbourg qui, en novembre 2019, a fait mention de Jürgen Conings pour la première fois, notamment son implication dans le groupement d'extrême droite *Belgian Commandery of Knights Templar*. Ensuite, jusque fin juin 2020, moment où le détachement provincial informe à nouveau les services centraux qu'il a été contacté par la Police fédérale et le parquet parce que l'intéressé recherchait l'adresse de Marc Van Ranst via Facebook, il n'y a eu pas eu d'autres communications entre les services centraux à Evere et le détachement provincial. Il n'a pas été demandé au détachement de recueillir des informations supplémentaires.

I.9.3.4. La 'watchlist' extrême droite

La ministre de la Défense a demandé au Comité permanent R d'évaluer la 'fiabilité' de la 'watchlist' établie par le SGRS. Dans le cadre de son enquête, le Comité a pu constater que la 'watchlist' constituait un processus interne au SGRS. Retravaillée à la suite de précédentes recommandations du Comité permanent R[108], une nouvelle 'watchlist' a été réalisée en avril 2021 et rassemble les fiches individuelles relatives aux personnes apparaissant dans le suivi de la menace extrême droite par le SGRS.

Ce processus a pour finalité de déterminer, sur la base d'une réévaluation périodique, les niveaux des menaces individuelles relevant de l'extrême droite et le suivi qu'il convient d'y donner (collecte additionnelle d'informations, échange d'informations avec d'autres services, identification de mesures curatives, retrait de la personne concernée de la 'watchlist' lorsqu'il s'avère qu'elle ne constitue pas/plus une menace, etc.).

Par conséquent, la 'watchlist' ne constitue pas un recueil exhaustif des données au sujet des personnes apparaissant dans le périmètre de la menace liée à l'extrémisme de droite et relevant de la compétence du SGRS. Elle doit être combinée avec d'autres informations. Aussi, en tant que processus interne, elle n'a pas vocation à être communiquée comme telle à des tiers au SGRS. Le concept de 'fiabilité' au regard duquel la ministre de la Défense a demandé d'évaluer la 'watchlist' n'étant pas consacré en tant que tel dans les règles régissant les activités du SGRS, le Comité permanent R a décidé d'évaluer les données (à caractère personnel) reprises dans la 'watchlist' au regard du standard juridique de qualité des données traitées prescrit dans les articles 75, 3° et 4°, et 83, 1° de la Loi sur la protection des données. En effet, plus les données traitées sont adéquates,

[108] Voir COMITÉ PERMANENT R, *Rapport d'activités 2020,* 169-171 ('Diverses recommandations relatives à l'enquête de contrôle sur le suivi de l'extrême droite').

pertinentes, non excessives, complètes et mises à jour *en fonction de la finalité* de la 'watchlist', plus cette dernière peut être considérée comme 'fiable'.

Dans ce cadre normatif, compte tenu de la finalité de la 'watchlist', à savoir un processus de travail interne, en cours d'élaboration, d'identification et de suivi de la menace émanant de l'extrême droite relevant de la compétence du SGRS, le Comité a considéré que la conformité de la 'watchlist' aux articles 75, 3° et 4°, et 83, 1° LPD n'appellait pas de commentaire particulier. Le Comité permanent R a toutefois estimé nécessaire d'émettre une série de recommandations à l'égard du SGRS, en vue de poursuivre, finaliser et documenter le processus de travail que constitue la 'watchlist'.

I.9.3.5. Les habilitations de sécurité successives de Jürgen Conings

Jürgen Conings était titulaire d'une habilitation de sécurité de niveau SECRET[109] depuis le 21 août 2006. Cette habilitation avait depuis fait l'objet de multiples renouvellements malgré l'existence de notices de police à propos de l'intéressé (concernant des faits de menaces et de coups et blessures).

Lors de la procédure de renouvellement initiée par son officier de sécurité en 2019, la VSSE signale un « *hit* » et, dans un document interne, rend notamment compte de deux faits à caractère judiciaire dont un concernant la détention illégale d'armes. Contactée par le SGRS, la VSSE transmet ces informations, d'abord oralement puis par voie électronique, mentionnant que Jürgen Conings est connu pour l'appartenance à un groupe Facebook défendant les intérêts assyriens en Irak. Les faits de 2015 sont mentionnés, mais pas ceux de 2018. Sur base de ces informations, le SGRS lance une première analyse SOCMINT. Celle-ci révèle des liens potentiels avec des mouvances d'extrême droite. À la suite d'une interview avec l'intéressé, les enquêteurs du SGRS concluent que les faits détectés en relation avec l'extrême droite ne sont pas de nature à nuire à son habilitation de sécurité, mais préconisent quand même une mise en garde.

Le 24 juin 2020, Conings obtient le renouvellement de son habilitation. Deux jours plus tard, alors que des menaces sont proférées à l'encontre de Marc Van Ranst, un analyste du SGRS identifie Jürgen Conings sur les vidéos de surveillance et un rapport administratif (RAR) de la police complète le tableau. Une deuxième analyse SOCMINT est diligentée et révèle de nouveaux liens plus inquiétants avec l'extrême droite. Sur la base de ces éléments, le SGRS refuse le renouvellement de l'habilitation de sécurité le 31 août 2020.[110]

---

109 Dans son article 4, la L.C&HS distingue trois degrés de classification : CONFIDENTIEL, SECRET, TRÈS SECRET.

110 Vu les délais, Jürgen Conings n'était plus habilité dès le 17 juillet 2020. Pour rappel, cette absence ou ce refus n'avait aucune conséquence sur sa nouvelle fonction au sein de la Défense.

I.9.3.6. La mission d'officier de sécurité

Le 2 juin 2020, Jürgens Conings a fait mutation vers sa nouvelle unité (PDT-IA) dans une fonction ne nécessitant plus d'habilitation de sécurité. L'officier de sécurité en charge de sa nouvelle unité n'a pas mis fin à la demande de renouvellement. En effet, dans certains cas de figure et dans le cadre de déploiements, une telle habilitation est nécessaire.

Début septembre 2020, l'officier de sécurité a été informé par le SGRS du non-renouvellement. Vu les circonstances liées au COVID, il a informé par téléphone l'intéressé dudit refus. La notification verbale a été confirmée par écrit le 12 novembre 2020 soit 2 mois et demi après le refus.

Au sein du SGRS, le Règlement IF5 décrit les responsabilités de l'officier de sécurité, en charge notamment de l'élaboration d'ordres permanents de sécurité et du contrôle de leur application. Aucune mention n'est toutefois faite de la collaboration et des interactions avec le personnel du SGRS.

Le cas de l'officier de sécurité de Jürgen Conings est particulier. Responsable d'une multitude de petites entités indépendantes, il est délocalisé par rapport aux unités qu'il doit contrôler. Cette délocalisation ne lui permet certainement pas un contrôle effectif de l'application des directives de sécurité.

Le Comité permanent R a en outre constaté que le SGRS n'avait pas communiqué avec l'officier de sécurité de l'unité de Jürgen Conings dans le cadre du refus de son habilitation. Le Comité a également constaté que l'officier de sécurité était dans l'incapacité d'exercer un contrôle sur l'ensemble des unités dont il a la charge.

I.9.3.7. Le dépôt d'armes et le rôle du SGRS

Le 18 mai 2021, un collègue de Jürgen Conings constate que des armes et des munitions sont manquantes dans l'armurerie et le dépôt de munitions dédiés à la Cellule PDT-IA. Il signale immédiatement l'incident à sa hiérarchie et déclenche une enquête interne au niveau de la Direction S du SGRS. Les directives internes du SGRS (en particulier le règlement IF5(bis)) excluent pourtant qu'un même individu puisse être à la fois gestionnaire d'armes et de munitions. Le Règlement IF5 attribue également un statut spécial à ces locaux. Ainsi, les gestionnaires des dépôts de munitions et d'armurerie devraient disposer d'une habilitation de sécurité. L'enquête a révélé que ces règles n'étaient pas respectées au sein de la Cellule PDT-IA. La multiplication d'adaptations aux règles, couplée aux aménagements liés à l'épidémie de Covid-19, ont permis à Jürgen Conings d'avoir accès à l'arsenal avec lequel il a pris la fuite.

I.9.4. CONCLUSIONS

L'affaire Conings est une illustration des manquements constatés par le Comité permanent R ces dix dernières années au sein des services de renseignement et de sécurité en général, et au sein du service de renseignement militaire en particulier. Avec l'affaire Conings, on ne peut pas nier que c'est le service de renseignement militaire qui se retrouve dans la tourmente. Il est indéniable que des erreurs (graves) ont été commises à tous les niveaux du SGRS, mais aussi dans toute la ligne hiérarchique de la Défense : un manque d'effectifs structurel dans les différents services et à tous les niveaux, une grande rotation du personnel, la perte de connaissances et d'expérience, une supervision limitée dans l'unité de Conings, une défaillance manifeste dans le flux d'informations (*bottom up* et *top down*), une nouvelle structure de travail complexe au SGRS, trop peu d'orientation, des problèmes relatifs au personnel, aucune politique claire en matière d'extrémisme, un échange d'informations défaillant au sein de la Défense et entre les différents acteurs de la sécurité, etc. Des erreurs ont peut-être aussi pu être constatées dans le chef d'autres acteurs (police, parquets, juges d'instruction, etc.). L'examen de ces éventuelles erreurs sort du domaine de compétence du Comité permanent R.

Il a pu être constaté que les faits dans cette affaire ont été détectés à temps par les services de renseignement et de sécurité, mais ils n'ont pas fait l'objet d'un suivi suffisamment actif. La marge d'amélioration est importante.

Il est indéniable, pour le Comité permanent R, que le SGRS est nécessaire, voire indispensable, dans l'architecture générale de la sécurité tant en Belgique qu'à l'étranger. Son fonctionnement doit néanmoins être modifié en profondeur. Et sa structure tout autant. L'idéal serait de réduire ses tâches au minimum afin de lui permettre de se régénérer calmement et d'aboutir au *change management* attendu dans le cadre d'une professionnalisation mise au service de la sécurité du citoyen.

I.10. ENQUÊTE COMMUNE DE CONTRÔLE SUR LE RÔLE DE L'OCAM DANS LE SUIVI DU MILITAIRE JÜRGEN CONINGS

En complément de l'enquête de contrôle concernant le suivi de Jürgen Conings par les deux services de renseignement[111], le Comité permanent R a également examiné, conjointement avec le Comité permanent P, « *le rôle de l'OCAM dans le suivi de Jürgen Conings, à savoir en ce qui concerne l'enquête préliminaire, l'évaluation de la menace de niveau 3 et ses conséquences et l'échange d'informations à propos de l'intéressé* ». Les Comités permanents R et P se sont ainsi intéressés à la

[111] Voir 'I.9. Enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings'.

position d'information de l'OCAM, au processus d'évaluation de la menace posée par l'intéressé ainsi qu'à l'échange d'informations entre les partenaires.[112]

I.10.1. ANALYSE DU CADRE LÉGAL

La Loi relative à l'analyse de la menace du 10 juillet 2006 (L.OCAM) confie à l'OCAM la mission d'effectuer ponctuellement une évaluation commune des éventuelles menaces en matière de terrorisme et d'extrémisme et, le cas échéant, les mesures qui s'avèrent nécessaires.

Pour évaluer la menace, l'OCAM se base sur les renseignements provenant de ses services d'appui (par exemple, la VSSE, le SGRS et la Police fédérale). Selon la L.OCAM, les services d'appui sont tenus (sous peine d'une sanction pénale), sauf en cas de procédure d'embargo, de communiquer à l'OCAM, d'office ou à la demande de son directeur, tous les renseignements dont ils disposent dans le cadre de leurs missions légales et qui s'avèrent pertinents pour l'accomplissement des missions de l'OCAM dans les délais prévus par l'Arrêté royal du 28 novembre 2006 portant exécution de la loi du 10 juillet 2006 relative à l'analyse de la menace. Le flux d'informations entre l'OCAM et ses services d'appui varie selon qu'il s'agisse de documents classifiés ou non. Les informations classifiées sont échangées par BINII et ensuite enregistrées par l'OCAM dans sa base de données PROTEUS. La messagerie fonctionnelle de l'OCAM est utilisée pour tout l'échange d'informations non classifiées.

L'article 11 §6 de l'arrêté d'exécution de la L.OCAM stipule que chaque évaluation déterminera le niveau de la menace en s'appuyant sur une description de la gravité et de la vraisemblance du danger ou de la menace.[113] Selon l'article 10 L.OCAM, les évaluations ponctuelles de la menace concernant des personnes, des groupements, des objets ou des événements, exécutées d'initiative par l'OCAM, sont communiquées aux membres du Conseil national de sécurité, aux services d'appui, à la Direction générale du Centre de crise, au Parquet fédéral et au membre du Collège des procureurs généraux à qui est confiée la matière du terrorisme et de l'extrémisme, à l'Autorité nationale de sécurité (ANS) ainsi qu'à tout membre du gouvernement que le directeur de l'OCAM juge nécessaire d'informer.

---

112 Jusqu'au 17 mai 2021, jour de la disparition de Jürgen Conings.

113 Les différents niveaux de la menace sont :
- le « Niveau 1 ou FAIBLE » lorsqu'il apparaît que la personne, le groupement ou l'événement qui fait l'objet de l'analyse n'est pas menacé ;
- le « Niveau 2 ou MOYEN » lorsqu'il apparaît que la menace à l'égard de la personne, du groupement, ou de l'événement qui fait l'objet de l'analyse est peu vraisemblable ;
- le « Niveau 3 ou GRAVE » lorsqu'il apparaît que la menace à l'égard de la personne, du groupement ou de l'événement qui fait l'objet de l'analyse est possible et vraisemblable ;
- le « Niveau 4 ou TRES GRAVE » lorsqu'il apparaît que la menace à l'égard de la personne, du groupement ou de l'événement qui fait l'objet de l'analyse est sérieuse et imminente.

L'évaluation de la menace que représente une personne est quant à elle régie par l'Arrêté royal relatif à la banque de données commune *Foreign Terrorist Fighters* du 21 juillet 2016 (AR BDC) et la circulaire du 22 mai 2018 du ministre de la Sécurité et de l'Intérieur et du ministre de la Justice relative à l'échange d'informations et au suivi des *Terrorist Fighters* et des Propagandistes de haine (diffusion restreinte) (CM BDC). Dans le cadre de cette enquête, les Comités permanents R et P se sont penchés plus spécifiquement sur la création et l'alimentation de la banque de données commune *Terrorist Fighters* (BDC TF).

I.10.2. L'OCAM ET LES BANQUES DE DONNÉES COMMUNES

Après les attentats de 2016, la Loi du 27 avril 2016 relative à des mesures complémentaires en matière de lutte contre le terrorisme a modifié la Loi du 5 août 1992 sur la fonction de police (LFP) et prévoit une base légale pour la constitution d'une banque de données commune afin de renforcer la prévention et la lutte contre le terrorisme et l'extrémisme pouvant mener au terrorisme.

L'AR BDC a ensuite effectivement créé la banque de données commune *Foreign Terrorist Fighters*. Par un arrêté de modification du 23 avril 2018, cette banque de données a été rebaptisée banque de données commune *Terrorist Fighters* (BDC TF) en raison de l'ajout d'une nouvelle catégorie *Homegrown Terrorist Fighters* à côté de la catégorie *Foreign Terrorist Fighters* existante. Un nouvel arrêté royal à la même date a créé une banque de données commune distincte pour les Propagandistes de haine (BDC PH).[114]

Enfin, l'arrêté royal du 20 décembre 2019 a ajouté deux nouvelles catégories à la banque de données commune *Terrorist Fighters*, à savoir les Extrémistes Potentiellement Violents et les Personnes condamnées pour terrorisme.[115] En application de l'AR FTF et des AR de modification de 2018 et 2019, la BDC TF organise donc désormais le suivi des *Foreign Terrorist Fighters* (FTF), des *Homegrown Terrorist Fighters* (HTF), des Extrémistes Potentiellement Violents (EPV) et des Personnes condamnées pour terrorisme (PCT).

Afin de renforcer l'échange d'informations, la loi prévoit une obligation d'alimentation de la BDC pour les services ayant un accès direct aux banques de données communes. Les données relatives à une entité enregistrée dans la BDC

---

114 Arrêté royal 23 avril 2018 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Foreign Terrorist Fighters portant exécution de certaines dispositions de la section 1 er*bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police et modifiant la banque de données commune Foreign Terrorist Fighters vers la banque de données commune Terrorist Fighters, et A.R. du 23 avril 2018 relatif à la banque de données commune Propagandistes de haine et portant exécution de certaines dispositions de la section 1er*bis* « de la gestion des informations » du chapitre IV de la loi sur la fonction de police, *M.B.*, 30 mai 2018.

115 A.R. du 20 décembre 2019 modifiant l'Arrêté royal du 21 juillet 2016 relatif à la banque de données commune Terrorist Fighters, *M.B.* 27 janvier 2020.

doivent ainsi continuellement être tenues à jour. C'est en ce sens que la BDC est une banque de données dynamique. Seuls les services de base (OCAM, VSSE, SGRS et police intégrée) peuvent créer une nouvelle entité dans la BDC et, après validation de l'OCAM, placer une personne en pré-enquête pour une durée de 6 mois maximum. Pour chaque entité enregistrée, les services avec accès direct à la BDC veillent à ajouter les données à caractère personnel et informations dont ils disposent. Chaque service ne peut modifier ou supprimer que les données et informations qu'il a lui-même enregistrées.

En tant que responsable opérationnel de la BDC, l'OCAM est chargé de l'évaluation des informations de la fiche de renseignements (voir *infra*) et de la validation d'une entité dans la BDC sur la base des informations fournies par les partenaires.

I.10.2.1. La procédure d'inscription

La procédure d'inscription pour la catégorie d'EVP – catégorie introduite par l'AR du 20 décembre 2019 et dans laquelle Jürgen Conings était repris – est développée dans la circulaire du ministre de l'Intérieur et de la Sécurité et du ministre de la Justice du 22 mai 2018 relative à l'échange d'informations et au suivi des TF et des PH (CM BDC).[116] Cette circulaire décrit en réalité l'échange d'informations concernant les catégories FTF, HTF et PH, mais elle est appliquée, par analogie, aux EPV[117].

La phase de « pré-enquête » (dite « phase d'enrichissement ») vise la phase de collecte de données et d'informations, à charge et à décharge, nécessaires à la

---

116 L'objectif général de la circulaire est : « *partant d'un objectif de sécurité, régler la gestion de l'information, la prise de mesures et la collaboration coordonnée entre les services concernés dans le but de garantir la protection maximale de la sécurité publique face à la menace potentielle et de contrecarrer la menace émanant des Terrorist Fighters (FTF/HTF) et des propagandistes de haine.* »

117 La catégorie EPV concerne toute personne physique ayant un lien avec la Belgique et qui répond aux critères cumulatifs suivants :

a) cette personne a des conceptions extrémistes qui justifient l'usage de la violence ou de la contrainte comme méthode d'action en Belgique ;

b) il existe des indications fiables qu'elle a l'intention de recourir à la violence, et ce en relation avec les conceptions mentionnées en a) ;

c) l'EPV répond au minimum à une des conditions suivantes quant au risque de violence : 1) il entretient systématiquement des contacts sociaux au sein de milieux extrémistes ; 2) il a des problèmes psychiques constatés par un professionnel compétent en la matière ; 3) il a commis des actes ou présente des antécédents qui peuvent être considérés comme soit a) un crime ou un délit portant atteinte à ou menaçant l'intégrité physique ou psychique de tiers ; soit b) des instructions ou des formations relatives à la fabrication ou l'utilisation d'explosifs, d'armes à feu ou d'autres armes ou substances nocives ou dangereuses, ou pour d'autres méthodes et techniques spécifiques en vue de commettre des infractions terroristes conformément à l'article 137 du Code pénal ; soit c) des agissements en connaissance de cause constituant un soutien matériel en faveur d'une organisation ou d'un réseau terroriste/extrémiste ; soit d) des agissements dont la nature indique un niveau de vigilance préoccupant de l'individu à l'égard de la sécurité.

validation ou non d'une entité en tant qu'EPV. La CM BDC encourage les services à déterminer ensemble, au sein des LTF et dans le respect de leurs missions légales respectives, la stratégie de récolte d'informations afin d'enrichir les renseignements ('qui fait quoi'). À l'issue de cette période de maximum six mois, sur la base des informations et renseignements disponibles, l'OCAM évalue si les critères légaux sont rencontrés. Si ce n'est pas le cas, les données de la personne en pré-enquête sont automatiquement effacées.

Conformément à ce que prévoit la CM BDC, la BDC se compose de fiches de renseignements reprenant les données à caractère personnel et les informations non classifiées qui proviennent de tous les services qui alimentent la BDC. Ces fiches permettent non seulement d'évaluer la menace que représentent les entités mais surtout d'en assurer le suivi afin d'anticiper et d'empêcher de potentielles infractions terroristes.

Lorsque le statut dans la BDC est validé, l'OCAM procède à une évaluation de la menace individuelle à partir des informations pertinentes dont il dispose. Cette évaluation, intégrée dans la fiche de renseignements individuelle, permet d'orienter les mesures de suivi prises par les partenaires.

Afin d'évaluer les critères d'attribution d'un statut et le niveau de la menace, l'OCAM s'appuie sur son propre outil d'évaluation du risque, RooT37. À l'aide d'indicateurs inspirés de la littérature scientifique, l'outil définit un score indicatif. Ce score est ensuite contrôlé par un évaluateur de l'OCAM, puis, une nouvelle fois, par une « équipe qualité » avant d'être définitivement validé.

I.10.2.2. L'échange d'informations avec les partenaires

Dans le cadre du Plan R[118], l'échange d'informations est notamment organisé au sein des LTF qui sont des plateformes de concertation opérationnelles et stratégiques, destinées aux services de police et de renseignement et installées dans chaque arrondissement judiciaire,[119] et des cellules de sécurité intégrale locales en matière de radicalisme, d'extrémisme et de terrorisme (CSIL-R), qui sont des plateformes de concertation communales chargées de la réalisation d'actions préventives, répressives et de suivi cohérentes. Comme les LTF, elles sont des plateformes de concertation, théâtre d'échange d'informations entre les services de prévention et sociaux, la LTF et les autorités administratives concernant le radicalisme, l'extrémisme et le terrorisme.

Conformément à la CM BDC, les LTF jouent un rôle crucial dans la définition des mesures de sécurité. Ainsi, lors des réunions des LTF, les partenaires s'accordent

118 Devenu 'Stratégie Extrémisme et Terrorisme' (Stratégie TER) en septembre 2021.

119 Elles ont pour but de garantir le suivi au niveau local d'individus et de groupements radicalisants ainsi que de réduire leur impact en proposant des mesures en échangeant et discutant notamment d'informations, de renseignements et d'analyses.

sur la priorisation des entités à suivre selon la menace qu'elles représentent et sur leur degré de coopération avec les autorités.

I.10.3. LE RÔLE DE L'OCAM DANS LE SUIVI DE JÜRGEN CONINGS : L'INSCRIPTION DANS LA BANQUE DE DONNÉES COMMUNE

En août 2020, l'OCAM a ouvert une pré-enquête EPV concernant Jürgen Conings. Cette décision repose sur l'analyse des informations transmises par la police et les services de renseignement dès juin 2020. L'OCAM a également procédé à une analyse de son activité sur les réseaux sociaux. Encodées dans la banque de données de l'OCAM, PROTEUS, ces informations concernaient notamment les menaces proférées par l'intéressé et ses contacts au sein des milieux d'extrême droite. Au regard des informations disponibles, les Comités permanents R et P estiment la décision de pré-enquête justifiée.

Dès l'ouverture d'une pré-enquête, les services de base ont l'obligation d'enrichir la BDC de toutes les informations pertinentes dont ils disposent. Le suivi doit en outre être assuré au sein de la LTF compétente. L'analyse des PV des réunions de la LTF et du groupe de travail Extrême droite (Plan R) confirme l'inscription du suivi de Jürgen Conings à l'ordre du jour dès septembre 2020.

À la fin de la pré-enquête et à l'aide de son outil Root37, l'OCAM a réalisé une évaluation des éléments dont il disposait au regard des critères de validation définis dans l'AR BDC. Le statut d'EPV a été confirmé et la menace présentée par Jürgen Conings a été évaluée au niveau 3 (grave). Cette évaluation a été confirmée par l'évaluateur de l'OCAM et l'équipe qualité à la mi-février 2021.

I.10.4. L'ÉCHANGE D'INFORMATIONS

L'OCAM a informé les différents partenaires de la LTF concernée de l'inscription de Jürgen Conings dans la BDC et de l'évaluation de la menace lors d'une réunion fin février 2021 à laquelle le SGRS n'a pas participé. Le procès-verbal de la réunion rend compte des échanges à propos de l'intéressé.

L'enregistrement de Jürgen Conings dans la BDC a en outre été communiqué à la Police fédérale (pour signalement dans la Banque de données nationale générale ou BNG), à BELPIU ainsi qu'à la CSIL-R pertinente (et donc au bourgmestre). L'OCAM n'a toutefois envoyé aucune alerte supplémentaire aux services de base et à ses partenaires concernant l'évaluation de niveau 3 de l'intéressé, estimant suffisante l'inscription dans la BDC.

Après son inscription dans la BDC, le suivi de Jürgen Conings figurait à l'ordre du jour de chaque réunion de la LTF et du groupe de travail Extrême droite, bien

que de nouvelles informations n'aient pas toujours été disponibles (voir *infra*). L'unique information complémentaire transmise à l'OCAM avant le 17 mai 2021 n'a pas justifié de modification du niveau de la menace.

L'inscription en tant qu'EPV/niveau 3 dans la BDC permet en outre l'échange d'informations avec les services ayant uniquement un accès *hit/no hit* qui, lors de la consultation de la BDC, sont également informés qu'une personne est connue. Dans le cas de Jürgen Conings, la Direction générale Sécurité & Prévention du SPF Intérieur a par exemple consulté la BDC (et obtenu un « *hit* ») dans le cadre de la demande par l'intéressé d'une carte d'identification d'agent de gardiennage.

Conformément à la CM BDC, chaque personne inscrite dans la BDC se voit attribuer une catégorie (A, B ou C) dans le cadre du suivi en LTF. Lors de son inscription, Jürgen Conings a été classé en catégorie B, à savoir une « menace pas particulièrement élevée ». Les Comités permanents R et P ont pointé le manque de cohérence entre le niveau de menace défini par l'OCAM (3 soit grave), d'une part, et la catégorie pour le suivi en LTF, d'autre part. L'OCAM précise que les mesures de suivi sont semblables pour les catégories A, B et C mais relève, plus généralement, la difficile application des mesures prévues dans la CM BDC qui reste non contraignante.[120]

En ce qui concerne les autres mesures, comme le « suivi proactif », l'OCAM constate que même avec les FTF, il n'est pas toujours évident d'y parvenir, étant donné que ceci n'est pas exécutoire et que la CM BDC se heurte à ses limites au niveau des mesures. Si aucune information ou enquête pénale pour terrorisme ne peut être ouverte, pas grand-chose n'est alors possible. Dans le cas de Jürgen Conings, une enquête judiciaire était en cours pour les menaces à l'encontre de Marc Van Ranst.[121] L'OCAM constate qu'en dehors de ce qui a été communiqué au sein de la LTF, il n'a reçu aucune autre information à propos de l'enquête judiciaire en cours.

Une autre conséquence du statut EPV de niveau 3 est qu'il devrait être abordé au sein de chaque LTF pour déterminer quelles informations émergent et identifier éventuellement les mesures à adopter pour réduire la menace. Aux yeux de l'OCAM, l'initiative incombe au SGRS, étant donné qu'il s'agissait d'un militaire. Néanmoins, la récolte d'informations est attendue de tous les services. Lors des réunions de la LTF de mars et d'avril 2021, l'intéressé figurait à l'ordre du jour mais n'a été abordé par aucun service, et aucune information à ce sujet n'a dès lors été partagée.

En application de la note 'Signalements' élaborée par DJSOC/Terro (Direction de la lutte contre la criminalité grave et organisée (section terrorisme) de la Police judiciaire fédérale), chaque EPV est signalé dans la BNG pour un « contrôle discret ». Selon l'OCAM, cette mesure n'a pas permis de récolter davantage

120 Pour l'OCAM, l'octroi de cette catégorie B ne veut pas dire qu'il est procédé à une évaluation supplémentaire. La catégorie B doit en effet également être suivie de près.

121

d'informations. Dans le cas contraire, ces informations auraient été abordées au sein d'une LTF.

I.10.5. CONCLUSIONS

L'enquête des Comités permanents R et P relative au rôle de l'OCAM dans le suivi de Jürgen Conings confirme le partage d'informations à l'OCAM par les services de base lors de la phase de pré-enquête dès août 2020. Sur la base de ces informations enregistrées dans PROTEUS et à l'aide de l'outil Root37, le statut EPV de Jürgen Conings a été validé et le niveau de menace évalué à 3.

C'est l'OCAM qui a pris l'initiative de placer Jürgen Conings en pré-enquête EPV et de lui attribuer le statut d'EPV de niveau 3. Les Comités permanents R et P ont estimé la décision de pré-enquête justifiée.

L'évaluation de la menace posée par Jürgen Conings a été communiquée par l'OCAM selon les modalités prévues par la L.OCAM. Evalué au niveau 3 de menace (grave), Jürgen Conings n'a par contre été placé qu'en catégorie B (menace pas particulièrement grande) dans le cadre du suivi en LTF. Les deux paramètres sont en effet indépendants.

I.11. LE SUIVI D'UN COMMISSAIRE DU GOUVERNEMENT PAR LA VSSE

Par arrêté royal du 17 mai 2021, Ihsane Haouach a été nommée comme commissaire du gouvernement auprès de l'Institut pour l'égalité entre les femmes et les hommes (IEFH). En cette qualité, elle représentait le gouvernement au conseil d'administration de l'IEFH. Elle a cependant été sous le feu des critiques dès sa nomination : d'une part en raison de son voile, et d'autre part, en raison des propos qu'elle a tenus sur la séparation entre l'Église et l'État. Le 9 juillet 2021, Ihsane Haouach a présenté sa démission. Le même jour, il a été suggéré dans les médias qu'une note de la Sûreté de l'État (VSSE) pourrait en être à l'origine.[122]

[122] B. DEMONTY, *Le Soir*, 9 juillet 2021 ('Ihsane Haouach démissionne, le gouvernement en possession d'informations sur de potentiels liens avec les Frères musulmans'). Le rapport de la VSSE en question ('Diffusion restreinte'/ 'Confidentiel') est également paru intégralement dans la presse (par ex. M. VERBERGT, *De Standaard*, 14 juillet 2021 ('Dit zegt de Staatsveiligheid letterlijk over Ihsane Haouach')).

I.11.1. UNE NOTE DE LA SÛRETÉ DE L'ÉTAT

Courant 2020, la Section d'Analyse Contre-extrémisme (CE) de la VSSE a rédigé une note de synthèse sur les Frères musulmans en Belgique.[123] Au moment où la controverse est née dans la presse autour de la nomination de Ihsane Haouach comme commissaire du gouvernement, on se souvient à la VSSE que son nom était apparu dans cette note de synthèse. L'intéressée n'était cependant pas une 'cible' du service. En revanche, la VSSE suit des agissements dans le cadre de la lutte contre diverses formes d'extrémisme, ce qui s'inscrit dans ses missions légales (art. 8 L.R&S, 'extrémisme').

La VSSE a jugé opportun d'informer par écrit le ministre de la Justice et le Premier ministre à ce propos. Une note classifiée a été rédigée à cet effet. Il semblait qu'Ihsane Haouach était *'gekend omwille van haar nauwe contacten met de Moslimbroeders. Deze contacten tussen de Moslimbroeders en Ihsane Haouach kunnen worden gekaderd binnen een bredere strategie van de Moslimbroeders, waarbij deze proberen te wegen op het publieke debat en de beleidsvorming […]'*.[124] Il était également mentionné que l'intéressée *'voor zover ons bekend zelf geen lid is van de Moslimbroeders en zelf nooit de aandacht heeft getrokken omwille van concrete extremistische stellingnames' […] Het is dan ook niet uit te sluiten dat Ihsane Haouach er zich zelf niet (ten volle) van bewust is dat ze nauwe contacten onderhoudt met de Moslimbroeders. We stellen dan ook voor om de bevoegde Staatssecretaris of haar Beleidscel, net als eventueel mevrouw Haouach zelf, een sensibiliserende briefing aan te bieden*'.[125] [126]

---

123 Voir à ce propos 'I.12. Une attention renouvelée pour les Frères musulmans' (*infra*).

124 *'connue en raison de contacts étroits avec les Frères musulmans. Ces contacts entre les Frères musulmans et Ihsane Haouach peuvent s'inscrire dans une stratégie plus large des Frères musulmans, par laquelle ils tentent d'influencer le débat public et l'élaboration de politiques […]'* (traduction libre).

125 *'du moins à notre connaissance, n'est elle-même pas membre des Frères musulmans et n'a jamais attiré l'attention en raison de positions extrémistes concrètes […]. Il ne peut donc être exclu que Ihsane Haouach elle-même ne soit pas (pleinement) consciente du fait qu'elle a des contacts étroits avec les Frères musulmans. Nous suggérons dès lors de briefer la Secrétaire d'État compétente et sa Cellule stratégique, mais éventuellement aussi Madame Haouach elle-même, et ce afin de les sensibiliser à cette problématique.'* (traduction libre).

126 Citation reprise de la note confidentielle de la VSSE qui a été publiée dans la presse (M. VERBERGT, *De Standaard*, 14 juillet 2021 ('Dit zegt de Staatsveiligheid letterlijk over Ihsane Haouach')).

I.11.2. CONSTATATIONS DE L'ENQUÊTE

I.11.2.1. Une attention renouvelée pour les Frères musulmans (et Ihsane Haouach) ?

Si la lutte contre le terrorisme continue de figurer en haut de la liste de ses priorités, la VSSE a de nouveau porté son attention sur d'autres dossiers au cours de ces dernières années. Dans le cadre des menaces 'extrémisme' et 'ingérence', il a été décidé en 2020 de rédiger une note de synthèse sur les Frères musulmans en Belgique, qui constitue une des priorités de la VSSE dans son Plan d'action. Le nom de Ihsane Haouach est apparu dans le contexte de cette note, comme étant une personne qui, consciemment ou non, était en contact avec cette mouvance. L'intéressée n'était cependant pas une 'cible' de la VSSE.

Par le biais de (l'agitation dans) la presse, la VSSE apprenait la nomination de Ihsane Haouach comme commissaire du gouvernement. Le service prit l'initiative de rédiger une note, estimant qu'il convenait en premier lieu d'informer le ministre de la Justice du fait que l'intéressée était connue dans le cadre du suivi des compétences légales en matière d'extrémisme. Étant donné qu'il n'était exclu que l'intéressée elle-même ne soit pas (pleinement) consciente d'entretenir des liens étroits avec les Frères musulmans, il était proposé au ministre d'organiser un briefing de sensibilisation pour la Secrétaire d'État ou sa Cellule stratégique, y compris pour Ihsane Haouach dans une phase ultérieure.

I.11.2.2. Le principe de précaution

Dans un contexte de renseignement, il n'y a que peu de certitudes, ce qu'il faut garder à l'esprit quand il s'agit de décider de communiquer des informations et de la manière de les communiquer (dans le cas présent, au ministre de la Justice). Le Comité avait précédemment affirmé que « *(p)our pouvoir être considérée comme légale, la communication d'informations doit être suffisamment étayée par des informations fiables. Elle doit également être formulée avec précaution. Par exemple, aucune image sans nuance ne peut être donnée des renseignements sous-jacents, ou un élément particulier ne peut être présenté comme une 'vision de ' ou une 'impression de'. En ce sens, les informations fournies doivent également être 'justes' en offrant une image objective de la façon dont le service de renseignement perçoit la menace et le rôle de la personne concernée, sans être 'manipulatrices' […]* ».[127] Le Comité estimait que la note répondait au principe de précaution précité et que la VSSE avait, dans sa communication, suffisamment expliqué au gouvernement les

[127] COMITÉ PERMANENT R, Enquête de contrôle sur la manière dont les services de renseignement belges communiquent avec un employeur, privé ou public, sur un collaborateur, 2020.

raisons pour lesquelles les liens de la commissaire du gouvernement avec les Frères musulmans étaient susceptibles de représenter une menace.

Bien qu'une note écrite ait été préparée, il a été décidé, dans les jours qui suivent, de ne pas envoyer cette note directement. À la VSSE, l'on avait conscience que la note était politiquement sensible, incomplète, et qu'il fallait éviter une fuite. Il a été décidé d'informer oralement le ministre de la Justice, mais l'entretien n'a pas eu lieu. L'article 19 L.R&S ne stipule pas de quelle manière les renseignements doivent être communiqués par la VSSE. Par le passé, le Comité était d'avis que la communication devait se faire par écrit, et ce pour des raisons de sécurité juridique (excepté en cas d'extrême urgence), et ce afin d'éviter des discussions par la suite et permettre un contrôle parlementaire (voire juridique). La Secrétaire d'État compétente n'a pas été informée directement, la VSSE ayant supposé que le Premier ministre ou le Vice-Premier ministre s'en chargerait.

I.11.2.3. Aucune autre constatation d'enquête ?

La VSSE était consciente – entre autres après la séance plénière de début juin 2021 au Parlement – de la sensibilité politique de la question de la nomination. Cela étant, il a été décidé d'attendre la confirmation des éléments repris dans la note avant d'envoyer celle-ci. La note a finalement été retenue plus d'un mois, la VSSE ne souhaitant pas être instrumentalisée. Il apparait néanmoins qu'aucune modification n'ait été apportée à la note qui a finalement été envoyée en juillet au Premier ministre, aux Vice-Premiers ministres et à la ministre de l'Intérieur. En d'autres termes, il n'y a pas eu d'autre constatation d'enquête.

Sur la base des éléments de l'enquête, le Comité permanent R n'a pas pu se prononcer sur un lien de causalité entre la note et la démission de la commissaire de gouvernement Ihsane Haouach.

I.11.2.4. La fuite d'une note classifiée

La note sur Ihsane Haouach a été classifiée 'Confidentiel Loi 11.12.1998'. Elle a néanmoins été publiée *in extenso* dans la presse à peine un jour après sa transmission au Premier ministre, aux Vice-Premiers ministres et à la ministre de l'Intérieur. Dès lors que la remise d'un document classifié à un tiers constitue une infraction pénale, la VSSE a, à juste titre selon le Comité, porté plainte contre X auprès du procureur du Roi de Bruxelles.

Le Comité permanent R a rappelé qu'il appartient aux officiers de sécurité des différents cabinets ministériels de veiller à l'utilisation adéquate de documents classifiés. Les destinataires des notes classifiées doivent également être extrêmement prudents avec ces informations. Ils doivent tout d'abord être conscients que la remise à un tiers non habilité est un fait punissable sur le plan pénal. Pareille action peut également être dommageable pour les personnes faisant l'objet de la note.

Enfin, cela préjudicie également aux services de renseignement et porte atteinte à la confiance que leur accordent les citoyens.

I.11.2.5. Une 'entrave' ?

Dans la note destinée au ministre de la Justice, il était proposé d'organiser également un 'briefing de sensibilisation' pour Ihsane Haouach. La finalité sous-jacente était double. Il n'était pas exclu que l'intéressée elle-même n'était pas (pleinement) consciente d'entretenir des liens étroits avec les Frères musulmans, une sensibilisation était par conséquent nécessaire/utile. Si toutefois elle en était consciente, l'objectif de ce genre de briefing pouvait être de créer un effet perturbateur (ici en l'occurrence 'dissuasif'). La VSSE affirmait à ce propos qu'elle entendait à l'avenir adopter une approche disruptive, et ce, en élaborant des procédures et des accords de coopération. La question qui se posait était de savoir si l'initiative d'entrave doit/peut émaner d'un service de renseignement et de sécurité. Cette question, comme le respect de la note de service 'entrave' (il n'y a finalement pas eu d'entrave) n'a pas fait l'objet d'enquête.

I.11.2.6. La nécessité d'un screening pour les fonctions revêtant un caractère public ?

La VSSE a-t-elle ou devait-elle prendre l'initiative (spontanée) d'informer le gouvernement lorsqu'elle a pris acte de la nomination de Ihsane Haouach comme commissaire du gouvernement ? Ceci s'applique-t-il tout autant pour d'autres fonctions revêtant un caractère public ? [128] Tout un chacun peut-il faire l'objet d'une vérification ou un extrait du casier judiciaire suffit-il (anciennement le certificat de bonne vie et mœurs) ? La VSSE ne procède pas systématiquement à une vérification lors de chaque nomination d'un commissaire du gouvernement ou de toute autre fonction publique. Il est vrai que dans le cadre des enquêtes effectuées par le service, une personne assumant une fonction publique apparaît de temps à autre. Il convient alors de s'interroger sur l'opportunité de rédiger une note concernant cette personne. La VSSE n'est pas demandeuse d'émettre systématiquement un avis dans ce contexte. Il s'agit d'une décision qui, le cas échéant, doit être prise au niveau politique.[129]

---

[128] Voir en ce sens les problèmes relatifs à la désignation/démission de Salah ECHALLOUI à la Grande Mosquée de Bruxelles et au sein de l'Exécutif des musulmans (avis négatif de la VSSE).

[129] *Cf.* Note classifiée 'CONFIDENTIEL Loi 11.12.1998' de la VSSE du 25 août 2021 adressée au président du Comité permanent R.

Il convient de toujours garder à l'esprit le risque d'instrumentalisation quand il est question d'un sujet politiquement sensible. La structure des notes doit être adaptée à cet effet (ce travail était en cours) : les analystes doivent notamment expliciter la finalité d'une note, les hiatus, les éléments à préciser, ainsi que les personnes à qui la note doit être transmise.

I.12. UNE ATTENTION RENOUVELÉE POUR FRÈRES MUSULMANS

Le 19 juillet 2021, la Commission de suivi a demandé au Comité permanent R de réaliser une enquête de contrôle visant à déterminer, d'une part, si la confrérie des Frères musulmans faisait l'objet d'un suivi par la VSSE et le SGRS, et d'autre part, si elle était constitutive, selon ceux-ci, d'une menace en Belgique.[130] Cette enquête s'inscrivait dans le prolongement de l'enquête de contrôle réalisée sur la manière dont la VSSE a assuré le suivi de la commissaire de gouvernement de l'époque, Ihsane Haouach.[131]

I.12.1. LES FRÈRES MUSULMANS : CONTEXTUALISATION

I.12.1.1. Genèse et internationalisation du mouvement

La confrérie des Frères musulmans (en abrégé 'les Frères musulmans') trouve son origine en Egypte où elle fût fondée, en 1928, par Hassan Al-Banna. L'organisation poursuit à sa genèse deux objectifs : libérer l'Egypte de la domination britannique et réinstaurer les valeurs de l'Islam au sein de la société égyptienne. Elle est interdite en Egypte en 1948 après une série d'affrontements entre une fraction du mouvement et le pouvoir en place.

Très rapidement après sa fondation, le mouvement s'internationalise. Il se développe notamment en Europe suite à l'exil de plusieurs de ses leaders politiques.

---

130 Deux enquêtes de contrôle ayant trait à cette problématique avaient déjà été réalisées par le Comité permanent R. En 2001, le Comité a mené une enquête de contrôle visant à examiner la manière dont les services de renseignement recueillaient et analysaient des informations relatives au terrorisme et à l'islamisme radical, et la manière dont ils informaient les autorités civiles et judiciaires de ce phénomène. Cette enquête s'était notamment intéressée à la présence des Frères musulmans en Belgique, et au suivi qui en était fait par la VSSE. (COMITÉ PERMANENT R, *Rapport d'activités 2001*, 82-131). En 2007, le Comité a mené une enquête de suivi visant à déterminer si les recommandations formulées dans le cadre du suivi de l'islamisme radical par les services de renseignement avaient été suivies (COMITÉ PERMANENT R, *Rapport d'activités 2007*, 7-29).

131 Voir 'I.11 Le suivi d'un commissaire du gouvernement par la VSSE'.

Les Frères musulmans sont présents à partir des années 1960 en Belgique, où ils se sont progressivement investis dans des activités sociales, religieuses et de jeunesse.

I.12.1.2. Quelle ampleur du phénomène en Belgique ?

Pour pouvoir déterminer l'ampleur d'un phénomène, il faut d'abord pouvoir le définir. Le Comité a pu constater qu'il n'existait pas de définition précise et communément acceptée par les services de renseignement belges et les partenaires de la chaine pénale au sens large des « Frères musulmans ». Il s'agit d'une entité aux contours flous, disposant d'antennes jouissant d'une autonomie importante dans de nombreux pays et prenant la forme de différentes organisations opérant de manière discrète voire secrète dans divers pans de la société, et avec des objectifs à long terme incompatibles avec l'ordre démocratique. La difficulté à circonscrire cette mouvance rend son étude, et en particulier l'analyse de sa présence et de son pouvoir d'influence en Belgique, complexe. Il est également extrêmement difficile de déterminer l'appartenance d'une personne à ce groupement, puisque ce dernier ne dispose pas en tant que tel de structures précises ni ne distribue de carte de membre.[132]

La VSSE a néanmoins procédé à une estimation de la présence du mouvement en Belgique indiquant que « *les 'Frères musulmans internationaux' sont représentés par une organisation, la Ligue des Musulmans de Belgique (LMB), qui compterait seulement une cinquantaine de membres et une centaine de partisans ou sympathisants. Notre pays abrite également le siège de Council of European Muslims (CEM ; l'ancien FIOE [Federation of Islamic Organizations in Europe]), une organisation faîtière européenne qui défend les intérêts des Frères musulmans auprès des institutions européennes* ».[133]

Sur la base de ces chiffres, le ministre de la Justice a qualifié la présence du mouvement en Belgique comme « relativement modeste ».[134] Néanmoins, le ministre et la VSSE précisaient que les Frères musulmans paraissent être 'plus influents et plus importants que ce à quoi l'on pourrait s'attendre au vu de leur nombre limité de membres' en raison de leur activisme social et politique intense, leur approche et le profil de leurs membres.[135]

---

132 Le Comité avait déjà pu relever cette difficulté dans son rapport d'activités 2001 (COMITÉ PERMANENT R, *Rapport d'activités 2001*, 103).

133 VSSE, *Rapport annuel 2020*, 13.

134 Réponse du Vice-Premier ministre et ministre de la Justice et de la Mer du Nord datée du 10 mai 2021 à la question écrite n° 7 – 1140 du sénateur Tom ONGENA du 5 mars 2021.

135 *Ibid.* ; VSSE, *Rapport annuel 2020*, 13.

I.12.1.3. Une mouvance considérée comme une menace à l'étranger ?

Le positionnement des États à l'égard du mouvement varie fortement. Dans certains pays, des partis politiques se réclamant de la mouvance frériste sont au gouvernement ou dans l'opposition parlementaire (p. ex. en Turquie, au Maroc, en Algérie et en Lybie). Dans d'autres pays, ladite mouvance est criminalisée.[136] Par l'adoption de sa nouvelle loi antiterroriste le 8 juillet 2021, l'Autriche est le premier pays européen à interdire les Frères musulmans au titre d'organisation liée à la « criminalité à motivation religieuse ». Sans être criminalisé, le mouvement a également retenu récemment l'attention de nos pays voisins.[137]

I.12.2. CONSTATATIONS DE L'ENQUÊTE

I.12.2.1. La mouvance fait-elle l'objet d'un suivi par les services de renseignement ?

L'enquête a révélé que les deux services de renseignement opéraient un suivi des Frères musulmans selon des angles et avec des moyens humains et techniques très différents.

---

136 En Egypte, en Russie, en Arabie Saoudite, aux Emirats Arabes unis et au Bahreïn, elle est considérée officiellement comme une organisation terroriste.

137 Aux Pays-Bas, à l'initiative du Parlement, une enquête a ainsi été réalisée en 2019-2020 sur l'influence qu'exercent certains pays étrangers dans le sillage des Frères musulmans notamment pour infléchir leur démocratie (*Tweede Kamer der Staten-generaal, (On)zichtbare invloed, verslag parlementaire ondervragingscommissie naar ongewenste beïnvloeding uit onvrije landen, Den Haag, 25 juin 2020, consultable en ligne :* https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z12034&did=2020D25817).
Les résultats de cette étude confirment l'exercice − sous diverses formes − d'une influence par plusieurs mouvances, dont celle des Frères musulmans. Il est renvoyé également à une étude réalisée par le service de renseignement néerlandais Algemene Inlichtingen- en Veiligheidsdiensten (AIVD) sur les Frères musulmans en 2011 concluant que les Frères musulmans ne représentaient pas de menace directe pour l'ordre démocratique ou la sécurité nationale mais que leurs activités pouvaient représenter à long terme un risque dès lors que les Frères musulmans sont anti-démocrates et opposés au processus d'intégration. En France, la présence des Frères musulmans et la menace qu'ils représentent ont également été étudiées dans le cadre d'une commission d'enquête du Sénat français lancée en novembre 2019 (*Rapport n° 595 (2019-2020), 7 juillet 2020, n° 595, consultable en ligne :* https://www.senat.fr/rap/r19-595-1/r19-595-1_mono.html#toc62). Dans ce rapport, on lit que le mouvement frériste compte en France environ 50 000 personnes. En Allemagne, les réponses du Gouvernement fédéral à plusieurs questions parlementaires nous apprennent que les organisations entretenant un lien avec les Frères musulmans sont observées par le service de sécurité nationale, le *Bundesambt für Verfassungsschutz* (BfV) et par tous les bureaux des Länder (*Ländesamts für Verfassungsschutz*). Une augmentation du nombre de membres et sympathisants à la confrérie des Frères musulmans dans le pays a été observée, passant de 1040 en 2018 à 1350 en 2019 (*Bundesam für Verfassungsschutz, Verfassungsschutzbericht 2019,* www.verfassungsschutz.de/SharedDocs/publikationen/DE/2020/verfassungsschutzbericht-2019.pdf?_blob=publicationFile&v=10, 180-181).

La VSSE réalise un suivi prioritaire de la mouvance dans le cadre de ses compétences pour le suivi de la menace extrémiste (art. 7, 1° & art.8, 1°, c L.R&S) et conformément aux objectifs stratégiques 2021-2024 fixés pour le service[138] et aux accords conclus entre la VSSE et le SGRS.[139] La VSSE collecte de l'information sur les Frères musulmans, les organisations et les personnes y liées, notamment par la mise en œuvre de méthodes de renseignements ordinaires (notamment des sources humaines) mais aussi des méthodes de renseignement particulières. Elle en extrait des renseignements qu'elle diffuse aux autorités et partenaires à titre d'information et de sensibilisation. Elle suit de près la problématique et a réorienté des capacités pour l'exercice de cette mission.[140]

Le SGRS étudie uniquement la mouvance dans le cadre de l'influence que celle-ci pourrait exercer au sein de la Défense conformément à ses compétences (art.11 L.R&S) et aux plans stratégiques. Il procède à une veille active en réceptionnant les informations produites par des tiers, mais il ne collecte pas proactivement des informations sur la mouvance dans sa globalité. Au terme de l'enquête, il est difficile de se prononcer sur la qualité de la position d'information du SGRS. Il est évident que les moyens déployés pour la collecte et l'analyse sont moins importants que ceux de la VSSE dès lors que – à la différence de la VSSE qui réalise un suivi du phénomène dans sa globalité – le SGRS étudie la mouvance fériste uniquement dans le cadre de l'influence que celle-ci pourrait exercer au sein de la Défense. Néanmoins, le Comité a relevé une inadéquation entre le niveau de priorité accordé au suivi du phénomène par le SGRS et les moyens déployés par le SGRS pour la collecte et l'analyse des données. Enfin, le Comité a constaté, sur la base des informations qu'il a réceptionnées, que le SGRS n'a pas pris l'initiative de diffuser des renseignements relatifs aux Frères musulmans aux autorités ou partenaires au cours des trois dernières années.

I.12.2.2. La mouvance est-elle identifiée comme une menace pour la Belgique ?

La VSSE et la SGRS présentent des conclusions similaires. Aucune menace immédiate n'a été détectée contre une institution spécifique directement liée à la mouvance des Frères musulmans. Néanmoins, la VSSE qualifie les Frères

138 Il y est indiqué que la lutte contre le terrorisme demeure une priorité mais que la VSSE ambitionne également de porter davantage d'attention à d'autres dossiers et qu'elle en tiendra compte dans la répartition du personnel et des ressources.

139 De ces accords, il découle que pour les domaines du terrorisme, du radicalisme et de l'extrémisme, la VSSE dispose en Belgique d'une compétence générale, et le SGRS d'une compétence réduite aux aspects d'extrémisme et de terrorisme qui concernent des intérêts militaires ou qui concernent des militaires belges.

140 Le dossier fût réinvesti peu avant 2020 après que des capacités engagées jusque-là sur des dossiers de 'terrorisme et extrémisme' furent libérées.

musulmans comme un mouvement extrémiste[141] représentant une menace haute et prioritaire en ce sens qu'ils peuvent conduire à des comportements antidémocratiques, à la polarisation ou à la violation des droits fondamentaux. La VSSE précise « *Les Frères musulmans respectent les règles démocratiques et la loi, et poursuivent à court terme des objectifs supposés légitimes. Or le discours, les convictions et la vision adoptés en interne à plus long terme sont contraires au bon fonctionnement de l'ordre constitutionnel et de la démocratie* ».[142] Elle ajoute que « *Le prosélytisme ('dawa') représente le moyen le plus approprié pour y parvenir, par le biais, entres autres, de la prédication et de l'enseignement (religieux). Dans ce contexte, les Frères musulmans se considèrent comme une avant-garde élitaire appelée à rassembler et diriger différentes communautés musulmanes. Ils visent à occuper des positions sociales influentes afin de pouvoir changer la société occidentale 'de l'intérieur' et tentent également d'influencer la politique gouvernementale par différents moyens* ».[143]

Le SGRS considère que « *les Frères musulmans promeuvent par certains aspects une vision extrémiste de la religion* » et qu'ils « *représentent un danger en ce qu'ils militent activement, et souvent de façon non transparente, en faveur d'une vision identitaire de l'Islam et renforcent ainsi les clivages au sein de la société et des institutions* ». Le SGRS précise également qu'il est particulièrement attentif au risque d'entrisme des Frères musulmans au sein de la Défense. Au terme de l'enquête, le Comité ignorait cependant si le risque d'entrisme est jugé élevé par le SGRS.

I.12.2.3. Collaboration entre partenaires

I.12.2.3.1. Collaboration entre services de renseignement

L'enquête a révélé que les deux services de renseignement belges échangent avec les services de renseignement étrangers sur le phénomène de manière bilatérale et multilatérale.

Au niveau national, le Comité a pu constater que la collaboration se faisait essentiellement dans un sens, à savoir le partage d'informations de la VSSE vers le SGRS.

---

141 L'extrémisme vise « *les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux fondements de l'État de droit en ce compris le processus de radicalisation* » (art.8, 1°, c L.R&S).

142 VSSE, *Rapport annuel 2020*, p.13.

143 *Ibid.*, p.12.

I.12.2.3.2. Collaboration avec l'OCAM

Au regard de la qualification et du niveau de la menace attribués par les services de renseignement au mouvement, le Comité s'est par ailleurs intéressé – sans entrer dans les détails – à la question de savoir si l'OCAM étudiait également celui-ci.[144] Questionné à ce sujet, l'OCAM a répondu n'avoir jamais rédigé de note ou d'étude sur les Frères musulmans. L'OCAM n'identifiait par ailleurs pas de menace directe de cette mouvance pour la Belgique, et n'évoquait ni une menace à court ou moyen terme ni ne confirmait le caractère élevé de la menace contrairement à l'analyse des deux services de renseignement.

Interpellé par l'absence de vision conjointe entre, d'une part, la VSSE et le SGRS, et d'autre part, l'OCAM quant à la menace que représentent les Frères musulmans, le Comité a conclu qu'une concertation entre ces services s'avérait nécessaire. Il s'étonnait d'ailleurs qu'elle n'avait pas encore eu lieu étant donné la priorité accordée à ce dossier par la VSSE et par le SGRS.

I.12.2.4. Quelles stratégies poursuivent les services de renseignement pour endiguer la menace identifiée?

Afin de contrer la stratégie des Frères musulmans et éviter que la mouvance puisse s'installer dans une position de médiateur entre les communautés musulmanes et les autorités, la VSSE estime qu'il est capital d'investir dans la sensibilisation des autorités et administrations. Les initiatives prises et celles à venir témoignent de cette stratégie poursuivie par la Sûreté de l'État. Le service a diffusé deux notes dans un but d'information et de sensibilisation, l'une aux services de renseignement et aux services partenaires de la chaine pénale associés, et l'autre aux ministres compétents, et prévoyait d'en diffuser d'autres destinées, cette fois, à un public plus large.

Le SGRS indique que la sensibilisation des acteurs institutionnels aux tentatives d'influence par les Frères musulmans en dehors de la Belgique fait partie des objectifs des briefings donnés à ces acteurs institutionnels sur la menace terroriste et le risque lié aux mouvements radicaux religieux. Le Comité ne dispose pas d'informations supplémentaires lui permettant de se prononcer sur la quantité ou la qualité de ces briefings de sensibilisation.

À la clôture de l'enquête, le Comité a conclu qu'une concertation entre les services de renseignement et ses partenaires (l'OCAM, la Police fédérale, etc.) sur le phénomène constituait une étape cruciale pour la réussite et le renforcement de la stratégie de sensibilisation poursuivie. La sensibilisation des autorités politiques

144 L'OCAM est en effet compétent pour l'évaluation de la menace en matière d'extrémisme lorsque cette menace est susceptible de porter atteinte à la sûreté intérieure et extérieure de l'État, aux intérêts belges et à la sécurité des ressortissants belges à l'étranger ou à tout autre intérêt fondamental du pays (art.3 L.OCAM).

et des administrations sera d'autant plus efficace si elle est portée par l'ensemble de ces services qui se sont préalablement accordés sur une définition commune du phénomène et sur la menace qu'il représente pour la Belgique.

I.13. LES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION DANS LE PROCESSUS DE RENSEIGNEMENT AU SEIN DE LA DIRECTION CYBER DU SGRS ET AU SEIN DE LA VSSE

I.13.1. LE CORE BUSINESS D'UN SERVICE DE RENSEIGNEMENT

Les technologies de l'information et de la communication (TIC ou ICT en anglais) jouent un rôle de plus en plus important dans les processus de renseignement, aussi bien dans la collecte et l'analyse des informations (par exemple, les écoutes (SIGINT) ou encore les prises d'images (GEOINT)) que dans la diffusion des renseignements. L'augmentation constante des flux de données nécessite des systèmes adéquats, prêts à absorber ces flux et permettant une analyse correcte, rapide et efficace. L'environnement informatique doit donc être un outil stable et orienté vers l'avenir, et ce afin de soutenir les différents acteurs intervenant dans le cycle du renseignement. Cet environnement, aussi bien matériel ('*hardware*') que logiciel ('*software*') doit se conformer aux standards en la matière, aux bonnes pratiques IT, tout en tenant compte des nouvelles et futures évolutions technologiques[145], telles que le '*big data*'.[146]

Dans des enquêtes antérieures, le Comité permanent R avait constaté que les services de renseignement étaient confrontés à des défis majeurs dans ce domaine. Surtout pour le SGRS, il est déjà apparu par le passé que l'ICT était un point d'attention. Le Comité avait relevé que les activités de renseignement n'étaient

[145] Les organes de contrôle ont aussi un rôle important à jouer à cet égard. Voir à ce propos : K. VIETH et T. WETZLING, *Data-driven Intelligence Oversight. Recommendations for a System Update*, Stiftung NeueVerantwortung, novembre 2019, 63 p.

[146] La notion de '*big data*' fait référence à la science qui consiste à collecter et analyser de grands volumes de données dans le but de découvrir certains '*patterns*' intéressants sur la base d'une classification ('*clustering*') et d'analyses statistiques permettant ainsi de fournir une aide à la décision. Ces données sont généralement caractérisées par une variété, une vélocité et un volume importants.

pas (ou plus) suffisamment soutenues par l'ICT et que les conditions d'une bonne gestion de l'information n'étaient pas (ou plus) complètement remplies.[147] [148]

Par conséquent, le Comité permanent R a initié, en mai 2019, une 'enquête de contrôle sur les moyens informatiques utilisés par les services de renseignement belges pour la collecte, le traitement, l'analyse et la communication de l'information dans le cadre du cycle du renseignement'. L'enquête se concentrait sur les moyens informatiques spécifiquement utilisés en soutien au cycle du renseignement. Il s'agit des systèmes qui sont utilisés, par exemple, pour la collecte d'informations, ou encore des outils d'analyse et bases de données spécifiques. Le Comité permanent R ne s'est pas penché sur les outils bureautiques génériques utilisés par les services (par ex. Windows, Word, Excel, etc.), dans la mesure où ils ne sont pas spécifiques aux services de renseignement. Le Comité n'a pas non plus examiné en détail le matériel informatique ('*hardware*') à la disposition des services, à moins qu'il ne soit spécifique au service de renseignement concerné.

Le premier volet de l'enquête portait sur le SGRS, et ce en raison de l'impact de la restructuration de ce service sur les outils ICT et les méthodes de travail. L'enquête ayant été finalisée en mai 2020, les résultats ont été présentés dans le rapport d'activités de l'année 2020.[149]

Les deuxième et troisième volets concernaient la direction Cyber du SGRS et la VSSE. Les résultats de ces deux volets sont discutés dans le présent chapitre.

Les questions d'enquête principales, soumises à la VSSE et à la direction cyber du SGRS, étaient les suivantes :

- Quelles sont les technologies et quels sont les outils utilisés par le service/la direction pour soutenir les activités de renseignement?
- Dans quelle mesure les instruments sont-ils développés en interne ou fournis par des partenaires externes ?
- Les 'bonnes pratiques' usuelles (ci-après 'ITIL')[150] sont-elles appliquées correctement? (plus précisément: '*change management*', '*inventory management*', '*business continuity*', '*incident management*', '*problem management*', etc.) ?

147 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 7-14 ('II.1. Un audit au sein du service de renseignement militaire') ; *Rapport d'activités 2018*, 2-18 ('I.1. Le fonctionnement de la Direction Counterintelligence (CI) du SGRS').

148 Le rapport de la Commission d'enquête parlementaire en réponse aux attentats de Zaventem et Maelbeek recommandait également de renforcer la gestion de l'information des services de renseignement, plus particulièrement pour garder la surinformation ('infobesitas') sous contrôle. Voir 'Commission d'enquête sur les attentats terroristes du 22 mars 2016. *Doc. parl.* Chambre, 2016-2017, n° 54-1752/008, 15 juin 2017, p. 53 et 180 et suiv.

149 COMITÉ PERMANENT R, *Rapport d'activités 2020*, (I.6 « Les technologies de l'information et de la communication dans le processus de renseignement au SGRS »), 33 et suiv.

150 ITIL est l'acronyme de '*Information Technology Infrastructure Library*', qui se traduit par 'Bibliothèque pour l'infrastructure des technologies de l'information'. Il s'agit des bonnes pratiques pour la gestion des services IT les plus utilisés au monde (source: www.heflo.com/fr/blog/technologie/definition-itil).

- Existe-t-il une politique de *'business continuity plan*' (BCP) ainsi que des procédures *'disaster recovery plan*' (DRP) prévoyant les backups et sont-elles actualisées ?[151]
- Les outils sont-ils tous inscrits dans un registre des traitements de données à caractère personnel disponible pour le Comité permanent R comme prévu par la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ?

L'enquête visait à identifier les risques[152] auxquels sont confrontés les deux services de renseignement et, par le biais de recommandations, à maitriser ces risques. À partir du modèle dit 'CIA'[153], trois types de risques ont été investigués :
- *Confidendiality* : le risque de prise de connaissance de données, classifiées ou non ;
- *Integrity :* le risque de modification non autorisée de données, classifiées ou non ;
- *Availability* : le risque que les données ne soient pas disponibles, ce qui empêcherait de mener à bien les missions du service.

I.13.2. L'ENVIRONNEMENT ET L'ORGANISATION ICT DE LA DIRECTION CYBER DU SGRS

I.13.2.1. Contexte

I.13.2.1.1. Équipe et personnel

L'informatique à la direction Cyber du SGRS est gérée par une équipe dédiée à cette fin, étant donné qu'il s'agit du *core business* de cette direction.

Fin mars 2021, les effectifs ICT cyber étaient insuffisants : il y avait 80 % d'effectifs ICT engagés par rapport aux postes prévus. Le turnover du personnel,

---

151 Il existe de bonnes pratiques généralement acceptées sur la manière la plus optimale d'effectuer des sauvegardes et sur les procédures à appliquer en cas de désastre. La gestion des backups s'inscrit, tout comme les procédures DRP (*'disaster recovery plan*'), dans un *'business continuity plan*' (BCP) global.

152 Un 'risque' a été défini comme étant l'éventualité de l'existence d'une défaillance ou d'une menace plus ou moins prévisible pouvant influencer la réalisation des objectifs d'une organisation ou l'accomplissement efficiente de ceux-ci, associé à la probabilité que survienne un événement nuisible suite à cette défaillance.

153 L'utilisation du modèle dit 'CIA' est préconisée comme base d'analyse de risques selon les normes internationales ISO 270 relatives à la sécurité de l'information.

non négligeable, est principalement dû aux changements de personnel du cadre E-Gov[154], mais aussi à des départs de civils.[155]

La 'capacité serveurs' (ou ressources physiques) était suffisante au moment de l'enquête mais ne répondait pas aux ambitions à long terme du service. Des acquisitions étaient prévues, mais dépendaient des attributions budgétaires et, de ce fait, des priorités imposées au service.

Concernant le recours à la sous-traitance et aux marchés publics, la division Cyber dispose de personnel soit militaire, soit civil engagé via Selor ou mis à disposition via des contrats E-Gov Select. Étant donné que la grande majorité des logiciels provient du monde open-source, il n'y a pas de recours systématique à de la sous-traitance ou à des marchés publics d'achat de logiciels. Les développements se font, quant à eux, en interne.

I.13.2.1.2. Serveurs et réseaux

L'accès aux salles serveurs s'effectue via un mécanisme sécurisé. Des backups sont effectués régulièrement.

Une base de données de gestion de configuration (CMDB)[156] existe et est mise à jour manuellement. Il serait préférable que cette CMDB soit mise à jour automatiquement afin d'être certain de l'exactitude des données, mais également afin de détecter des anomalies.

Le monitoring est effectué par différents logiciels. Cependant, la multiplication de ces logiciels pourrait avoir un effet négatif sur la réactivité par rapport à une alerte. Il serait dès lors intéressant de se concentrer sur un logiciel central.

I.13.2.1.3. Logiciels impliqués dans la mission de renseignement

En ce qui concerne les principaux systèmes logiciels impliqués dans le cycle du renseignement, le Comité a pu constater que la division Cyber a construit toute son infrastructure en s'appuyant sur un plan stratégique à long terme et sur des domaines d'activités précis. De plus, aussi bien pour le côté matériel que logiciel, elle s'efforce de suivre les bonnes pratiques 'ITIL'.

---

154 E-gov est actif dans le recrutement et la sélection d'informaticiens spécialisés pour des services publics et institutions.

155 Le personnel de Cyber est composé de militaires, de fonctionnaires sous statut Camu et d'externes engagés via E-Gov Select.

156 Il s'agit d'une base de données – appelée Component Management DataBase (CMDB) – reprenant tous les composants ICT aussi bien les réseaux (switchs, routeurs, etc.) que les systèmes (serveurs, pc, etc.) et logiciels. Lorsque l'infrastructure informatique devient plus complexe, il est important d'exploiter une base de données de ce type car elle permet d'assurer un suivi de l'information au sein de l'environnement informatique.

Le nombre d'applications métier utilisées par la direction Cyber est conséquent et englobe tout le spectre de ses missions. Le Comité permanent R a choisi d'examiner un ensemble représentatif de ces applications.[157]

Les constats principaux sont les suivants :

- Il existe peu d'outils de type *big data* et *datamining* étant donné que les missions de Cyber (recherche et analyse de menaces, sensibilisation, protection des réseaux, etc.) ne le nécessitent pas. Cependant, certains outils disposent de mécanismes internes pouvant s'y apparenter.
- Le registre des traitements tel qu'exigé par la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel était en cours de construction pour les applications gérées par la direction Cyber.[158] Celui-ci n'était pas entièrement opérationnel, mais les adaptations à effectuer étaient mineures.
- Le Comité a pu constater que le réseau Cyber est stable et rapide. Un monitoring du réseau ainsi que de l'infrastructure en général est en place et permet de détecter les pannes.
- Les backups sont effectués régulièrement. Un processus DRP existe pour les applications principales. Celui-ci devrait être complété et mis à jour au fur et à mesure des changements effectués sur l'infrastructure.

I.13.2.1.4. Test de vulnérabilité et sécurité

Le Comité a pu constater qu'aussi bien pour les outils développés en interne que ceux acquis, une attention particulière est donnée aux aspects de sécurité et de test des applications. Celles-ci sont soumises à une série de tests automatiques et manuels, en utilisant à cet effet des produits reconnus sur le marché pour leur efficacité.

La sécurité a également été prise en compte lors de l'implémentation physique de l'infrastructure.

Enfin, les analyses d'éléments potentiellement nuisibles (tels qu'un *possible malware*) sont réalisées dans des environnements sécurisés.

I.13.2.2. Évaluation des risques

Différents points d'attention ont été énumérés pour chaque section de l'organisation ICT de la Direction Cyber du SGRS. Au cours de cette enquête, le Comité a mis

---

157 Les applications qui n'ont pas été choisies pour une démonstration sont soit similaires aux applications exposées, soit bien connues dans le monde IT. Une préférence a également été donnée aux applications développées en interne ou aux équipements nécessitant la création de scripts spécifiques par le personnel de la division Cyber.

158 Ce registre doit permettre au Comité permanent R (en tant qu'autorité de protection des données) de connaître à tout moment les traitements sur données personnelles effectués ainsi que les types de données, les durées de rétention et les responsables du traitement.

en évidence certains risques, leur probabilité ainsi que les pistes d'atténuation ('*mitigation*') afin de réduire ces risques.[159] Parmi les risques les plus importants encourus par le service, le Comité a insisté sur les points suivants :
- Le manque de personnel et la rotation dans le personnel ;
- Le renforcement de l'infrastructure physique ;
- Les outils de monitoring du réseau ;
- Les collaborations avec les firmes externes.

I.13.3. L'ENVIRONNEMENT ET L'ORGANISATION ICT DE LA VSSE

I.13.3.1. Contexte

I.13.3.1.1. Équipe et personnel

L'informatique à la VSSE est gérée par une équipe réduite. Son rôle est central, car elle offre un appui aux différents services et bureaux qui récoltent, analysent et disséminent les informations et renseignements.

En date du 1er juin 2021, les effectifs ICT étaient insuffisants. Cela est d'autant plus vrai pour le nombre de développeurs qui est extrêmement faible.

Concernant le recours à la sous-traitance et aux marchés publics, la VSSE exige une habilitation de sécurité pour les soumissionnaires. Les développements software se font souvent par des externes via des marchés publics ou sont en réalité des acquisitions. Les développements commandés via marchés publics ne donnent cependant pas nécessairement satisfaction : retard sur les délais, spécifications et technologies changeantes, dépassement des budgets, etc.

I.13.3.1.2. Serveurs et réseaux

Les salles serveurs et les systèmes de backups correspondent à des standards de sécurité élevés, sont efficaces et ont été conçus suite à une analyse de risques spécifique renouvelée régulièrement.

Une base de données de gestion de configuration (CMDB) existe et est mise à jour manuellement. Il serait préférable que cette CMDB soit mise à jour automatiquement afin d'être certain de l'exactitude des données, mais également afin de détecter des anomalies.

La gestion des configurations ainsi que le monitoring sont réalisés par un outil commercial s'intégrant à l'ensemble de l'architecture et se font sur les points

[159] La confidentialité ne permet pas de détailler cette analyse de risques dans ce rapport d'activités public.

de contrôle les plus critiques (applications, matériel, réseau, ...). Cet outil est de qualité mais pourrait être plus performant en termes de détection de problèmes en agissant de manière proactive.

I.13.3.1.3. Logiciels impliqués dans la mission de renseignement

En ce qui concerne les principaux systèmes logiciels impliqués dans le cycle du renseignement, le Comité a pu constater que la VSSE utilise une seule base de données « métier ». D'autres bases de données peuvent exister en tant que composant d'applications mais ne sont que des bases de données techniques permettant le travail de ces applications. Cette base de données métier a été régulièrement améliorée et récemment migrée vers une technologie plus moderne.

Pour la modernisation de la base de données « métier » début 2020, l'option retenue est la consolidation et la réorganisation des bases de données (de type SQL) avec l'ajout d'index de recherches. Cette méthode peu onéreuse fournit des résultats satisfaisants pour les opérations les plus courantes.

Le projet Atlas, débuté en 2015 (dossier budgétaire) et 2017 (développement) avec comme livraison finale prévue fin 2021, opte pour une autre approche, celle de l'utilisation de nouveaux types de bases de données axées sur la présence ou non d'éléments (données, tags) permettant d'établir un score de pertinence de l'information.[160] Ce projet, réalisé en collaboration avec la firme Smals, correspond aussi aux prescrits de l'analyse *big data*. Tous les composants du projet n'étaient pas encore livrés ou mis en production au terme de l'enquête. Le Comité permanent R a pu assister à une démonstration des fonctionnalités stables déjà développées. Le but de ce projet est de centraliser toutes les données de la VSSE, qu'elles proviennent ou non de l'extérieur. Il a été rapporté au Comité des problèmes concernant la prise en compte de certains besoins des utilisateurs, ainsi que des soucis de planning.[161]

Quant au registre des traitements tel qu'exigé par la Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, il était en cours d'élaboration pour les applications gérées par la VSSE. Le Comité a pu constater que celui-ci n'était pas entièrement opérationnel, mais les adaptations à effectuer étaient mineures.

Le Comité a noté que le réseau était stable et rapide. Un monitoring du réseau ainsi que de l'infrastructure en général est en place et permet de détecter les pannes.

---

160 Il s'agit de bases de données '*no-sql*' qui ont une structure beaucoup plus simple et permettent des recherches sur des contenus de fichiers ou de tags.

161 Il apparait que la communication entre l'équipe de projet et les utilisateurs clés relayant des besoins spécifiques (notamment ceux liés aux BIM) est sommaire. Le projet Atlas souffrait également de retards dans son ensemble ainsi que d'un dépassement de budget. Ces retards et dépassements ne sont pas imputables à la VSSE. La Smals a rencontré certaines difficultés lors de l'implémentation, ce qui a augmenté le temps de travail et, de ce fait, le budget nécessaire. Des choix de priorité d'implémentation ont donc dû être opérés.

Néanmoins, ce monitoring est axé sur la détection de problèmes effectifs et non sur des recherches proactives.

Les backups sont effectués quotidiennement dans le respect des règles en la matière. Un processus DRP existe pour les applications principales. Les autres applications étant des éléments de support et fonctionnant en *stand-alone* sur des postes fixes, celles-ci ne nécessitent que la documentation fournie par la firme. Le processus DRP s'inscrit bien dans le cadre d'un plan BCP plus global.

Enfin, le Comité s'est penché sur plusieurs logiciels existants ou en développement, dont le projet Tardis (également appelé Bavak), lancé fin 2016. Ce logiciel, à développer, devait permettre d'automatiser les actions en ligne sur les différents réseaux sociaux, d'extraire les informations (avec une traduction automatique de celles-ci), de les analyser et de les exporter dans un rapport. Au fil du temps, le projet s'est complexifié au vu de plusieurs fonctionnalités qui ont été ajoutées. Ce projet a finalement été abandonné début 2021 par la VSSE après avoir constaté qu'il ne répondait pas aux attentes. En effet, les comptes des réseaux sociaux sur lesquels le logiciel opérait étaient rapidement supprimés car la présence du logiciel était détectée.[162]

I.13.3.1.4. Test de vulnérabilité et sécurité

Le Comité a pu constater que des tests de sécurité sont effectués sur les programmes développés en interne. Les autres applications sont soit issues du monde *open source*, soit commerciales. Pour certaines d'entre elles, il existe une certification, tandis que pour d'autres, il n'y a pas de garantie qu'un test d'intrusion ait été effectué. Cependant, les mises à jour fréquentes sont fournies et appliquées par la VSSE.

La VSSE travaille notamment avec un réseau sécuriré non connecté à internet et soumis à une homolgation de l'ANS.

Par ailleurs, une journalisation des activités sur les applications est effectuée (logging et actions des utilisateurs), permettant de disposer d'une preuve des activités des utilisateurs.

I.13.3.2. Évaluation des risques

Une série de points d'attention ont été énumérés pour chaque section de l'organisation ICT de la VSSE. Au cours de cette enquête, le Comité a mis en évidence certains risques, leur probabilité ainsi que les pistes d'atténuation

[162] Voir à ce propos notamment la Question de S. THEMONT au ministre de l'Intérieur sur 'Le logiciel de détectage de menaces terroristes ou de radicalisation' (*Q.R.*, Chambre, 2020-2021, 3 mai 2021, n°50, p.306, Q. n°456) ; la Question de V. SCOURNEAU au ministre des Affaires étrangères et de la Défense sur 'OSINT.' (*Q.R.*, Chambre, 2019-2020, 5 août 2020, n°24, p.465, Q. n°407).

(‘*mitigation*’) afin de réduire ces risques.[163] Parmi les risques les plus importants encourus par le service, le Comité a insisté sur les points suivants :
– Le manque de personnel, et de certains profils en particulier ;
– Les communications sécurisées ;
– Le projet Atlas au regard des problèmes rapportés au Comité concernant le manque de prise en compte de certains besoins des utilisateurs ainsi que des soucis de planning (*supra*).

I.14. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D’ENQUÊTE ONT ÉTÉ EFFECTUÉS EN 2021 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2021

I.14.1. L’APPLICATION DE NOUVELLES MÉTHODES (PARTICULIÈRES) DE RENSEIGNEMENT

Le Comité s’est vu attribuer une série de possibilités de contrôle en ce qui concerne certaines méthodes ‘ordinaires’. Il s’agit notamment du contrôle de l’identification de l’utilisateur de télécommunications (art. 16/2 L.R&S), de l’accès à des données des dossiers passagers (*Passenger Name Record*, art. 16/3 L.R&S), de l’accès aux images des caméras utilisées par les services de police (art. 16/4 L.R&S), ou encore du contrôle préalable aux interceptions, aux intrusions dans un système informatique et la prise d’images animées (art. 44/3 L.R&S).

Le Comité a décidé d’étudier cette matière dans une enquête intitulée : *‘enquête de contrôle sur l’application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R’*.

En 2020, l’accent a été mis sur l’élaboration d’une méthodologie dans le cadre du contrôle de l’identification de l’utilisateur de télécommunications (art. 16/2 L.R&S), ainsi que l’accès aux données PNR (art. 16/3).

Début 2021, le volet méthodologique relatif au contrôle préalable aux interceptions, aux intrusions dans un système informatique et à la prise d’images animées (art. 44/3 L.R&S) a été finalisé.

En 2021, le Comité s’est en outre penché sur l’opérationnalisation de l’article 16/4, §2 L.R&S. Cet article régit l’extraction rétroactive des images des caméras de police par les services de renseignement. Cette disposition législative a une portée générale. Cela implique que les exigences procédurales qui y sont énoncées sont d’application pour l’extraction ciblée des images des caméras de police par un accès direct (en ligne) aux banques de données de la police concernées ainsi que pour

[163] La confidentialité ne permet pas de détailler cette analyse de risques dans ce rapport d’activités public.

l'extraction ciblée via une requête écrite adressée au service de police compétent (à savoir la Direction de l'information policière et des moyens ICT (DRI)). En raison d'une plainte DPA, l'enquête a été interrompue. La plainte a conduit à la rédaction d''Instructions de traitement du Comité permanent R (APD) concernant les extractions rétroactives par les services de renseignement des images de caméras de police sur la base de l'article 16/4, §2 L.R&S' (traduction libre).[164] Après réception et analyse des statistiques des deux services de renseignement quant à l'utilisation de cette méthode, le rapport d'enquête sera finalisé en 2022.

I.14.2 LE SUIVI PAR LA VSSE DES CONDAMNÉS POUR TERRORISME QUI ONT ÉTÉ LIBÉRÉS

En Belgique, près de 500 personnes ont été condamnées pour des faits de terrorisme entre 2015 et 2021.[165] Certains condamnés l'ont été par contumace et n'ont donc pas pu être placés en détention. Une série d'autres ont obtenu une permission de sortie de prison et ont entre-temps purgé leur peine en prison ou ont été libérés sous conditions (avant la fin de la peine) suite à une décision du tribunal d'application des peines.

Compte tenu de l'inquiétude des services de renseignement belges et européens quant à une potentielle récidive, le Comité a décidé, à la mi-2019, d'ouvrir une enquête de contrôle sur *'le suivi par les services de renseignement et de sécurité belges, d'une part des inculpés en Belgique pour infractions terroristes perpétrées en Belgique ou ailleurs et bénéficiant d'une modalité visée par la loi du 20 juillet 1990 et d'autre part, des condamnés en Belgique pour infractions terroristes qui sortent de prisons belges, soit dans le cadre d'une des modalités visées dans le cadre de la loi du 17 mai 2006, soit qui sont libérés définitivement (art. 71 de ladite loi)'*.

Le Comité a examiné la manière dont les deux services de renseignement (VSSE et SGRS) suivent cette thématique, quels moyens et quelles méthodes sont utilisés, la manière dont se déroule la coopération avec les partenaires (entre autres l'OCAM, la Direction générale des Établissements pénitentiaires, la Police fédérale et locale, etc.) et au sein de quelles structures (Local Task Forces, Groupe de travail Prisons, etc.). Enfin, les approches française et anglaise ont été étudiées à travers un benchmarking.

En 2021, face aux premiers résultats, le spectre de l'enquête a été élargi. En effet, pour comprendre l'organisation du suivi *après* la libération de ces détenus, il est apparu nécessaire de s'intéresser également au suivi par les services de renseignement et de sécurité *pendant* la détention. Il a aussi été tenu compte des évolutions législatives et des nouveaux cadres de coopération, par exemple la

164 '*Verwerkingsinstructie van het Vast Comité I (DPA) m.b.t. de door de inlichtingendiensten ingestelde retroactieve opvragingen van politionele camerabeelden gegrond op artikel 16/4, §2 W.I&V*'.

165 *Doc. parl.* Chambre 2021-22, CRIV55PLEN148, 25.

publication par l'OCAM de la Stratégie Extrémisme et Terrorisme (dite Stratégie TER) en septembre 2021. L'enquête sera finalisée au premier semestre 2022.

I.14.3. LE RISQUE D'INFILTRATION AU SEIN DES DEUX SERVICES DE RENSEIGNEMENT

Le monde du renseignement, au niveau international, a été secoué ces dernières années par une série de cas d'infiltration (et '*insider threat*'). Le Comité a pris l'initiative de lancer une enquête de contrôle sur la manière dont les deux services de renseignement gèrent le risque d'infiltration : quels risques ont été identifiés ? Quelles mesures ont été prises pour les maîtriser et pour réagir si ces risques venaient à se concrétiser ?

Plusieurs réunions de travail ont été organisées avec le SGRS et la VSSE sur la thématique 'cartographie et évaluation du risque d'infiltration au sein des services de renseignement'. À cet égard, le processus de gestion du risque, tel que repris dans la norme ISO 31000, constituait une base de départ.[166]

Prévu en 2021, le traitement des informations récoltées a pris du retard, principalement en raison de la crise sanitaire et de son impact sur les effectifs du Comité ainsi que de la prise en charge de dossiers urgents (l'affaire Conings, *supra*).

I.14.4. MENACES ÉVENTUELLES POUR LE POTENTIEL ÉCONOMIQUE ET SCIENTIFIQUE (PRISM/PES) : ENQUÊTE DE SUIVI

En 2016, une enquête de contrôle relative à la protection du potentiel économique et scientifique, dans la foulée desdites 'révélations de Snowden', a été finalisée.[167] Ces révélations ont notamment donné un aperçu de l'existence du programme PRISM, au travers duquel la National Security Agency (NSA) américaine récoltait des (méta)données de télécommunication. Elles ont également révélé les opérations de renseignement montées par les services américains, mais aussi britanniques, contre certaines institutions internationales et structures de coopération (ONU, UE et G20). Des pays dits 'amis' étaient eux aussi visés. L'enquête portait sur les implications éventuelles des programmes étrangers sur la protection du potentiel économique et scientifique du pays. Il s'agissait de vérifier si les services de renseignement belges étaient attentifs à ce phénomène ; s'ils avaient détecté une menace réelle ou éventuelle contre le potentiel économique et scientifique belge ; s'ils avaient informé les autorités compétentes et leur avaient suggéré des mesures

166 www.iso.org:fr/iso-31000-risk-management.html

167 COMITÉ PERMANENT R, *Rapport d'activités 2016*, 52 et suiv.

de protection et, enfin, s'ils disposaient de moyens suffisants et adéquats pour suivre cette problématique. Le Comité a par ailleurs examiné les conséquences du programme PRISM et/ou de systèmes analogues sur le potentiel économique et scientifique du pays.

Fin novembre 2019, la Commission parlementaire de suivi a demandé au Comité permanent R de reprendre l'enquête de contrôle et de l'actualiser. En 2020, après des premiers devoirs d'enquête, en particulier la collecte et l'analyse de sources ouvertes, il a été décidé de fusionner cette enquête avec l'enquête de contrôle sur l'opération Rubicon (Voir I.14.5). En 2021, le Comité a rencontré et interrogé les deux services de renseignement à ce sujet. Des questions ont également été posées au Centre pour la Cybersécurité Belgique (CCB). Après l'analyse de ces réponses, la rédaction du rapport a toutefois été interrompue par la prise en charge d'enquêtes de contrôle urgentes et prioritaires, en particulier sur l'affaire Conings (Voir I.9). Les résultats de l'enquête sont attendus pour début 2022.

I.14.5. ESPIONNAGE VIA DU MATÉRIEL DE CRYPTAGE : L'OPÉRATION RUBICON

Mi-février 2020, des révélations ont été faites sur l''Operation Rubicon'[168], c'est-à-dire l'opération de renseignement par laquelle les services de renseignement américains et allemands ont, des décennies durant, écouté des communications cryptées émanant d'autorités dans des dizaines de pays, en utilisant la société suisse Crypto AG comme couverture.[169] Les Pays-Bas, la France, la Suède et le Danemark (les 'pays Maximator'), entre autres, étaient '*cognescenti*', c'est-à-dire initiés aux détails cryptologiques de certains appareils. La Belgique, "*précieuse pour les éclaircissements que ses rapports apportaient sur les événements diplomatiques*" (traduction libre)[170] et surtout intéressante comme centre diplomatique de l'OTAN et de ce qui était à l'époque la Communauté économique européenne, aurait notamment été visée.

---

168 La revue *Intelligence and National Security* (Volume 35, August 2020, Issue 5) y a consacré un numéro thématique. Voir notamment : R. ALDRICH et al., 'Operation Rubicon: sixty years of German-American success in signals intelligence'; M.J. DOBSON, 'Operation Rubicon: Germany as an intelligence 'Great Power" et B. JACOBS, 'Maximator: Europan signals intelligence cooperation from a Dutch perspective'.

169 Les rapports d'évaluation des services de renseignement américains et allemands ont été publiés par la chaîne de télévision allemande ZDF et le Washington Post. La plateforme de recherche néerlandaise Argos a pu consulter les rapports, qui ont notamment été repris par De Tijd (L. BOVÉ, *De Tijd*, 13 février 2020, ('Geheime documenten onthullen spionage van België door CIA en Duitse BND')).

170 *«waardevol voor de verheldering die zijn rapporten bood over diplomatieke gebeurtenissen ».*

Le Comité a décidé d'ouvrir une enquête de contrôle, tentant d'apporter une réponse à des questions telles que[171] : dans quelle mesure les services de renseignement belges étaient-ils au courant (ou dans quelle mesure devaient-ils l'être) de ces opérations compte tenu de leurs missions légales ? Des renseignements ont-ils été recueillis à ce propos ou cela n'a-t-il pas été jugé souhaitable ? Mais plus important encore : les services offrent-ils actuellement une protection suffisante en la matière ? Des analyses de risques ont-elles été effectuées ? En cas d'utilisation avérée de matériel du cryptage, quelles mesures de précaution ont alors été prises ? Comment cette problématique de cryptage est-elle gérée aujourd'hui ? Fin septembre 2020, il a été décidé de fusionner cette enquête avec l'enquête de suivi PRISM/PES (Voir I.14.4).

I.14.6. CAPACITÉS DE RENSEIGNEMENT (SUPPLÉMENTAIRES) À L'ÉTRANGER POUR LES SERVICES DE RENSEIGNEMENT BELGE ?

Compte tenu de la mission de renseignement décrite par le législateur, les informations pertinentes pour les services de renseignement se trouvent à la fois en Belgique et à l'étranger. Par conséquent, une enquête de contrôle a été ouverte en 2020 sur 'les capacités de renseignement (supplémentaires) des services de renseignement belges à l'étranger'. Cette enquête poursuit divers objectifs :

- Vérifier si la VSSE et/ou le SGRS procèdent actuellement à un recueil opérationnel d'informations à l'étranger, et dans l'affirmative, sous quelle forme et par le biais de quelles activités de renseignement ;
- Examiner les activités menées à l'étranger sous l'angle du cadre réglementaire en vigueur ;
- Vérifier si les services ont besoin de moyens supplémentaires, parmi lesquels des moyens juridiques (en d'autres termes, des compétences d'enquête) pour pouvoir recueillir des informations à l'étranger.

En 2021, après analyse du cadre juridique pertinent, la VSSE et le SGRS ont été interrogés sur les éventuelles activités de renseignement qu'ils mènent à l'étranger. En raison d'autres priorités et de l'impact de la crise sanitaire sur les effectifs du Comité, le traitement de leurs réponses a été interrompu. L'enquête sera finalisée courant 2022.

---

171 Mais par exemple aussi : quelle est la signification/valeur de la notion d'État ami' dans le contexte des services de renseignement et dans quelle mesure cette notion détermine-t-elle la position de nos propres services de renseignement ?

I.14.7. CONTRÔLE DES FONDS SPÉCIAUX : ENQUÊTE DE SUIVI

À l'instar de tout service public, les services de renseignement se voient également allouer des fonds publics pour exercer leurs missions légales. La règle normale pour l'utilisation de ces fonds doit être une transparence parfaite et un contrôle total. Cependant, comme certaines tâches de la VSSE et du SGRS sont imprévisibles ou doivent être tenues secrètes, une partie de leur budget échappe à cette 'règle normale'. Cette partie est mieux connue sous le nom de 'fonds spéciaux'. Bien que le montant de ces fonds soit intégré dans le budget alloué aux services, des règles particulières s'appliquent à leur gestion, leur utilisation et leur contrôle. En 2015[172], le Comité s'est notamment attaché à déterminer la nature de ces 'fonds spéciaux', leur montant et leur répartition. Il a également contrôlé l'utilisation des moyens et les interactions entre ces 'fonds spéciaux' et les budgets dits 'normaux'. Enfin, le Comité s'est penché sur le cadre réglementaire et a examiné les mécanismes de contrôle, et ce tant en interne (au sein des services) qu'en externe (Cour des comptes, Inspection des Finances, Comité permanent R, etc.). Différentes recommandations ont été formulées.

Depuis 2018 (VSSE) et 2020 (SGRS), la Cour des comptes a exprimé son intention de réaliser un contrôle périodique de ces fonds. Dans ce contexte, la Cour des comptes a pu recourir à une assistance technique, telle que proposée par le Comité permanent R.[173] Le Comité pouvait à son tour « *exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds* ». Une enquête de suivi a été ouverte fin 2020 sur la gestion, l'utilisation et le contrôle des fonds spéciaux. Interrompus en raison de la prise en charge de dossiers prioritaires en 2021, les devoirs d'enquête reprendront en 2022.

172 COMITÉ PERMANENT R, *Rapport d'activités 2015*, 11-16 ('La gestion, l'utilisation et le contrôle des fonds spéciaux').

173 *« Ce contrôle sera périodique et comportera, outre un examen des processus et un contrôle de caisse, un contrôle formel réalisé par sondage et portant sur l'existence des pièces justificatives conformes aux instructions et approuvées par les fonctionnaires compétents. Le contrôle ne portera pas sur le bien-fondé ou la bonne gestion des opérations sous-jacentes et sera mis en œuvre, dans le respect des missions du SGRS, par des auditeurs disposant de l'habilitation de sécurité requise ».*

I.14.8. ENQUÊTE DE CONTRÔLE SUR LA DÉTECTION ET LE SUIVI PAR LES SERVICES DE RENSEIGNEMENT DES ORGANISATIONS PHILOSOPHIQUES A VISÉES POLITIQUES CONTRAIRES À L'ORDRE DÉMOCRATIQUE

En juillet 2021, le Comité permanent R a reçu la demande de la Présidente de la Chambre, d'ouvrir une enquête portant sur « *la manière dont les services de renseignement s'intéressent aux activités des mouvements sectaires à obédience religieuse ayant des visées politiques (autres mouvements salafistes politiques, Opus Dei, mouvement Civitas, etc.)* ».[174]

Cette demande fait suite à deux enquêtes réalisées par le Comité, à savoir l'enquête de contrôle sur la manière dont la Sûreté de l'État a assuré le suivi de la commissaire du gouvernement Ihsane Haouach[175] et l'enquête de contrôle relative au suivi par les services de renseignement de la mouvance des Frères musulmans.[176]

Fin 2021, après clarifications et en accord avec la Présidente de la Chambre, le spectre de l'enquête a été adapté. L'enquête sera réalisée en 2022.

174 Courrier du 19 juillet 2021 de la Présidente de la Chambre, E. TILLIEUX, au Président du Comité permanent R.

175 Voir 'I.11. Le suivi d'une commissaire du gouvernement par la VSSE' (*supra*).

176 Voir 'I.12. Une attention renouvelée pour les Frères musulmans' (*supra*).

CHAPITRE II.
LE CONTRÔLE DES MÉTHODES PARTICULIÈRES ET DE CERTAINES MÉTHODES ORDINAIRES DE RENSEIGNEMENT

Le Comité permanent R est tenu de faire preuve de transparence quant à l'utilisation des 'méthodes de recueil de données' (MRD) par les services de renseignement : l'article 35 §1, 1° de la Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (L.Contrôle) – tel que modifié par l'article 25 de la Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité (Loi MRD)[177] – précise que dans son rapport d'activités, le Comité « *consacre une attention spécifique aux méthodes spécifiques et exceptionnelles de recueil de données, telles qu'elles ont été visées dans l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité […]* ». Par ailleurs, conformément à l'article 35 §2 L.Contrôle, le Comité doit faire annuellement rapport à la Chambre « *sur l'application de l'article 16/2 et de l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité […].*[178] *Le rapport indique le nombre d'autorisations accordées, la durée des méthodes exceptionnelles de recueil de données, le nombre de personnes concernées et, le cas échéant, les résultats obtenus.*[179] *Il précise également les activités du Comité permanent R.* »

Le présent chapitre détaille les chiffres de la mise en œuvre par la Sûreté de l'État (VSSE) et par le Service Général du Renseignement et de la Sécurité (SGRS) des méthodes spécifiques et exceptionnelles (regroupées en 'méthodes particulières

177 Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, *M.B.* 10 mars 2010.

178 Une copie de ce rapport est également adressée aux ministres de la Justice et de la Défense ainsi qu'à la Sûreté de l'État et au Service Général du Renseignement et de la Sécurité, qui ont la faculté d'attirer l'attention du Comité permanent R sur leurs observations (art.35 § 2 L.Contrôle).

179 Un rapport spécifique sur les 'résultats obtenus' n'est pas à l'ordre du jour pour l'instant. Le Comité est conscient qu'il s'agit d'une mission importante : *"there will be an important job for oversight bodies to measure the effectiveness of these new techniques while nonetheless providing public assurance that any new powers or resources are proportionate to the threat and not abused"*, in: I. LEIGH and N. WEGGE, *Intelligence oversight in the twenty-first century. Accountability in a changing world*, Routledge, 2020, 18.

de renseignement') ainsi que de certaines méthodes ordinaires, pour lesquelles le Comité s'est vu confier une mission de contrôle supplémentaire (lesdites 'méthodes ordinaires plus').

La manière dont le Comité a assuré sa mission de contrôle (juridictionnel) sur ces méthodes y est également présentée. Il y a plusieurs années, le Comité a fait le choix de publier sa jurisprudence dans les rapports d'activités annuels. Ces décisions, contenant pour certaines des éléments classifiés, ne sont pas publiées dans leur intégralité. Y sont mentionnés uniquement les éléments juridiques pertinents ainsi que les faits essentiels. Une telle transparence est (assez) unique. L'expérience des années passées a pu démontrer que pareille démarche est possible sans compromettre le fonctionnement des services de renseignement.

Notons également que le Comité peut être saisi en sa qualité d''auteur d'avis préjudiciels' (articles 131*bis*, 189*quater* et 279*bis* CIC).[180] Le cas échéant, le Comité rend un avis sur la légalité des méthodes spécifiques ou exceptionnelles ayant fourni des renseignements qui sont utilisés dans le cadre d'une affaire pénale. Jusqu'à présent, il s'agit d'un concept resté théorique, qui n'a donc pas été concrétisé au cours de la décennie écoulée.[181]

II.1. LES CHIFFRES RELATIFS AUX MÉTHODES PARTICULIÈRES ET À CERTAINES MÉTHODES ORDINAIRES

II.1.1. TENDANCES GÉNÉRALES

II.1.1.1. Quant aux méthodes particulières de renseignement à la VSSE et au SGRS

Le législateur a opté, à l'époque, pour une subdivision claire entre les différentes méthodes de recueil de données, désignées dans la loi comme méthodes ordinaires, spécifiques ou exceptionnelles. Elles sont (ou plutôt devraient être) classées selon leur degré d'ingérence (croissant) dans la vie privée et disposent chacune d'un cadre et d'un mécanisme de contrôle qui leur sont propres. La sévérité du contrôle

180 À ce propos, Voy. COMITÉ PERMANENT R, *Rapport d'activités 2010*, p.59.

181 La décision de demander un avis appartient aux juges d'instruction et aux juges pénaux. Au sujet de son application limitée, voir VANDERBORGHT, J., '*If you torture the data long enough, it will confess. Enkele cijfers over de inzet van bijzondere inlichtingenmethoden*', in VANDERBORGHT, J. (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, Intersentia, Antwerpen, 2020, 25.

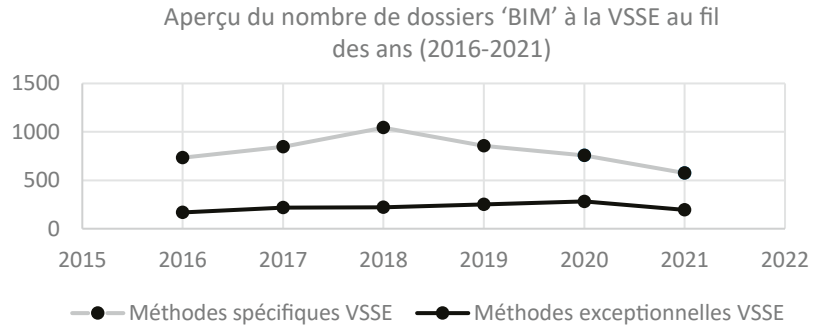
est proportionnelle au degré d'intrusion de la méthode utilisée.[182] L'objectif était d'éviter que les services recourent d'emblée aux mesures les plus lourdes.

Entre le 1er janvier et le 31 décembre 2021, 1823 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 1570 par la VSSE (1220 spécifiques et 350 exceptionnelles) et 253 par le SGRS (166 spécifiques et 87 exceptionnelles).[183]

---

182 De l'avis de certains experts, cette répartition semble trop théorique et ne tient pas suffisamment compte de la réalité. Voir par ex. W. VAN LAETHEM, 'Enkele reflecties over tien jaar BIM-controle door het Vast Comité I', in VANDERBORGHT, J. (ed.), *o.c.*, 70-72. Le Comité est du même avis et a cité, à titre d'exemples, les articles 16/3 L.R&S (collecte et traitement des données des passagers) et 16/4 L.R&S (collecte et traitement des images enregistrées par les caméras des services de police). Bien que ces pouvoirs d'investigation soient qualifiés de méthodes ordinaires, leur degré d'intrusion dans la vie privée et dans la protection des données est souvent plus important que certaines méthodes de renseignement spécifiques, voire exceptionnelles. C'est certainement le cas de l'utilisation des images caméras lorsque ce sont des caméras intelligentes ou des logiciels intelligents qui sont utilisés, tels que le système ANPR. Voir COMITÉ PERMANENT R, Avis n°001/CPR/2021 du 12 juillet 2021 (modifications Loi Renseignements), consultable sur www.comiteri.be. Les services de renseignement, pour leur part, soulignent la nécessité de maintenir le principe d'égalité avec les méthodes particulières de recherche.

183 Les services de renseignement s'appuient sur d'autres méthodes pour la comptabilisation. La VSSE calcule en nombre de dossiers 'BIM', un dossier pouvant contenir plusieurs méthodes. Une tendance similaire est néanmoins observée :

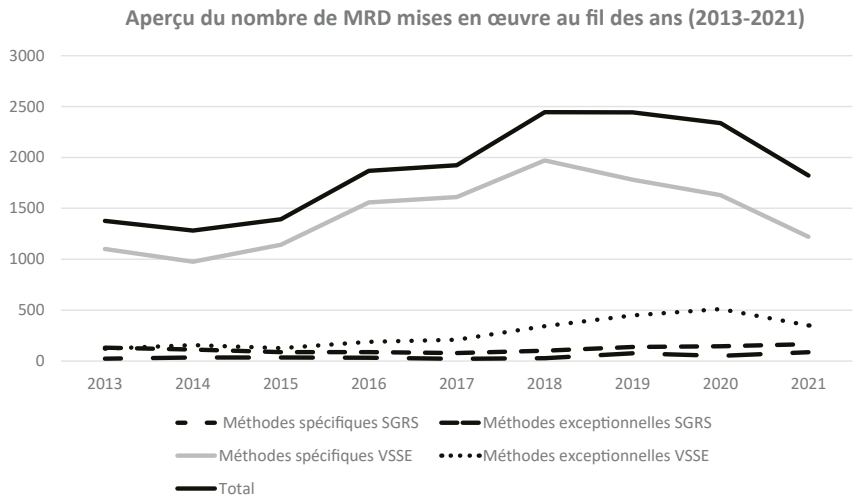


Le SGRS procède lui aussi d'une autre manière, puisqu'il comptabilise les méthodes par article sans subdivisions entre les différents paragraphes au sein d'un article comme le fait le Comité. Dans les chiffres du SGRS figurent également l'ensemble des demandes introduites en interne (même celles ayant fait l'objet d'un refus en interne). Enfin, une méthode est comptabilisée dans l'année où sa demande a été introduite, indépendamment de la date à laquelle elle a été autorisée.

Le tableau ci-dessous établit une comparaison avec les chiffres des années précédentes.

	SGRS		VSSE		TOTAL
	Méthodes spécifiques	Méthodes exceptionnelles	Méthodes spécifiques	Méthodes exceptionnelles	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445
2019	138	76	1781	449	2444
2020	146	51	1629	511	2337
2021	166	87	1220	350	1823

Cela donne schématiquement :



Après une augmentation constante du nombre de MRD mises en œuvre jusqu'en 2018 et une stagnation en 2019-2020, on remarque une diminution significative en 2021.[184] Une nuance s'impose car en divisant les chiffres par service, on constate pour 2021 une nette augmentation (environ 30 %) du nombre de MRD mises en œuvre par le SGRS. On note, à l'inverse, une nette diminution (environ 28 %) à la VSSE (*infra*).

[184] À noter que plusieurs *targets* (tels que des personnes, des organisations, des lieux, des objets, des moyens de communication, etc.) peuvent être visés dans une même autorisation.

Nonobstant un léger mouvement de rattrapage enregistré du côté du SGRS, la VSSE continue de se tailler la part du lion, avec 86 % des méthodes mises en œuvre. Bien que les deux services aient été dotés des mêmes compétences, leurs missions sont à ce point différentes (par exemple l'importance des missions du SGRS à l'étranger) que l'on ne peut guère tirer d'enseignements d'une comparaison entre les deux services. Une autre raison invoquée par les services pour expliquer ces différences, est notamment le fait que les MRD mises en œuvre par la Plateforme commune contre-terrorisme (Plateforme CT) concernant la menace terroriste sont comptabilisées dans les chiffres de la VSSE.

Une ventilation de ces chiffres permet de constater une poursuite de l'augmentation, constatée l'an dernier, du nombre de méthodes spécifiques mises en œuvre par le SGRS, passant de 146 à 166. Le nombre de méthodes exceptionnelles mises en œuvre connaît une forte augmentation, passant de 51 en 2020 à 87 en 2021.[185] Selon le SGRS, ce phénomène s'explique par la restructuration interne de la cellule BIM, qui implique une prestation de services plus efficace[186], et le recrutement de *case-managers* supplémentaires, avec pour conséquence davantage de '*request for operations*'. En termes de contenu, l'affaire Jürgen Conings (cf. *supra*) et les ramifications de ce dossier (extrême droite dans l'armée) ont eu un impact majeur. Mais abstraction faite de l'affaire précitée, une augmentation considérable du nombre de MRD mises en œuvre est encore constatée par le SGRS.

À la VSSE, on observe la tendance inverse, c'est-à-dire une diminution remarquable de l'utilisation des méthodes spécifiques (de 1629 en 2020 à 1220 en 2021) ainsi qu'une baisse de l'utilisation des méthodes exceptionnelles (de 511 en 2020 à 350 en 2021, soit une diminution de plus de 30 %). Selon le VSSE, plusieurs raisons expliquent cette tendance baissière : le nombre de méthodes dites « ordinaires plus » s'est inscrit à la hausse (principe des vases communicants) ; le service a connu un recrutement considérable, suivi d'une formation intensive accaparant de nombreuses forces vives et ayant impliqué une diminution du nombre d'agents disponibles pour les enquêtes ; les conséquences persistantes des mesures COVID, etc.

---

185 Ce qui est important à souligner dans ce contexte, c'est que le SGRS dispose également de compétences particulières pour le recueil d'informations, telles que réglées dans les articles 44 et suiv. L.R&S. Voir à ce propos 'Chapitre III. Le contrôle des interceptions à l'étranger, des prises d'images et des intrusions dans des systèmes informatiques'.

186 La procédure de soumission des MRD au SGRS resterait néanmoins sensiblement plus lourde (d'un point de vue administratif) qu'à la VSSE, ce qui donnerait lieu, selon le SGRS, à une forme d''autocensure'.

II.1.1.2. Quant aux méthodes ordinaires plus, en particulier l'article 16/2 L.R&S

L'identification de l'abonné ou de l'utilisateur habituel d'un service ou d'un moyen de télécommunication (par ex. le numéro de GSM ou l'adresse IP[187]) est considérée comme une méthode ordinaire, dans la mesure où elle est effectuée par une réquisition auprès des opérateurs ou des fournisseurs de télécommunication ou par un accès direct à leurs fichiers clients.[188] L'article prévoit l'obligation pour les services de renseignement de tenir un registre de toutes les identifications réquisitionnées et de toutes les identifications obtenues par accès direct.[189] Il stipule également que le Comité doit recevoir une liste mensuelle des identifications réquisitionnées et une liste de chaque accès.

En ce qui concerne cette méthode, la diminution déjà observée se poursuit. On dénombre une dizaine de réquisitions de moins au SGRS par rapport à 2020, et plus de 1000 réquisitions de moins du côté de la VSSE.[190]

	Réquisitions par le SGRS	Réquisitions par la VSSE
2016	216	2203
2017	257	4327
2018	502	6482
2019	442	5674
2020	433	5123
2021	420	4080

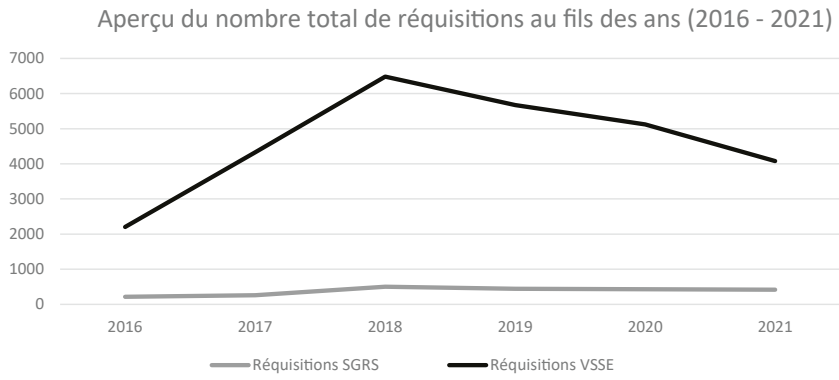
187 À compter de 2022, le nombre de réquisitions sera réparti entre les 'réquisitions IP' et les 'autres réquisitions'.

188 Lorsque l'identification est réalisée à l'aide d'un moyen technique (et donc pas via une réquisition auprès d'un opérateur) la collecte demeure une méthode spécifique (art. 18/7 § 1er L.R&S).

189 La possibilité offerte aux services de renseignement (par l'introduction du dernier alinéa de l'article 16/2 §1 L.R&S) de demander des identifications via un accès direct aux fichiers des clients d'un opérateur ou d'un fournisseur de télécommunications n'a pas encore été mise en œuvre.

190 Dans le cadre de son pouvoir général de contrôle, le Comité en a analysé les raisons. Les résultats ont été inclus dans l'"*enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R*" (cf. I.14.1. 'L'application de nouvelles méthodes (particulières) de renseignement').

Cela donne schématiquement :



Un certain nombre de commentaires importants s'imposent. On peut déduire du tableau ci-dessus qu'après la mise en œuvre des modifications de la loi en 2016 et 2017, le nombre de réquisitions a atteint un pic en 2018. Bien que le nombre de demandes soit une indication de la charge de travail, on ne peut rien en déduire concernant l'augmentation ou la diminution du nombre de 'sélecteurs' visés (numéros de téléphone, noms, adresses IP...). Alors que le nombre de réquisitions pour le service de renseignement militaire, par exemple, a diminué (de 433 en 2020 à 420 en 2021), le nombre de sélecteurs a remarquablement augmenté : de 5334 en 2020 à 6385 en 2021 (soit une augmentation de près de 20 %). Pour la VSSE, malgré la diminution du nombre de réquisitions, le nombre de sélecteurs est resté relativement stable (31.730[191] en 2021 contre 31.204 en 2020).

Par ailleurs, les deux services ne font aucune distinction dans le décompte entre l'article 16/2 § 1er L.R&S et l'article 16/2 § 2 L.R&S[192] (identification du titulaire d'une carte prépayée).

[191] À la VSSE, le nombre d'identifications d'adresses IP était de 4 925 (3 188 en 2020). Les autres identifications s'élevaient à 26 805 (28 016 en 2020).

[192] L'article 16/2 L.R&S stipule : '*§ 2 Les services de renseignement et de sécurité peuvent, dans l'intérêt de l'exercice de leurs missions, requérir le concours d'une banque ou d'une institution financière pour procéder à l'identification de l'utilisateur final d'une carte prépayée visée dans l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques, sur la base de la référence d'une transaction bancaire électronique qui est liée à la carte prépayée et qui a préalablement été communiquée par un opérateur ou un fournisseur en application du paragraphe 1er.*'

II.1.1.3. Les conséquences de l'annulation de la Loi sur la conservation des données ?[193]

Par son arrêt du 22 avril 2021, la Cour constitutionnelle a annulé la loi sur la conservation des données (loi *data retention*).[194] La Cour a jugé que la conservation généralisée et indifférenciée des données relatives aux communications électroniques viole le droit au respect de la vie privée et à la protection des données personnelles. Cet arrêt constitue un obstacle notamment pour les enquêtes de renseignement.

Il va sans dire que les données d'identification, de trafic et de localisation jouent un rôle important dans le travail de renseignement. C'est une des raisons pour lesquelles l'obligation de conservation des données a été créée à l'article 126 de la Loi relative aux communications électroniques (LCE).[195] Cet article imposait aux fournisseurs de services de téléphonie publique et aux opérateurs de réseaux publics de communications électroniques de conserver ces données pendant douze mois.[196]

Concrètement, la Cour constitutionnelle a jugé que la conservation des données doit désormais être l'exception ; la conservation ciblée des données doit toujours être proportionnée à l'objectif poursuivi.

Interrogés sur les implications de cet arrêt sur le fonctionnement des deux services de renseignement en 2021, tant le SGRS que la VSSE ont déclaré qu'elles étaient négligeables et qu'aucune conséquence majeure n'était observée à ce stade.

Entre-temps, le gouvernement a déposé un projet de loi qui vise essentiellement à rétablir un cadre juridique conforme à la jurisprudence en matière de conservation des « métadonnées » ou « données de trafic et de localisation » par les opérateurs.[197] Le gouvernement exprime le souhait que cette loi réparatrice entre en vigueur avant l'été 2022.[198]

---

193 Voir le chapitre VI.3. 'Avis relatif à la rétention des données'.

194 Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, *M.B.* 18 juillet 2016. Communiqué de presse de la Cour constitutionnelle, "La Cour constitutionnelle annule l'obligation de la conservation généralisée et indifférenciée des données relatives aux communications électroniques", 22 avril 2021.

195 Loi du 13 juin 2005 relative aux communications électroniques, *M.B.* 20 mai 2005, 28070.

196 L'obligation de conservation de données vise non seulement le trafic téléphonique, mais aussi divers types de trafic Internet.

197 Projet de loi du 17 mars 2022 relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités, *Doc. parl.*, Chambre, 2021-2022, n°55-2572/001.

198 Question de E. GILISSEN au ministre des Télécommunications relative à 'la loi sur la conservation des données' (*C.R.I.*, Chambre 2021-2022, 9 mars 2022, CRIV55 COM715, 11).

II.1.2. MÉTHODES UTILISÉES PAR LE SGRS

II.1.2.1. MÉTHODES ORDINAIRES 'PLUS'

Identification de l'abonné ou de l'utilisateur habituel de télécommunications

La diminution du nombre de réquisitions, précédemment observée, se poursuit. On dénombre une dizaine de réquisitions de moins au SGRS par rapport à 2020 (*supra*).

Accès aux données PNR

À côté de l'identification de l'abonné ou de l'utilisateur habituel de télécommunications comme méthode ordinaire plus, une loi a introduit début 2017,[199] la possibilité pour les services de renseignement d'avoir accès aux informations détenues par l'Unité d'information des passagers (BELPIU), et ce par le biais de recherches ciblées (art. 16/3 L.R&S et art. 27 de la Loi du 25 décembre 2016 relative au traitement des données des passagers (Loi PNR).[200] Le Comité est informé de l'utilisation de cette méthode et peut l'interdire le cas échéant.[201]

La réglementation PNR permet également de réaliser ce que l'on appelle une 'évaluation préalable', qui consiste à vérifier automatiquement la correspondance entre les données PNR et les listes ou fichiers de noms des services de renseignement et à envoyer des informations sur la base de '*hits*' validés (art. 24 Loi PNR). Le nombre de recherches effectuées dans les données PNR est resté stable en 2021 (28 en 2020, 29 en 2021). Plus de la moitié concernait des dossiers liés à la menace d'"espionnage".

Utilisation d'images enregistrées par les caméras des services de police

La Loi du 30 novembre 1998 organique des services de renseignement et de sécurité a été adaptée par la Loi du 21 mars 2018 (*M.B.* 16 avril 2018) pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des

199 Loi du 25 décembre 2016 (*M.B.* 25 janvier 2017).

200 La Cellule BIM du SGRS n'intervient pas ici ; la mise en œuvre s'opère via le membre du personnel du SGRS détaché au sein de BELPIU.

201 À l'inverse des méthodes reprises à l'article 16/2 L.R&S, il n'est pas prévu qu'un rapport doive être rédigé à l'intention du Parlement, l'article 35 § 2 L. Contrôle n'ayant pas été adapté. Suivant la suggestion émise par la Commission de suivi, le Comité a décidé de reprendre ces chiffres dans son rapport annuel et de ne pas attendre une éventuelle modification de la loi.

services de police. Une nouvelle méthode ordinaire a été introduite à cet effet (art. 16/4 §2 L.R&S).[202] [203]

Le SGRS a utilisé cette méthode en 2021 (pour la première fois) à quinze reprises. Trois des quinze demandes concernaient des demandes pour une période de moins d'un mois.

Les chiffres

Méthodes ordinaires plus (SGRS)	Nombre d'autorisations 2020	Nombre d'autorisations 2021
Identification de l'abonné ou de l'utilisateur habituel de télécommunications	433	420
Recherches ciblées de données PNR	28	29
Utilisation d'images enregistrées par les caméras des services de police[204]	Pas en vigueur	15

202 Cette même loi a étendu la possibilité d'observation spécifique et exceptionnelle existante (articles 18/4 § 3 et 18/11 § 3 L.R&S).

203 Début 2019, le Conseil des ministres a approuvé un projet d'arrêté royal en application de l'art. 16 § 4 L.R&S, qui a été soumis à l'avis du Comité permanent R. Cet avis 002/CPR-ACC/2019 du 9 avril 2019 peut être consulté sur le site internet du Comité (www.comiteri.be).

204 Le champ d'application de l'article 16/4 L.R&S (par ex. en ce qui concerne les consultations de la Direction de l'information policière et des moyens ICT (DRI) de la Police fédérale) fait l'objet d'une analyse juridique (2021).

II.1.2.2. Les méthodes spécifiques

Le tableau ci-dessous reprend les chiffres relatifs à l'application des méthodes spécifiques par le SGRS. On en distingue sept.

Méthodes spécifiques (SGRS)	Nombre d'autorisations 2020	Nombre d'autorisations 2021
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)[205]	6	12
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	0	0
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	2	0
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 §1, 1° L.R&S)	2	6

[205] La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/4 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées, n'a pas encore été opérationnalisée.

Méthodes spécifiques (SGRS)	Nombre d'autorisations 2020	Nombre d'autorisations 2021
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 §1, 2° L.R&S)	0	0
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 §1, 1°L.R&S)	69	75
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 §1, 2° L.R&S)	67	73
TOTAL	**146**	**166**

En ce qui concerne la mise en œuvre des méthodes spécifiques, ce sont le repérage des données d'appel d'un trafic de communications électroniques' (art. 18/8, §1, 1° L.R&S) et la 'prise de connaissance de données de localisation d'un trafic de communications électroniques' (art. 18/8, §1, 2° L.R&S), tous deux assortis d'une réquisition du concours d'un opérateur, qui se hissent distinctement en tête du classement (148 des 166 méthodes spécifiques mises en œuvre). Il y a deux fois plus d'observations dans des lieux accessibles au public à l'aide d'un moyen technique qu'en 2020, passant de 6 en 2020 à 12 en 2021.

Selon le SGRS, un certain nombre de méthodes n'ont pas été utilisées en raison d'un manque de personnel. Il a par ailleurs été constaté par le SGRS qu'un certain nombre de méthodes spécifiques n'étaient pas suffisamment connues du personnel et, par conséquent, pas assez utilisées. Pour y remédier, des briefings internes ont été organisés début 2022.

II.1.2.3. Les méthodes exceptionnelles

Dans le cadre de ses missions visées aux articles 11, § 1er, 1° à 3° en 5°, et § 2 L.R&S, le SGRS peut mettre en œuvre différentes méthodes exceptionnelles :

Méthodes exceptionnelles (SGRS)	Nombre d'autorisations 2020	Nombre d'autorisations 2021
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)[206]	2	3
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	0	2
Recourir à une personne morale visée à l'article 18/3, § 1er L.R&S afin de collecter des données	0	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	0	2
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	6	8
S'introduire dans un système informatique (article 18/16 L.R&S)	4	14
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	39	60
TOTAL	**51**	**89**

Comme indiqué, une forte augmentation du nombre de méthodes exceptionnelles mises en œuvre est constatée. La forte augmentation en pourcentage (quasi un doublement) du nombre de méthodes exceptionnelles mises en œuvre par le SGRS s'explique principalement par l'augmentation du nombre d'intrusions dans un système informatique (18/16 L.R&S) (passant de 4 en 2020 à 14 en 2021) et du nombre d'interceptions, de prises de connaissance et d'enregistrements de communications (art. 18/17 L.R&S) (de 39 en 2020 à 60 en 2021). La méthode exceptionnelle consistant à recourir à une personne morale afin de collecter des

[206] La Loi du 21 mars 2018 (*M.B.* 16 avril 2018) a ajouté un nouveau paragraphe à l'article 18/11 L.R&S pour permettre aux services de renseignement d'utiliser des images enregistrées par les caméras des services, et ce afin d'effectuer des observations en temps réel. Cette méthode, qui nécessite un accès direct aux informations visées, n'a pas encore été opérationnalisée.

données (art. 18/13 L.R&S) n'a encore jamais été utilisée par le SGRS, et ce depuis l'entrée en vigueur de la loi de 2010. En 2016, le même constat était déjà posé et expliqué par le fait que « *la procédure de création est trop lourde pour la mettre en œuvre pour un seul dossier* ».[207] Le Comité rappelait[208] au SGRS l'obligation d'informer la Commission BIM toutes les deux semaines de la mise en œuvre de ces méthodes exceptionnelles (art. 18/10 § 1er, alinéa 3 L.R&S et art. 9 AR 12 octobre 2010). À cette fin, une réunion dite 'de quinzaine' a été mise en place. Les mesures sanitaires imposées dans le cadre de la crise du coronavirus ont empêché la tenue de ces réunions. Elles ont repris au printemps 2022.

II.1.2.4. Les missions et les menaces justifiant le recours aux méthodes ordinaires et particulières[209]

Le SGRS est autorisé à employer les méthodes spécifiques et exceptionnelles dans le cadre de quatre missions[210] suivants différentes menaces.

1. **La mission de renseignement (art. 11, 1° L.R&S)**
   Le recueil, l'analyse et le traitement du renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir. Le recueil, l'analyse et le traitement du renseignement relatif à toute activité qui menace ou pourrait menacer les intérêts suivants :
   - l'intégrité du territoire national ou la survie de tout ou partie de la population ;
   - les plans de défense militaires ;
   - le potentiel économique et scientifique en rapport avec la défense ;
   - l'accomplissement des missions des Forces armées ;
   - la sécurité des ressortissants belges à l'étranger.
2. **Veiller au maintien de la sécurité militaire (art. 11, 2° L.R&S)**
   - la sécurité militaire du personnel relevant du ministre de la Défense nationale ;

---

207 Exposé des motifs du projet de loi modifiant la loi du 30 novembre 1998, *Doc. Parl.*, Chambre, 2015-2016, n°54-2043/001, 11.

208 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 109, ('XII.II.3.3. Obligation d'information dans le cadre des méthodes exceptionnelles').

209 Plusieurs intérêts et menaces peuvent figurer dans une même autorisation.

210 Ces méthodes ne peuvent donc pas être utilisées dans le cadre d'enquêtes de sécurité ou d'autres missions assignées au SGRS par ou conformément à des lois particulières (par ex. effectuer des vérifications de sécurité pour des candidats militaires)

- les installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires ;
- dans le cadre des cyberattaques de systèmes informatiques et de communications militaires ou de ceux que le ministre de la Défense nationale gère, neutraliser l'attaque et en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit des conflits armés.

3. **La protection de secrets (art. 11, 3° L.R&S)**
   La protection du secret qui, en vertu des engagements internationaux de la Belgique ou afin d'assurer l'intégrité du territoire national et l'accomplissement des missions des Forces armées, s'attache aux installations militaires, armes, munitions, équipements, aux plans, écrits, documents ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que gère le ministre de la Défense nationale.
4. **La recherche, l'analyse et le traitement du renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge (art. 11, 5°, L.R&S).**

Depuis l'entrée en vigueur de la Loi du 30 mars 2017, la mise en œuvre de méthodes particulières n'est plus limitée au territoire belge (art. 18/1, 2° L.R&S). Le SGRS a fait savoir qu'aucune MRD n'avait été mise en œuvre à l'étranger en 2021.[211] Cette compétence, qui n'a pas encore été exercée, avait pourtant été présentée, dans l'exposé des motifs de la Loi du 30 mars 2017, comme une nécessité pour permettre au SGRS de mener à bien ses missions à l'étranger (notamment celles exécutées dans le cadre des opérations avec mandat donné par le Conseil de Sécurité des Nations Unies).[212] Une enquête plus approfondie devrait permettre d'établir si le SGRS n'a effectivement jamais eu recours à des MRD à l'étranger depuis l'entrée en vigueur de cette loi – ce qui reviendrait à contredire l'argumentaire développé dans l'exposé des motifs – ou si des MRD ont été mises en œuvre à l'étranger sans recours à la procédure MRD qui s'impose pourtant. Le Comité vérifiera en 2022 si le SGRS a fait usage (à tort ?) exclusivement du régime décrit à l'article 44 (voir chapitre III 'Le contrôle des interceptions à l'étranger, des prises d'images et des intrusions dans les systèmes informatiques').[213]

---

211 Il a par contre été fait recours aux possibilités offertes à l'article 44 L.R&S. (Voir à ce propos le chapitre III 'Le contrôle des interceptions à l'étranger, des prises d'images et des intrusions dans les systèmes informatiques').

212 Exposé des motifs, *Doc. Parl.*, Chambre 2015-2016, n°54-2043/001.

213 Cette initiative s'inscrit d'ailleurs dans la logique de la loi de 2017 dont l'exposé des motifs indiquait *« dans cinq ans, il sera procédé à une nouvelle évaluation de la situation pour voir si les prérogatives en faveur du SGRS sont praticables à l'étranger et si elles couvrent suffisamment les mandats des Nations Unies »*.

Aucune méthode particulière de renseignement n'a par ailleurs été mise en œuvre à la demande d'un service partenaire étranger.[214] Par contre, comme le précise le SGRS, les informations obtenues d'un service étranger peuvent être à la source de la mise en œuvre d'une MRD.

La pratique a montré que plusieurs menaces peuvent figurer dans une même autorisation. Une légère baisse peut être observée dans la mise en œuvre des MDR pour les menaces 'espionnage' et 'terrorisme'. Il convient de noter la forte augmentation du nombre de méthodes exceptionnelles mises en œuvre dans le cadre de la menace 'extrémisme' (de 20 en 2020 à 82 en 2021). Il n'est pas surprenant que cette forte augmentation soit due à l'affaire Jürgen Conings[215] et à l'attention particulière portée à l'extrême droite au sein des Forces armées qui en a résulté. Pour la première fois, les 'organisations criminelles' sont également mentionnées comme une menace (29 méthodes utilisées).[216]

NATURE DE LA MENACE	NOMBRE EN 2020	NOMBRE EN 2021
Espionnage	139	120
Ingérence	19	16
Extrémisme	20	82
Terrorisme	19	9
Organisations criminelles	-	26
Autre	-	0
Total	**197**	**253**

Contrairement à la mise en œuvre de méthodes particulières, le Comité ne dispose pas de données chiffrées relatives à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question dans le présent chapitre. Dans son précédent rapport d'activités, le Comité recommandait aux services de consigner ces données et de les tenir à disposition.[217] Étant donné que ce n'est pas encore le cas, le Comité réitère sa recommandation.

214 Cela semblait être le cas pour la mise en œuvre de mesures 'ordinaires plus' (mais uniquement dans la mesure où cela représente également un intérêt manifeste pour le SGRS lui-même et que cela entre dans son champ de compétence).

215 Voir 'I.9. Enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings'

216 Deux dossiers spécifiques semblent l'expliquer : l'un relatif au trafic d'armes/crime organisé et l'autre relatif au trafic de drogue (initialement ouvert dans le cadre du suivi de l'extrême droite).

217 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 43.

II.1.3. LES MÉTHODES UTILISÉES PAR LA VSSE

II.1.3.1. Les méthodes ordinaires 'plus'

Méthodes ordinaires plus (VSSE)	Nombre d'autorisations en 2020	Nombre d'autorisations en 2021
Identification de l'abonné ou de l'utilisateur habituel de télécommunications	5123	4080
Recherches ciblées de données PNR[218]	30	98[219]
Utilisation d'images enregistrées par les caméras des services de police	Pas en vigueur	

En ce qui concerne les « méthodes ordinaires plus », on constate pour la troisième année consécutive une forte diminution (+/-1000 identifications demandées) du nombre d'' identifications de l'abonné ou de l'utilisateur habituel de télécommunications'.[220] En revanche, le recours aux méthodes fondées sur les articles 16/3 et 16/4 L.R&S est en augmentation constante. Le nombre d'autorisations de recherches ciblées dans les données des passagers (PNR) (Art. 16/3 L.R&S) a plus que triplé (de 30 à 98). L'utilité de cette méthode ne cesse de croître compte tenu de l'augmentation exponentielle du nombre de compagnies aériennes intégrées au système.[221] Depuis 2021, l'art. 16/4 §2 L.R&S, régissant la demande de consultation par les services de renseignement des images préalablement enregistrées des caméras de police, peut également être invoqué.[222] Les exigences procédurales s'appliquent à la fois aux récupérations ciblées d'images de caméras de police par un accès direct (en ligne) aux bases de données policières pertinentes (ce qui n'est

---

218 Le profilage n'est pas (encore) utilisé.

219 Le rapport d'activités de BELPIU indique qu'en 2021 « *la VSSE a introduit 133 demandes de recherches dans le passé* », Centre de crise national, *Rapport annuel BELPIU 2021*, 14.

220 Dans la pratique, c'est le '*common reference database center*' (CRDC) qui est consulté en premier lieu. Cette base de données fournit exclusivement de l'information sur l'opérateur assurant le service du numéro demandé, sans mentionner si ce numéro a été attribué à un utilisateur final. Aucune donnée à caractère personnel n'est conservée dans cette 'banque de données de localisation de numéro accessible au public'.

221 "*Le nombre de données passagers traitées en 2021 a été plus faible qu'en 2019. En revanche, davantage de données ont été traitées qu'en 2020, car l'unité traite les données relatives aux passagers d'un plus grand nombre de compagnies aériennes. Actuellement, les données de 94 % du trafic aérien international sont traitées. En outre, au sein de la BelPIU, les données relatives aux passagers sont traitées de manière plus ciblée et les collaborations avec d'autres unités européennes d'information sur les passagers (PIU) sont plus nombreuses*", dans : Rapport annuel BELPIU 2021.

222 Début 2022, le Comité permanent R, en sa qualité d'autorité de contrôle, a rendu une décision à ce propos : COMITÉ PERMANENT R, décision APD n° VCI-DPA/2022/2 – Instruction de traitement concernant la récupération rétroactive d'images de caméras de police par les services de renseignement sur la base de l'article 16/4, §2 L.R&S.

pas possible pour le moment) et aux récupérations ciblées par une demande écrite adressée aux services de police compétents[223] (en l'occurrence, la Direction de l'information policière et des moyens ICT de la Police fédérale (DRI)). La méthode a été utilisée à 46[224] reprises.

L'identification des titulaires des cartes prépayées n'est pas comptabilisée comme une méthode séparée.

II.1.3.2. Les méthodes spécifiques

Méthodes spécifiques (VSSE)	Nombre d'autorisations en 2020	Nombre d'autorisations en 2021
Observer, à l'aide d'un moyen technique, dans des lieux accessibles au public ou observer, à l'aide ou non d'un moyen technique, dans un lieu non accessible au public qui n'est pas soustrait à la vue (art. 18/4 L.R&S)	245	195
Inspecter des lieux accessibles au public, à l'aide d'un moyen technique, inspecter le contenu d'objets verrouillés ou les emporter (art. 18/5 L.R&S)	0	0
Prendre connaissance de données d'identification d'un trafic postal et requérir le concours d'un opérateur postal (art.18/6 L.R&S)	1	0
Requérir des données de transport et de voyage auprès de fournisseurs privés de service en matière de transport ou de voyage (art. 18/6/1 L.R&S)	70	33

223 Depuis l'entrée en vigueur de la Loi caméras du 21 mars 2018, les demandes écrites d'images de caméras de police doivent être fondées sur la base de l'article 16/4, §2 L.R&S. Les services de renseignement ne peuvent plus utiliser l'article 14, alinéa 2 L.R&S à cette fin. Voir à cet égard la décision-APD n° VCI-DPA/2022/2 (*supra*).

224 En 2021, seules les méthodes dépassant le délai d'un mois ont été mentionnées. Dans sa décision n° VCI-DPA/2022/2, le Comité a souligné que « *les demandes écrites de DRI ne peuvent avoir lieu qu'en respectant les deux exigences procédurales mentionnées ci-dessus (confirmation écrite et notification), et ce indépendamment du fait que l'accès aux données des caméras de police ait lieu pendant ou après le premier mois de conservation* » .

Méthodes spécifiques (VSSE)	Nombre d'autorisations en 2020	Nombre d'autorisations en 2021
Identifier, à l'aide d'un moyen technique, les services et de moyens de communications électroniques auxquels une personne déterminée est abonnée ou qui sont habituellement utilisés par une personne déterminée (art. 18/7 §1, 1° L.R&S)	46	22
Requérir le concours de l'opérateur d'un réseau de communications électroniques afin d'obtenir les données relatives à la méthode de paiement, identifier le moyen de paiement et le moment du paiement de l'abonnement ou de l'utilisation du service de communications électroniques (art. 18/7 §1, 2° L.R&S)	0	2
Prendre connaissance des données d'appel d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	650	491
Prendre connaissance des données de localisation d'un trafic de communications électroniques et requérir le concours d'un opérateur (art. 18/8 L.R&S)	617	477
TOTAL	**1629**	**1220**

Le nombre de méthodes spécifiques mises en œuvre a de nouveau nettement diminué (1629 à 1220). Pour pratiquement toutes les méthodes spécifiques, une diminution est observée. En plus des raisons générales mentionnées ci-dessus (nouveaux recrutements, mesures prises dans le cadre de la crise sanitaire), il y a selon la VSSE plusieurs éléments qui peuvent l'expliquer. Par exemple, l'utilisation de la méthode spécifique régie par l'article 18/6/1 L.R&S (la réquisition de données de transport ou de voyage) semble être liée aux recherches PNR ; étant donné l'augmentation du nombre de recherches ciblées dans les données PNR, l'utilisation de cette méthode spécifique a diminué (principe des vases communicants).[225] En ce qui concerne les inspections dans les lieux accessibles au public (art. 18/5 L.R&S) et la prise de connaissance des données d'identification du courrier postal

[225] Pour les données des compagnies aériennes qui ne sont pas (encore) intégrées dans BELPIU, les demandes sont encore effectuées sur la base de l'article 18/6/1 L.R&S. La VSSE souhaite pouvoir, à l'avenir, interroger également l'économie collaborative (Uber, trottinettes partagées) dans ce cadre.

(art. 18/6 L.R&S)[226], la VSSE préfère, comme en 2020, l'utilisation d'une méthode exceptionnelle afin de s'assurer d'opérer dans le respect du cadre légal.

II.1.3.3. Les méthodes exceptionnelles

Méthodes exceptionnelles (VSSE)	Nombre d'autorisations en 2020	Nombre d'autorisations en 2021
Observer, à l'aide ou non de moyens techniques, des lieux non accessibles au public qui sont soustraits à la vue et pénétrer dans des lieux non accessibles au public qui sont soustraits ou non à la vue pour exécuter une observation, installer un moyen technique, ouvrir un objet ou l'emporter (art. 18/11 L.R&S)	9	13
Inspecter, à l'aide ou non de moyens techniques, des lieux non accessibles au public, ainsi que l'inspection du contenu d'objets verrouillés ou non qui s'y trouvent (art. 18/12 L.R&S)	8	11
Recourir à une personne morale visée à l'article 13/3, § 1er L.R&S afin de collecter des données	0	0
Ouvrir et prendre connaissance du courrier confié ou non à un opérateur postal (art. 18/14 L.R&S)	11	13
Collecter des données concernant des comptes bancaires et des transactions bancaires (art. 18/15 L.R&S)	186	73
S'introduire dans un système informatique (article 18/16 L.R&S)	74	61
Écouter, prendre connaissance et enregistrer des communications (art. 18/17 L.R&S)	223	192
TOTAL	**511**	**363**

Comme pour les méthodes spécifiques, le nombre de méthodes exceptionnelles mises en œuvre par la VSSE est en diminution (de 511 en 2020 à 363 en 2021). Cette forte baisse s'explique presque entièrement par une réduction de moitié de l'utilisation de la méthode 'Collecte des données concernant des comptes bancaires et des transactions bancaires' (art. 18/15 L.R&S), passant de 186 en 2020 à 73 en

[226] Au regard des informations réceptionnées concernant l'envoi postal, il est plus indiqué d'introduire une demande de méthode exceptionnelle.

2021. Il s'avère que la mise en œuvre de cette méthode (le traitement de données financières) nécessite un travail particulièrement intensif.[227] On observe par ailleurs une légère diminution du nombre de méthodes utilisées pour l'écoute, la prise de connaissance et l'enregistrement des communications (art. 18/17 L.R&S) (de 223 en 2020 à 192 en 2021). Selon la VSSE, le recours à une personne morale (art. 18/13 L.R&S) requiert également trop de moyens.

II.1.3.4. Les menaces et les intérêts justifiant le recours aux méthodes (ordinaires et) particulières

Le tableau suivant reprend les menaces (potentielles) dans le cadre desquelles la VSSE a mis en œuvre des méthodes spécifiques et exceptionnelles. Une méthode peut naturellement viser plusieurs menaces. La VSSE peut utiliser les méthodes spécifiques dans le cadre de toutes les menaces qui entrent dans ses compétences (art. 8 L.R&S).

En considérant que plusieurs menaces peuvent figurer dans une même autorisation, les chiffres sont les suivants :

NATURE DE LA MENACE	NOMBRE EN 2020	NOMBRE EN 2021
Espionnage	816	478
Ingérence	27	121
Extrémisme	296	279
Prolifération	3	2
Organisations sectaires nuisibles	0	0
Terrorisme	998	690
Organisations criminelles	0	0
Suivi des activités des services étrangers en Belgique	(inclus dans les chiffres ci-dessus)	(inclus dans les chiffres ci-dessus)
TOTAL	**2140**	**1570**

Le tableau repris ci-dessus montre pour ce qui est de la mise en œuvre de MRD en 2021 que la menace 'terrorisme' – bien qu'une diminution soit observée (de 998 à 690) – demeure la priorité absolue de la VSSE suivie par la menace 'espionnage'.

---

[227] L'avant-projet de loi 'modifiant la loi organique des services de renseignements', pour lequel le Comité a rendu un avis en 2021, propose d'introduire, à cet égard, une nouvelle méthode ordinaire. Il propose de créer une obligation pour les institutions financières, au sens large du terme, de coopérer afin d'identifier les produits ou services financiers dont dispose une personne ou, inversement, d'identifier quelle personne peut être liée à certains produits ou services financiers. Dans l'exposé des motifs, ce choix est justifié par le fait que « *le caractère intrusif d'une telle méthode […] faible à très faible* ». Le Comité ne partage pas cet avis. Dans son avis n°001/CPR/2021 du 12 juillet 2021 – modifications Loi Renseignement, il a recommandé de considérer cette méthode comme une méthode spécifique.

Alors qu'en 2020, il était question d'une forte diminution du nombre de dossiers 'ingérence', on relève à nouveau une importante augmentation (de 27 en 2020 à 121 en 2021). Dans la pratique, il n'est cependant pas toujours évident d'établir une distinction entre l'espionnage (recueillir clandestinement des données) et l'ingérence (influencer des processus décisionnels). La menace 'extrémisme-radicalisme' est restée stable (279 dossiers). Étant donné que les organisations sectaires nuisibles et les organisations criminelles ne font plus l'objet d'un suivi actif depuis 2015[228], ces menaces, sans surprise, ne figurent pas dans les chiffres.

En termes de territorialité, la VSSE est compétente pour mettre œuvre des MRD 'sur et à partir du territoire belge' (art.18/1, 1° L.R&S). À l'instar du SGRS, la VSSE n'a pas mis en œuvre de MRD à l'étranger. Le nombre de MRD mises en œuvre en Belgique à la demande de services partenaires étrangers est également négligeable. La mise en œuvre de certaines MRD a néanmoins été décidée sur la base d'informations obtenues de services partenaires.

La compétence de la VSSE n'est pas seulement définie par la nature de la menace. Le service n'est autorisé à intervenir que pour la sauvegarde d'intérêts bien déterminés :

1. La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel, c'est-à-dire :
   a) la sécurité des institutions de l'État et la sauvegarde de la continuité du fonctionnement régulier de l'État de droit, des institutions démocratiques, des principes élémentaires propres à tout État de droit, ainsi que des droits de l'homme et des libertés fondamentales ;
   b) la sécurité et la sauvegarde physique et morale des personnes et la sécurité et la sauvegarde des biens.
2. La sûreté extérieure de l'État et les relations internationales : la sauvegarde de l'intégrité du territoire national, de la souveraineté et de l'indépendance de l'État, des intérêts des pays avec lesquels la Belgique poursuit des objectifs communs, ainsi que des relations internationales et autres que la Belgique entretient avec des États étrangers et des institutions internationales ou supranationales.
3. La sauvegarde des éléments essentiels du potentiel économique et scientifique.

Comme le SGRS, la VSSE combine plusieurs intérêts. On peut néanmoins mentionner que la 'sauvegarde des éléments essentiels du potentiel économique et scientifique' est un intérêt qui mobilise peu.

Pour rappel, le Comité ne dispose pas des chiffres relatifs à la menace visée et aux intérêts à défendre en ce qui concerne les méthodes ordinaires dont il est question dans le présent chapitre.

---

228 Voir à ce propos, 'I.5. Le suivi des organisations sectaires nuisibles et des organisations criminelles par la Sûreté de l'État'.

II.2. LES ACTIVITÉS DU COMITÉ PERMANENT R EN SA QUALITÉ D'ORGANE (JURIDICTIONNEL) ET D'AUTEUR D'AVIS PRÉJUDICIELS

II.2.1. CONTRÔLE DE CERTAINES MÉTHODES ORDINAIRES

II.2.1.1. Généralités

Le contrôle de certaines méthodes ordinaires est réglementé différemment pour chacune de ces méthodes.

En ce qui concerne l'identification de l'utilisateur de télécommunications (et l'identification de l'utilisateur d'une carte prépayée qui y est associée), la loi n'a pas instauré de contrôle spécifique. À l'article 16/2 § 4 L.R&S, il est stipulé uniquement que la liste des identifications requises et de tous les accès directs doit être communiquée chaque mois au Comité. Comme déjà mentionné, le Comité reçoit uniquement le nombre de réquisitions. Il a toutefois proposé de contrôler annuellement une sélection de réquisitions.[229]

En ce qui concerne l'accès aux données PNR, qui sont détenues par l'Unité d'information des passagers, l'article 16/3 L.R&S dispose que c'est le dirigeant du service qui doit décider de tout accès, et ce '*de façon dûment motivée*'. Le Comité doit en être informé *et* '*interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales*'. Le Comité a prononcé quatre interdictions de ce type en 2021. Trois décisions de la VSSE ainsi qu'une décision du SGRS ne répondaient en effet pas pleinement à l'obligation légale de motivation. Dans le cadre de ces dossiers, les deux services ont été interdits d'exploiter les données recueillies.

Enfin, le Comité s'est vu attribuer des modalités de contrôle particulières dans le cadre de la possibilité pour les services de renseignement d'avoir accès à des informations provenant d'images enregistrées par des caméras utilisées par les

---

229 COMITÉ PERMANENT R, *Rapport d'activités 2017*, 25, note de bas de page 41. Ce contrôle a débuté en 2020. Le Comité a décidé de reprendre cette thématique dans l'enquête qu'il a initiée en 2019 et qui est intitulée *'enquête de contrôle sur l'application et le contrôle interne des services de renseignement des méthodes et instruments récemment insérés ou adaptés par le législateur et dont un rôle de contrôle spécifique a été attribué au Comité permanent R.'*

services de police (article 16/4 L.R&S): un contrôle *a priori* [230] et un contrôle *a posteriori*.[231]

II.2.2. CONTRÔLE DES MÉTHODES PARTICULIÈRES

II.2.2.1. Les chiffres

Cette section reprend les activités du Comité permanent R relatives aux méthodes de renseignement spécifiques et exceptionnelles. L'attention se focalise ici sur les décisions juridictionnelles prises en la matière, et non sur les données opérationnelles. Il convient toutefois de souligner au préalable que le Comité soumet *toutes* les autorisations de mise en œuvre de méthodes particulières à une enquête *prima facie*, et ce en vue de décider d'une éventuelle saisine. Avant le début des mesures covid, un commissaire-auditeur du service d'Enquêtes participait aux réunions de quinzaine, au cours desquelles la VSSE informe la Commission BIM sur l'exécution des méthodes exceptionnelles. Pour des raisons évidentes, ces réunions ont été suspendues. Comme mentionné ci-dessus, ce type d'initiative reprendra au printemps 2022.

L'article 43/4 L.R&S stipule que le Comité permanent R peut être saisi de cinq manières :

1. D'initiative ;
2. À la demande de l'Autorité de protection des données (APD);
3. Par le dépôt d'une plainte d'un citoyen ;
4. De plein droit, chaque fois que la Commission BIM a suspendu une méthode spécifique ou exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données ;
5. De plein droit, quand le ministre compétent a donné son autorisation sur base de l'article 18/10, § 3 L.R&S.

Par ailleurs, le Comité peut aussi être saisi en sa qualité d'ʻauteur d'avis préjudiciels' (articles 131*bis*, 189*quater* et 279*bis* CIC). Le cas échéant, le Comité rend un avis sur la légalité des méthodes spécifiques ou exceptionnelles ayant fourni des

---

230 '*Les critères d'évaluation visés à l'alinéa 1er, 2°, sont préalablement présentés au Comité permanent R.*'

231 '*La décision du dirigeant du service ou de son délégué et sa motivation sont transmises au Comité permanent R dans les meilleurs délais. La décision peut porter sur un ensemble de données relatives à une enquête de renseignement spécifique. Dans ce cas, une liste des accès ponctuels est communiquée une fois par mois au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les conditions qui ne respectent pas les conditions légales*' et '*Chaque liste avec laquelle la corrélation visée à l'alinéa 1er, 1°, est réalisée, est communiquée dans les meilleurs délais au Comité permanent R. Le Comité permanent R interdit aux services de renseignement et de sécurité d'exploiter les données recueillies dans les circonstances qui ne respectent pas les conditions légales.*'

renseignements qui sont utilisés dans le cadre d'une affaire pénale. Les demandes d'avis sont introduites par les juridictions d'instruction ou par les juridictions de fond. Le Comité n'intervient pas alors *stricto sensu* comme un organe juridictionnel.

TYPE DE SAISINE	2013	2014	2015	2016	2017	2018	2019	2020	2021
1. D'initiative	16	12	16	3	1	1	4	2	1
2. Commission Vie Privée/ Autorité de protection des données	0	0	0	0	0	0	0	0	0
3. Plainte	0	0	0	1	0	0	0	0	0
4. Interdiction d'exploitation par la Commission BIM[232]	5	5	11	19	15	10	12	9	8
5. Autorisation du ministre	2	1	0	0	0	0	0	0	0
6. Auteur d'avis préjudiciel	0	0	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**	**9**

Le nombre de décisions prises par le Comité a continué à diminuer (de 11 en 2020 à 9 en 2021). En outre, toutes les saisines, à une exception près, résultent d'une suspension décidée par la Commission BIM. Le Comité n'a encore jamais été saisi par l'Autorité de protection des données ou par un citoyen.

Une fois saisi, le Comité peut prendre plusieurs types de décisions et de décisions intermédiaires.

1. Constater la nullité de la plainte pour cause de vice de forme ou absence d'un intérêt personnel et légitime (art. 43/4, alinéa 1er, L.R&S) ;
2. Ne pas donner suite à une plainte qui est manifestement non fondée (art. 43/4, alinéa 1er, L.R&S) ;
3. Suspendre la méthode contestée dans l'attente d'une décision définitive (art. 43/4, dernier alinéa, L.R&S) ;
4. Demander des informations complémentaires à la Commission BIM (43/5 § 1er, alinéa 1er à 3, L.R&S) ;
5. Demander des informations complémentaires au service de renseignement concerné (43/5 § 1er, alinéa 3, L.R&S) ;
6. Ordonner une mission d'enquête pour le service d'Enquêtes R (art. 43/5 § 2 L.R&S). Dans cette rubrique, il est fait référence à la fois aux multiples

[232] Elles découlent, par exemple, de problèmes d'enregistrement ou d'enlèvement d'appareillages.

informations complémentaires recueillies de manière plutôt informelle par le Service d'Enquêtes R avant la saisine proprement dite et aux informations recueillies par le Comité après la saisine ;

7. Procéder à l'audition des membres de la Commission BIM (art. 43/5 § 4, alinéa 1er, L.R&S) ;
8. Procéder à l'audition du dirigeant du service de renseignement ou des membres du service de renseignement concerné (art. 43/5 § 4, alinéa 1er, L.R&S) ;
9. Statuer sur les secrets relatifs à une information ou à une instruction judiciaire en cours dont les membres des services de renseignement sont dépositaires, après concertation avec le magistrat compétent (art. 43/5 § 4, alinéa 2, L.R&S) ;
10. Pour le président du Comité permanent R, statuer, après avoir entendu le dirigeant du service, si le membre du service de renseignement estime devoir garder le secret dont il est dépositaire parce que sa divulgation est de nature à porter préjudice à la protection des sources, à la protection de la vie privée de tiers ou à l'accomplissement des missions du service de renseignement (art. 43/5 § 4, alinéa 3, L.R&S ;
11. Mettre fin à la méthode concernée si celle-ci est toujours en cours ou si elle a été suspendue par la Commission BIM, et interdire l'exploitation des données recueillies grâce à cette méthode et leur destruction (art. 43/6 § 1er, alinéa 1er, L.R&S) ;
12. Mettre fin partiellement à une méthode autorisée. Il est question ici, par exemple, d'une situation où une méthode est limitée dans le temps, pas d'une situation où une seule autorisation d'un dirigeant du service autorise plusieurs méthodes et où le Comité ne met fin qu'à une seule d'entre elles ;
13. Lever totalement ou partiellement la suspension et l'interdiction qui ont été décidées par la Commission BIM (art. 43/6 § 1er, alinéa 1er, L.R&S). Ceci implique que la méthode autorisée par le dirigeant du service soit (partiellement) considérée comme légale, proportionnelle et subsidiaire par le Comité ;
14. Constater l'incompétence du Comité permanent R ;
15. Déclarer le caractère infondé de l'affaire pendante et permettre la poursuite de la méthode ;
16. Délivrer un 'avis préjudiciel' (art. 131*bis*, 189*quater* et 279*bis* CIC).

NATURE DE LA DÉCISION	2014	2015	2016	2017	2018	2019	2020	2021
Décisions préalables à la saisine								
1. Plainte frappée de nullité	0	0	0	0	0	0	0	0
2. Plainte manifestement non fondée	0	0	0	0	0	0	0	0
Décisions intermédiaires								
3. Suspension de la méthode	3	2	1	0	0	0	1	0
4. Information complémentaire de la Commission BIM	0	0	0	0	0	0	0	0
5. Information complémentaire du service de renseignement	1	1	4	0	0	0	1	1
6. Mission d'enquête confiée au Service d'Enquêtes R[233]	54	48	60	35	52	52	24	33
7. Audition membres de la Commission BIM	0	2	0	0	0	0	0	0
8.Audition membres des services de renseignement	0	2	0	0	0	1	1	0
9. Décision relative au secret de l'instruction	0	0	0	0	0	0	0	0
10. Informations sensibles lors de l'audition	0	0	0	0	0	0	0	0
Décisions finales								
11. Cessation de la méthode	3	3	6	9	4	11	10	5
12. Cessation partielle de la méthode	10	13	4	6	6	4	0	3
13. Levée (partielle) de l'interdiction de la Commission BIM	0	4	11	0	0	0	0	0
14. Non compétent	0	0	0	0	0	0	0	0
15. Autorisation légale/ Non- cessation de la méthode/Non-fondement	4	6	2	1	1	0	0	1
Avis préjudiciels								
16. Avis préjudiciel	0	0	0	0	0	0	0	0

[233] Le Comité demande au service d'Enquêtes d'effectuer des recherches complémentaires et/ou de contacter le service concerné ou la Commission BIM.

II.2.2.2. La jurisprudence

La substance des décisions finales prises en 2021 par le Comité permanent R dans le cadre de son rôle juridictionnel en matière de contrôle des méthodes particulières de renseignement est reprise ci-après.[234] Les synthèses sont expurgées des données opérationnelles. Seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue juridique.

Les décisions ont été regroupées dans les rubriques suivantes :
- Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode ;
- La légalité d'une méthode quant aux techniques employées, aux données recueillies, à la durée de la mesure et à la nature de la menace ;
- La légalité de l'exécution d'une méthode légale.

Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode

SUBSIDIARITÉ, PROPORTIONALITÉ ET ORIENTATION DE LA MENACE

En vertu de l'article 18/3 § 1er, alinéa 1er L.R&S, une méthode spécifique ne peut être utilisée par un service de renseignement que s'il existe une menace potentielle pour les intérêts fondamentaux du pays qui relève de la compétence du service concerné. En outre, une telle MRD ne peut être mise en œuvre que si les méthodes ordinaires de collecte de données sont jugées insuffisantes pour recueillir les informations nécessaires à l'accomplissement de la mission de renseignement (exigence de subsidiarité). Enfin, la disposition légale susmentionnée impose le choix d'une méthode spécifique en fonction du degré de gravité de la menace potentielle pour laquelle elle est utilisée (exigence de proportionnalité).

Dans le dossier 2021/10548, un service de renseignement souhaitait obtenir les données de trafic et de localisation qui passaient par un numéro de téléphone spécifique.[235] La mise en œuvre de la méthode s'inscrivait dans le cadre d'une opération lancée par le service de renseignement pour savoir si un fonctionnaire donné était impliqué, sciemment ou non, dans des activités d'espionnage d'une puissance étrangère. En effet, le collaborateur avait été actif dans le pays concerné pendant de nombreuses années et certains comportements spécifiques ont amené le service de renseignement à se demander si un service de renseignement de cette puissance étrangère avait utilisé un « piège à miel » (*'honey trap')* ; autrement dit qu'un service étranger avait tenté, par des avances manipulatrices, amoureuses et sexuelles, d'obtenir des informations de la part de cette personne. Le profil de ce collaborateur, selon le service de renseignement concerné, correspondait au profil jugé intéressant par les services de renseignement étrangers pour l'utilisation

234 Dans certains dossiers, le Comité a été saisi en 2020, mais n'a rendu sa décision finale qu'en 2021.
235 *Cf.* article 18/8, § 1er, alinéa 1er, 1° et 2° L.R&S.

d'un tel procédé. En demandant les données relatives au trafic et à la localisation, un service de renseignement belge voulait identifier les contacts sociaux et professionnels du collaborateur concerné. Il a ensuite été possible de vérifier si ces contacts étaient légaux dans le cadre de l'exercice de son travail ou s'il s'agissait de contacts non officiels, irréguliers et/ou non autorisés, susceptibles de constituer une menace.

La Commission BIM a décidé de suspendre la mise en œuvre de cette méthode spécifique. Elle a estimé que les arguments et les éléments factuels avancés par le service de renseignement ne démontraient pas qu'il existait des raisons sérieuses et factuelles de supposer la présence d'indices à l'encontre de l'intéressé selon lesquels il aurait participé à des activités de renseignement clandestines pour un service de renseignement étranger. La Commission a établi que le comportement invoqué par le service de renseignement était insuffisant pour conclure que le collaborateur aurait pu faire l'objet d'un '*honey trap*'. La Commission BIM a également estimé que le service de renseignement n'avait pas suffisamment étayé le fait que les méthodes demandées étaient proportionnées à la gravité de la menace et que l'objectif poursuivi par les méthodes, compte tenu de l'état d'avancement de l'enquête de renseignement, ne pouvait être atteint de manière moins intrusive (subsidiarité). En ce qui concerne ce dernier aspect, la Commission était d'avis que de nombreuses informations pouvaient être obtenues par des méthodes ordinaires (par ex. une enquête de personnalité du *target*).

Conformément à l'article 43/4 L.R&S, le Comité permanent R est saisi de plein droit chaque fois que la Commission a suspendu l'utilisation d'une méthode spécifique ou d'une méthode exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données pour cause d'illégalité d'une méthode spécifique ou d'une méthode exceptionnelle. Contrairement à la Commission, le Comité a considéré que le comportement invoqué par le service de renseignement était suffisant pour démontrer l'existence d'une menace potentielle, du moins en combinaison avec la position spécifique de la personne concernée, la position sensible qui y est associée et le profil (privé) spécifique de la personne concernée. Le Comité a également jugé que les exigences de subsidiarité et de proportionnalité avaient été respectées par le service de renseignement.

PROCÉDURE PARTICULIÈRE D'AUTORISATION POUR LES CATÉGORIES PROFESSIONNELLES PROTEGÉES

Dans son *Rapport d'activités 2020*, le Comité permanent R a indiqué qu'au cours de cette année de référence et pour la première fois depuis l'entrée en vigueur de la Loi MRD du 4 février 2010, il avait soumis une question préjudicielle à la Cour constitutionnelle concernant la législation MRD (dossier 2020/9606).[236]

[236] COMITÉ PERMANENT R, *Rapport d'activités 2020*, 94-97.

La question portait sur la décision d'un service de renseignement d'utiliser les méthodes spécifiques visées à l'article 18/8, § 1, 1° et 2° L.R&S sur un numéro de téléphone utilisé par un médecin. La mise en œuvre d'une méthode ordinaire a permis de constater que le numéro de téléphone en question n'était enregistré en Belgique qu'au nom de l'intéressé. Bien que le service de renseignement savait qu'il avait affaire à un médecin, il a suivi la procédure classique d'autorisation de méthodes spécifiques.[237] La Commission BIM n'était pas de cet avis et a suspendu les méthodes en cours. Compte tenu de la qualité de médecin de la personne visée, la Commission a estimé qu'il fallait recourir à la procédure d'autorisation spéciale pour les catégories professionnelles protégées prévue à l'article 18/3, § 5 L.R&S: *« (l)es méthodes spécifiques ne peuvent être mises en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de moyens de communication que ceux-ci utilisent à des fins professionnelles qu'à la condition que le service de renseignement et de sécurité dispose au préalable d'indices sérieux attestant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle et après que la commission a rendu, conformément à l'article 18/10, un avis conforme sur le projet de décision du dirigeant du service* ». Ce régime de protection particulière signifie que si un service de renseignement veut utiliser une méthode spécifique à l'égard de médecins, d'avocats ou de journalistes, il doit suivre la procédure d'autorisation des méthodes exceptionnelles. Ainsi, chaque méthode est soumise au contrôle préalable de la Commission BIM. En plus de la suspension de la méthode concernée, la Commission BIM a imposé une interdiction d'utiliser les données déjà obtenues.

L'ordonnance de suspension de la Commission BIM a donné lieu à une saisine d'office par le Comité permanent R. Compte tenu de l'importance du régime particulier de protection des catégories professionnelles susmentionnées, et en sa qualité d'organe juridictionnel[238] dans le cadre du contrôle des méthodes spécifiques et exceptionnelles, le Comité a décidé de soumettre à la Cour constitutionnelle la question préjudicielle suivante : « *L'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité viole-t-il les articles 10 et 11 de la Constitution, lus seuls ou conjointement avec l'article 22 de la Constitution et/ou combinés ou non avec l'article 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 et approuvée par la loi du 13 mai 1955, en tant qu'il ne prévoit pas en faveur de l'avocat, du médecin ou du journaliste de protection particulière pour les moyens de communication qu'ils utilisent à des fins autre que professionnelles ?* ». En effet, le Comité a noté que l'article 18/2, § 3, alinéas 1er et 2 L.R&S limite la protection accordée aux avocats, médecins et journalistes aux moyens de communication qu'ils utilisent à des fins professionnelles. Il ressort du texte actuel de la disposition susmentionnée que

237 Immédiatement après que le service de renseignement s'est rendu compte de son erreur, une nouvelle demande, qui tenait compte du caractère protégé de la profession, a été introduite.

238 Cour constitutionnelle, 22 septembre 2011, n°145/2011, cons. B.38.1

les moyens de communication utilisés à des fins autres que professionnelles ne relèvent pas (ne semblent pas relever) de la protection juridique.

En avril 2021, la Cour constitutionnelle a statué en ces termes : « *Sous réserve de l'interprétation mentionnée en B.15.2, l'article 18/2, § 3, de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité ne viole pas les articles 10, 11 et 22 de la Constitution, lus en combinaison avec l'article 8 de la Convention européenne des droits de l'homme.* »[239] Le considérant B.15.2 s'énonce comme suit : « *Eu égard à la protection particulière censée s'appliquer à toutes les informations médicales, notamment en vertu de la jurisprudence de la Cour européenne des droits de l'homme et du droit pénal belge, l'article 18/2, §3 de la loi du 30 novembre 1998 doit s'interpréter comme obligeant les services de renseignement et de sécurité à appliquer la protection offerte par le législateur en ce qui concerne les moyens de communication utilisés à des fins professionnelles lorsqu'il n'est pas certain que le moyen de communication qu'un médecin a utilisé l'a été exclusivement à des fins autres que professionnelles.* »

Suite à l'arrêt de la Cour constitutionnelle, le Comité permanent R a pris une décision finale dans le présent dossier MRD : « *Vu la qualité de médecin de [la personne X] et en rappelant l'arrêt n°64/2021 du 22 avril 2021 de la Cour Constitutionnelle, [le service de renseignement concerné] est obligé, dans le présent dossier, de démontrer que le moyen de communication en question utilisé l'est exclusivement à des fins autres que professionnelles, et ce afin que [le service de renseignement concerné] puisse utiliser en toute légalité la procédure ordinaire pour les méthodes spécifiques. Le Comité constate que la motivation de [le service de renseignement concerné] dans la décision contestée se limite à indiquer que « le sélecteur XXX et apparu comme étant le seul enregistré à son nom en Belgique ». Cette constatation ne suffit pas à démontrer que le moyen de communication en question est utilisé par [la personne X] exclusivement à des fins autres que professionnelles. Par conséquent, [le service de renseignement concerné] a utilisé de manière irrégulière la procédure ordinaire qui s'applique aux méthodes spécifiques.* »

NOTIFICATION TARDIVE À LA COMMISSION BIM

Un service de renseignement souhaitait prolonger une méthode spécifique, à savoir l'observation à l'aide de moyens techniques d'un lieu accessible au public (dossier 2021/10346). Conformément à l'article 18/3, § 4 L.R&S, une prolongation (ou

239 Cour constitutionnelle, 22 avril 2021, n°64/2021.

un renouvellement) [240] d'une méthode spécifique ne peut avoir lieu qu'après une nouvelle décision du dirigeant du service et après une notification à la Commission BIM. La période autorisée de mise en œuvre de la première méthode spécifique s'est terminée le 25 du mois à minuit. Or, la décision du dirigeant du service de prolonger l'observation, bien que prise le 25, n'a été notifiée à la Commission BIM que le 26 à 9h45. Suite à l'interdiction d'exploitation prononcée par la Commission BIM, le Comité a ordonné une interdiction d'exploitation et une destruction des données obtenues pendant la période non couverte.

ABSENCE D'AVIS CONFORME VERBAL DU PRÉSIDENT DE LA COMMISSION BIM

Conformément à l'article 18/10, § 4, alinéa 1er L.R&S, une méthode exceptionnelle peut être autorisée verbalement par le dirigeant d'un service de renseignement en cas d'extrême urgence, mais seulement après un avis conforme verbal du président de la Commission BIM. Dans le dossier 2021/10612, un service de renseignement a initié une interception (visée à l'art. 18/17, §§ 1er et 3 L.R&S), par erreur et dans un contexte d'extrême urgence, sans l'avis conforme du président de la Commission. Le service de renseignement concerné a constaté lui-même cette erreur, a immédiatement averti la Commission BIM et a placé en quarantaine les données obtenues illégalement. Comme le prévoit la loi, la Commission a interdit l'exploitation des données concernées et en a informé le Comité permanent R, qui a ordonné la destruction des données obtenues illégalement.

La légalité d'une méthode quant aux techniques employées, aux données recueillies, à la durée de la mesure et à la nature de la menace

OBJET ERRONÉ DE LA MÉTHODE

Dans le dossier 2020/10180, il s'est avéré que le service de renseignement avait par erreur inclus dans son autorisation un numéro de téléphone qui n'était pas couvert par la méthode spécifique concernée, à savoir la demande de données relatives au trafic et à la localisation des communications électroniques visée à l'article 18/8, § 1er, alinéa 1er, 1° et 2° L.R&S. Ce numéro d'appel erroné a également été mentionné dans la demande ultérieure adressée à l'opérateur de télécommunications. Mais le service s'en est lui-même aperçu, alors qu'il avait déjà reçu de l'opérateur de

[240] Bien que l'article 18/3, § 4 L.R&S ne fasse pas de distinction entre une « prolongation » d'une méthode spécifique et un « renouvellement » quant aux conditions formelles à respecter (c'est-à-dire la décision du dirigeant de service et la notification à la Commission BIM), un service de renseignement devrait être plus attentif à la gestion de la méthode concernée dans le cas d'une prolongation. Sinon, le risque existe que des périodes pendant lesquelles une méthode spécifique est en cours ne soient pas couvertes par une décision notifiée, ce qui entraîne alors une collecte illégale de données. Voir également : COMITÉ PERMANENT R, *Rapport d'activités 2020*, 97-98.

télécommunications les données réclamées. Le service de renseignement a lui-même pris l'initiative de placer les données obtenues en quarantaine électronique et a informé la Commission BIM de cette erreur. La Commission a interdit l'utilisation des données obtenues illégalement, a informé le Comité permanent R, qui a ordonné la destruction des données obtenues illégalement.

DURÉE DE LA MÉTHODE

En vertu de l'article 18/10, § 2 L.R&S, le projet d'autorisation concernant la mise en œuvre d'une méthode exceptionnelle doit, sous peine d'illégalité, indiquer la période pendant laquelle la méthode peut être utilisée. La procédure d'autorisation légale pour les méthodes exceptionnelles requiert ensuite un avis conforme de la Commission BIM. Avant de rendre cet avis, la Commission vérifie la légalité, la subsidiarité et la proportionnalité. L'un des aspects à vérifier par la Commission est la période de mise en œuvre proposée.

Dans le dossier 2021/10428, un service de renseignement avait demandé une prolongation pour une opération d'écoute téléphonique telle que visée à l'article 18/17, §§ 1er et 2 L.R&S.

Toutefois, le projet d'autorisation prévoyait deux périodes de mise en œuvre différentes (à savoir un mois *vs* deux mois). La Commission a rendu un avis conforme sur ce projet d'autorisation et a accepté une période de mise en œuvre de deux mois. Il est important de noter, cependant, que l'avis conforme de la Commission ne s'étendait pas sur la mention, dans le projet d'autorisation, de deux périodes de mise en œuvre différentes. Il n'est donc pas certain qu'un choix délibéré ait été opéré entre les deux périodes proposées par le service concerné. Le Comité permanent R s'est saisi d'office dans ce dossier. Il a établi *'dat de vermelding van deze verschillende data (1 maand, respectievelijk 2 maanden) in het ontwerp van machtiging waarschijnlijk op een materiële vergissing berust.'*[241] Le Comité a cependant estimé *'dat, zelfs bij een materiële vergissing, met het oog op het streven naar duidelijkheid en rechtszekerheid, een uitzonderlijke methode enkel kan worden toegestaan voor de kortste periode vermeld in het ontwerp van machtiging.'*[242] Le Comité a décidé que la méthode exceptionnelle était légale pour une période d'un mois à compter de l'autorisation du dirigeant du service.

---

241 *« que la mention de ces dates différentes (respectivement 1 mois et 2 mois) dans le projet d'autorisation est probablement due à une erreur matérielle »* (traduction libre).

242 *« que, même en cas d'erreur matérielle, dans un souci de clarté et de sécurité juridique, une méthode exceptionnelle ne peut être autorisée que pour la période la plus courte prévue dans le projet d'autorisation »* (traduction libre).

La légalité de l'exécution d'une méthode légale

DONNÉES RECUEILLIES PAR ERREUR

Dans trois dossiers distincts (2021/10533, 2021/10550 et 2021/10982), le service de renseignement concerné avait légalement décidé de rechercher des communications électroniques et de localiser l'origine ou la destination de communications électroniques.[243] Cependant, la transmission des données réclamées a posé un problème dans la mesure où les données transmises par le service NTSU-CTIF[244] ne correspondaient pas aux données réclamées. Dans le cas présent, en raison d'une erreur de manipulation de la part du service NTSU-CTIF, une écoute a systématiquement été lancée au lieu d'une localisation[245]. Il s'agissait donc d'un acte illégal, indépendant de la volonté du service de renseignement, ce que ce dernier a lui-même établi dans les trois cas. La Commission BIM et le NTSU-CTIF ont été immédiatement informés après chaque constatation. Dans les trois cas, le service de renseignement concerné a également décidé de son propre chef de rendre inaccessibles les données obtenues de manière irrégulière. La Commission BIM a émis à chaque fois une interdiction d'exploitation, qui a été suivie d'une ordonnance de destruction par le Comité permanent R.

II.3. CONSTATATIONS GÉNÉRALES

Le Comité permanent R formule les constatations générales suivantes :

- Entre le 1er janvier 2021 et le 31 décembre 2021, 1823 autorisations ont été émises par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement : 1570 par la VSSE (1220 spécifiques et 350 exceptionnelles) et 253 par le SGRS (166 spécifiques et 87 exceptionnelles). Après une augmentation constante du nombre total de MRD mises en œuvre ces dernières années et une stagnation observée en 2019-2020, on remarque une diminution considérable en 2021.
- La VSSE continue de se tailler la part du lion, avec 86 % des méthodes mises en œuvre. Un léger mouvement de rattrapage est constaté dans le chef du SGRS.
- Une ventilation de ces chiffres permet de constater une augmentation considérable du nombre de méthodes mises en œuvre par le SGRS (environ 30%), aussi bien pour les méthodes spécifiques (passant de 146 à 166) que

243 *Cf.* article 18/8, § 1er, alinéa 1er, 2° L.R&S (méthode spécifique).

244 Le service NTSU-CTIF (*National Technical & Tactical Support Unit – Central Technical Interception Facility*) est le système central d'interception technique de la police intégrée. Voir : Arrêté royal du 9 janvier 2003 déterminant les modalités de l'obligation de collaboration légale en cas de demandes judiciaires concernant les communications électroniques.

245 Cf. article 18/17 L.R&S (méthode exceptionnelle).

les méthodes exceptionnelles (passant de 51 à 87). À la VSSE, on observe la tendance inverse, c'est-à-dire une diminution remarquable par rapport à 2020 de l'utilisation des méthodes spécifiques (de 1629 à 1220) ainsi que des méthodes exceptionnelles (de 511 à 350).

- En ce qui concerne les méthodes ordinaires de réquisitions adressées aux opérateurs afin d'identifier certains moyens de communication, on note de nouveau une diminution, que ce soit pour la VSSE ou le SGRS. Cependant, le nombre de 'sélecteurs' concernés par ces méthodes a augmenté au SGRS de près de 20 %, et est resté stable à la VSSE.
- Pour la première fois, les deux services de renseignement ont eu recours à la méthode ordinaire plus 'utilisation des images des caméras de police'. Le nombre de recherches ciblées au sein des données PNR a considérablement augmenté pour les deux services.
- Aucune conséquence n'a pu être constatée pour l'heure par les services de renseignement à l'annulation par la Cour constitutionnelle de la loi relative à la rétention des données.
- À la VSSE, on peut encore noter que les MRD mises en œuvre dans le cadre des menaces 'terrorisme' et 'espionnage' ont diminué en nombre, mais continuent d'occuper le haut du classement. Une hausse du nombre de dossiers 'ingérence' a été constatée ; la menace 'extrémisme-radicalisme' est restée stable en nombre de MRD.
- Au SGRS, une augmentation considérable a été constatée du nombre de MRD mises en œuvre dans le cadre de la menace 'extrémisme-radicalisme', due au dossier Jürgen Conings et l'attention spécifique accordée à la présence de l'extrême droite au sein de la Défense à la suite de celui-ci. La menace 'espionnage' est celle pour laquelle le plus de MRD ont été mises en œuvre.
- Le SGRS n'a pas (encore) mis en œuvre de MRD à l'étranger. Une enquête plus approfondie devrait permettre d'établir si c'est effectivement le cas ou s'il a été fait usage (à tort) des possibilités offertes par l'article 44 L.R&S. Une telle enquête s'inscrirait d'ailleurs dans la logique de la Loi du 30 mars 2017 dont l'exposé des motifs indiquait « *dans cinq ans, il sera procédé à une nouvelle évaluation de la situation pour voir si les prérogatives en faveur du SGRS sont praticables à l'étranger et si elles couvrent suffisamment les mandats des Nations Unies* ».
- Le Comité a été saisi dans 9 dossiers, à savoir 1 saisine d'initiative et 8 saisines de plein droit, après la suspension décidée par la Commission BIM pour illégalité (art. 43/4 L.R&S). Les illégalités concernaient notamment des problèmes quant à la durée ou l'objet des méthodes, la réception des données erronées ou encore, la notification tardive de la Commission BIM.
- En 2020, pour la première fois depuis l'entrée en vigueur de la Loi MRD, le Comité permanent R a posé une question préjudicielle à la Cour constitutionnelle concernant la législation MRD. En avril 2021, la Cour s'est prononcée sur celle-ci.

Le choix opéré par le législateur MRD en 2010 visant à établir une structure logique dans la Loi relative aux services de renseignement en ce qui concerne les compétences (d'enquête) des services de renseignement (entre autres une distinction entre les méthodes exceptionnelles, spécifiques et ordinaires en fonction du degré d'ingérence dans la vie privée) a été largement abandonné par les modifications législatives apportées ces dernières années. Les récentes propositions de modifications à la loi relative aux services de renseignement[246] n'améliorent guère la situation. Le Comité déplore que cette réglementation devienne ainsi trop complexe et incohérente. Une initiative législative, à laquelle le Comité est prêt à collaborer, s'avère nécessaire et offrira une sécurité juridique plus grande pour les services de renseignement mais aussi pour le citoyen.

246 Voir à ce propos 'VI.4. Avis concernant l'avant-projet de loi modifiant la loi organique des services de renseignement'.

CHAPITRE III.
LE CONTRÔLE DES INTERCEPTIONS À L'ÉTRANGER, DES PRISES D'IMAGES ET DES INTRUSIONS DANS DES SYSTÈMES INFORMATIQUES

III.1. LES COMPÉTENCES DU SGRS ET LA MISSION DE CONTRÔLE DU COMITÉ PERMANENT R[247]

Dès 2017, la compétence du Service Général du Renseignement et de la Sécurité (SGRS) a été élargie dans le cadre des interceptions de sécurité.[248] Les interceptions pouvaient alors porter sur des communications *'émises ou reçues à l'étranger'*. Cette possibilité vaut pour presque toutes les missions du SGRS. Il est d'ailleurs intéressant d'observer que les descriptions des missions ont, elles aussi, été élargies. Le législateur a en même temps introduit deux autres méthodes, à savoir 'l'intrusion dans un système informatique' (art. 44/1 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S)) et 'la prise d'images animées' (art. 44/2 L.R&S). Par ailleurs, la manière dont le Comité peut contrôler ces méthodes a été modifiée.

Le contrôle *préalable* aux interceptions, prises d'images fixes ou animées s'effectue sur la base d'une liste établie annuellement.[249] Cela signifie qu'en plus du plan annuel d'interceptions, le SGRS doit également élaborer un plan d'intrusions et d'images.[250] Le SGRS doit envoyer ces listes au ministre de la Défense au mois de décembre pour autorisation. Le ministre prend une décision endéans les dix

---

247 Voir articles 44 à 44/5 inclus L.R&S.

248 À propos des modifications de loi successives relatives à la compétence d'interception, voir COMITÉ PERMANENT R, *Rapport d'activités 2018*, 63 et suiv.

249 Ceci n'implique pas que le Comité permanent R a la compétence d'approuver ou non la liste approuvée par le ministre.

250 Dans ces plans, le SGRS dresse une liste *'d'organisations et d'institutions qui feront l'objet d'interceptions de leurs communications, d'intrusions dans leurs systèmes informatiques ou de prises d'images fixes ou animées dans le courant de l'année à venir. Ces listes justifieront pour chaque organisation ou institution la raison pour laquelle elle fera l'objet d'une interception, intrusion ou prise d'images fixes ou animées en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°, et mentionneront la durée prévue'* (art. 44/3 L.R&S).

jours ouvrables et doit la communiquer au SGRS[251], qui transmet à son tour les listes pourvues de l'autorisation ministérielle au Comité permanent R.[252]

Le contrôle réalisé *pendant* l'interception, l'intrusion ou la prise d'images s'effectue *'à tout moment moyennant des visites aux installations dans lesquelles le Service Général du Renseignement et de la Sécurité effectue ces interceptions, intrusions et prises d'images fixes ou animées'*.

Le contrôle réalisé *après* l'exécution s'effectue '*sur base de listes mensuelles des pays ou des organisations ou institutions ayant effectivement fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images durant le mois écoulé*' et qui justifient '*la raison pour laquelle l'écoute, l'intrusion ou la prise d'images a été effectuée en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°*'. Ces listes doivent être notifiées au Comité permanent R. Le contrôle *ex post* s'effectue aussi sur la base *'du contrôle de journaux de bord tenus d'une façon permanente sur le lieu d'interception, d'intrusion ou de prise d'images fixes ou animées par le Service Général du Renseignement et de la Sécurité'*. Le Comité permanent R doit toujours avoir accès à ces journaux de bord.

Que peut faire le Comité permanent R en cas d'irrégularité ? L'article 44/4 L.R&S stipule que, '*le Comité permanent de contrôle des services de renseignement, sans préjudice des autres compétences attribuées à ce Comité par la loi du 18 juillet 1991, a le droit de faire cesser des interceptions, intrusions ou prises d'images en cours lorsqu'il apparaît que celles-ci ne respectent pas les dispositions légales ou l'autorisation [ministérielle]. Il ordonne l'interdiction d'exploiter les données recueillies illégalement et leur destruction, selon les modalités à fixer par le Roi.*' Malgré la recommandation pressante du Comité[253], un tel arrêté d'interception n'a toujours pas été pris.[254] Aussi, le Comité recommande une nouvelle fois de le faire au plus vite.

---

251 Si le ministre n'a pas pris de décision ou ne l'a pas transmise au SGRS avant le 1er janvier, le service peut procéder aux interceptions, intrusions et prises d'images fixes ou animées prévues, sans préjudice de toute décision ultérieure du ministre.

252 Pour les interceptions, les intrusions ou les prises d'images qui ne figurent pas dans les listes annuelles mais qui *'s'avèrent indispensables et urgentes'*, le ministre est averti dans les plus brefs délais, au plus tard le premier jour ouvrable qui suit le début de l'interception. S'il n'est pas d'accord, il peut faire cesser l'interception. Cette décision est communiquée au Comité permanent R le plus rapidement possible par le SGRS.

253 COMITÉ PERMANENT R, *Rapport d'activités 2018*, 131.

254 Le Comité doit de toute manière motiver sa décision de manière circonstanciée et la communiquer au ministre et au SGRS.

III.2. LES CONTRÔLES EFFECTUÉS EN 2021

III.2.1. LE CONTRÔLE PRÉALABLE À L'INTERCEPTION, L'INTRUSION OU LA PRISE D'IMAGES

L'ensemble des plans relatifs aux interceptions, aux intrusions et aux prises d'images pour l'année 2021 a été remis au Comité permanent R à la mi-janvier 2021.

Préalablement à la remise de ces documents, le SGRS a organisé une réunion de travail à leur sujet avec le Comité. Lors de celle-ci, le Comité a formulé un certain nombre de remarques quant aux prescrits légaux à respecter. À la réception des plans, le Comité permanent R a constaté que, conformément à ses recommandations, les trois plans (les plans relatifs aux interceptions, aux intrusions et aux prises d'images) avaient été regroupés dans un document unique. Le SGRS a ainsi visé à uniformiser à brève échéance l'ensemble des plans qu'il produit conformément à l'art. 44 L.R&S. Les autres remarques formulées ayant également été prises en compte, le Comité a pu conclure que les plans pour l'année 2021 respectent les prescrits légaux.

III.2.2. LE CONTRÔLE PENDANT L'INTERCEPTION, L'INTRUSION OU LA PRISE D'IMAGES

Le Comité permanent R a visité en 2021 les installations à partir desquelles sont effectuées les interceptions. Il a notamment pu vérifier, lors de sa visite, la conformité du *logbook* avec les lois et les directives d'application. Le Comité a relevé des manquements mineurs qui ont été immédiatement rectifiés par le responsable présent sur place.

Le Comité permanent R a également réalisé, pour la première fois, une inspection sur site du service du SGRS en charge de l'exécution du plan d'intrusion. À cette occasion, il a pu constater que le service atteignait progressivement son entière capacité opérationnelle. Il a rappelé les prescrits légaux d'application (et plus précisément l'obligation de tenir un *logbook*), et a invité le service à s'y conformer. Cet élément retiendra l'attention du Comité lors de ses visites ultérieures.

Quant au plan de prises d'images, le Comité permanent R n'a pas pu effectuer de contrôle des installations en 2021. Ce contrôle sera prioritairement réalisé en 2022.

III.2.3. LE CONTRÔLE APRÈS L'EXÉCUTION DE LA MÉTHODE

Le Comité a reçu douze '*listes mensuelles des pays ou des organisations ou institutions ayant effectivement fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images durant le mois écoulé*' et qui justifient '*la raison pour laquelle l'écoute, l'intrusion ou la prise d'images a été effectuée en lien avec les missions visées à l'article 11, § 1er, 1° à 3° et 5°*'.

Le Comité permanent R a donc reçu l'ensemble des listes légalement prévues. Il évaluera la forme et le contrôle lié auxdites listes avec le SGRS courant 2022.

CHAPITRE IV.
LE COMITÉ PERMANENT R EN SA QUALITÉ D'AUTORITÉ DE CONTRÔLE COMPÉTENTE DANS LE CADRE DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

IV.1. INTRODUCTION

Le Règlement Général sur la Protection des Données 2016/679 (RGPD)[255] et la Directive 2016/680 (Directive)[256] règlent la manière dont les acteurs publics et privés doivent opérer lorsqu'ils collectent, sauvegardent, conservent et communiquent des données à caractère personnel. Les deux instruments européens ont donné lieu à quelques modifications de loi substantielles au niveau national : en décembre 2017, l'Autorité de protection des données (APD) [257] – qui a succédé à la Commission Vie privée – a été créée et en juillet 2018, une nouvelle Loi relative à la protection des données (LPD) a été votée.[258] Cette loi modifie à son tour la L.Contrôle du 18 juillet 1991. Le Comité permanent R a, en effet, été désigné comme autorité de contrôle compétente pour les traitements de données à caractère personnel qui relèvent de la 'sécurité nationale'.

Le rôle du Comité en la matière est décrit dans la Loi portant création de l'Autorité de protection des données (Loi APD), dans la Loi relative à la protection des données (LPD) et dans la Loi organique du contrôle des services de police

---

255 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD), Journal Officiel de l'Union européenne, 2 mai 2016.

256 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes, de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la Décision-cadre 2008/977/JAI du Conseil, Journal Officiel de l'Union européenne, 4 mai 2016, n° 119/89.

257 Loi du 3 décembre 2017 portant création de l'Autorité de protection des données (Loi APD), *M.B.* 10 janvier 2018.

258 Dénomination complète : Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (LPD), *M.B.* 5 septembre 2018.

et de renseignement et de l'Organe de contrôle pour l'analyse de la menace (L.Contrôle).[259]

L'article 35 § 3 L.Contrôle énonce que le '*Comité permanent R fait rapport annuellement à la Chambre des représentants sur les avis rendus en sa qualité d'autorité de protection des données, sur les enquêtes effectuées et mesures prises en cette même qualité ainsi que sur sa collaboration avec les autres autorités de protection des données*'. Ce chapitre répond à cette obligation. Il aborde successivement les thèmes suivants :

- les contrôles effectués par le Comité – seul ou avec l'Organe de contrôle de l'information policière (C.O.C.) ou le Comité P – à la demande de citoyens qui souhaitent exercer leur droit d'accès indirect à leur 'dossier' dans l'un des services contrôlés par le Comité ;
- les avis rendus par le Comité concernant la protection des données ;
- la notification d'une potentielle brèche de sécurité ;
- les travaux dans le cadre de l'évaluation de loi sur la protection des données.

IV.2. LE TRAITEMENT DES REQUÊTES INDIVIDUELLES

Le Comité permanent R est compétent pour le traitement des requêtes individuelles relatives aux traitements de données à caractère personnel par les personnes et les services susmentionnés ainsi que leurs sous-traitants (art. 34 L.Contrôle et articles 79, 113, 145 et 173 LPD). Le requérant est en droit de demander la rectification ou la suppression de données à caractère personnel inexactes le concernant. Et il peut demander à ce que le respect des règles qui sont d'application en matière de protection des données soit vérifié. Il peut encore se plaindre de l'éventuel non-respect des règles de protection des données par un responsable du traitement relevant de la compétence du Comité.

Pour être recevable, une requête doit être écrite, datée, signée et motivée (art. 51/2 L.Contrôle).[260] Si la requête est manifestement non fondée, le Comité peut décider de ne pas y donner suite. Cette décision doit être motivée et communiquée par écrit au requérant.[261]

Le tableau suivant donne un aperçu des dossiers traités (ouverts et/ou clôturés) en 2021. Les colonnes du tableau ventilent les requêtes selon que la compétence du

---

259 Pour plus de détails, voir COMITÉ PERMANENT R, *Rapport d'activités 2018*, 75-86.

260 Cette disposition stipule également que la requête doit '*justifier de l'identité de la personne concernée*'. Il est difficile de saisir d'emblée la signification de cette disposition. Il s'agit vraisemblablement de l'obligation de prouver son identité. Cette obligation est en fait reprise dans les dispositions concernées de la Loi relative à la protection des données (voir les articles 80, 114, 146 et 174 LPD).

261 Ces vérifications sont effectuées sans frais (voir les articles 80, 114, 146 et 174 LPD).

Comité permanent R est exclusive ou conjointe avec d'autres autorités de contrôle (AC).[262]

Tableau 1. Le traitement des requêtes individuelles[263]

2021	Comité permanent R		Comités permanents R et P	Comités permanents R et P et le C.O.C.	**Total**
1. Dossiers ouverts en 2021	14		2	0	**16**
2. Requêtes irrecevables en 2021	3		0	0	**3**
3. Requêtes recevables en 2021	8		0	0	**8**
	c. SGRS	2			
	c. VSSE	6			
	c. VSSE&SGRS	-			
4. Requêtes en suspens en 2021	3		0	0	**0**
5. Dossiers en cours en 2021	10[264]		1	2[265]	**13**
6. Dossiers clôturés en 2021[266]	10[267]		2[268]	1[269]	**13**
7. Mesures correctives	3		0	1	**4**
8. Nombre total de requêtes traitées	20		3	3	**26**

262 Le tableau n'indique donc pas les hypothèses dans lesquelles une coopération a pu se réaliser avec une autre autorité de contrôle, le C.O.C. par exemple, lorsque les compétences de chaque AC sont distinctes.

263 La ligne 1 indique le nombre de dossiers ouverts en 2021. Les lignes 2 et 3 répartissent les requêtes selon la décision d'irrecevabilité ou de recevabilité. Pour les dossiers traités uniquement par le Comité permanent R, la ligne 3 précise encore le nombre de requêtes recevables selon les services visés. À la ligne 4 figure le nombre de requêtes dont la décision de recevabilité est encore en suspens. Les lignes 5 et 6 précisent l'état d'avancement des dossiers en 2021 (toujours en cours ou clôturés). Enfin, la ligne 7 indique le nombre de dossiers pour lesquels des mesures correctives ont été exigées par le Comité.

264 Dont un dossier ouvert en 2020.

265 Dont deux dossiers ouverts en 2020.

266 Complètement clôturés. Lorsque des mesures correctives sont exigées, le Comité permanent R clôture le dossier lorsqu'il a pu constater que les mesures ont été mises en œuvre.

267 Dont cinq dossiers ouverts en 2020.

268 Dont un dossier ouvert en 2020.

269 Dont un dossier ouvert en 2020.

Il peut être relevé que dans 85 % des requêtes, les personnes concernées allèguent[270] une interférence concrète dans leurs droits et libertés causée par, ou en tout cas liée à, un traitement de données d'un responsable du traitement relevant de la compétence du Comité permanent R. Une telle interférence existerait, par exemple, dans le cadre d'une demande d'acquisition de la nationalité ou de titre de séjour à l'occasion de laquelle un service de renseignement communique des informations au Ministère public, lorsque la personne concernée allègue faire l'objet de contrôles réguliers de police, lorsqu'elle constate que l'accès à un territoire lui est refusé, lorsque des données d'un service de renseignement ont été utilisées dans une procédure judiciaire pénale.

En 2021, le Comité a ainsi eu à traiter plusieurs requêtes déposées dans le cadre de procédures de demande de nationalité ou de droit de séjour. Confrontés à une décision négative motivée sur la base d'informations fournies par la Sûreté de l'État (VSSE), le Service Général du Renseignement et de la Sécurité (SGRS) et/ou l'Organe de coordination pour l'analyse de la menace (OCAM), les requérants s'adressent (entre autres) au Comité permanent R pour un contrôle du traitement de leurs données personnelles.

Une requête déposée en 2020 a également donné lieu à l'ouverture en 2021 d'un dossier d'information. Lors du traitement de la requête, le Comité permanent R a en effet constaté des pratiques non conformes au prescrit légal. À partir d'une requête individuelle, le Comité a ainsi souhaité interroger le traitement général des données à caractère personnel par les services de renseignement dans un contexte spécifique.

Les 15 % restant de requêtes se composent de demandes d'exercice indirect de droits, sans précision particulière ou grief concret. Typiquement, la personne concernée se demande si des données sont traitées à son sujet et si le traitement de celles-ci est conforme à la réglementation applicable (accès indirect).

Ce déséquilibre (85-15 %) n'est pas surprenant dès lors que la réponse fournie à la personne concernée exerçant ses droits ne lui apprend rien sur ce qu'il en est du traitement (éventuel) de ses données à caractère personnel par les services relevant de la compétence du Comité. Ce n'est que lorsque la personne concernée suspecte ou subit concrètement l'effet d'un tel traitement de données, qu'elle verra un intérêt à s'adresser au Comité permanent R pour qu'il réalise les vérifications nécessaires, dans l'espoir d'obtenir une amélioration de sa situation.

---

[270] Il est à noter que dans plusieurs dossiers, ces interférences ne sont pas seulement alléguées par les personnes concernées mais bien étayées par elles et avérées (s'agissant par exemple, de la communication de notes d'analyse dont disposent les personnes concernées dans le cadre des procédures où ces notes sont utilisées par les autorités publiques). Dans d'autres cas, ces allégations sont des suspicions, plus ou moins, voire non, étayées en fait.

IV.3. LES AVIS

Le Comité peut rendre un avis *'sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant des orientations politiques des ministres compétents'* dans deux cas : lorsque la loi impose son avis ou à la demande de la Chambre des représentants ou du ministre compétent (art. 33, alinéa 8 L. Contrôle). Ce genre d'avis porte spécifiquement sur la problématique du traitement de données et doit donc être distingué de la compétence d'avis générale qui porte, par exemple, sur l'efficacité et la coordination (cf. Chapitre VI. Avis). Cette compétence d'avis générale est, en ce sens, plus large, tout en étant plus restreinte puisque limitée au fonctionnement des services de renseignement et de l'OCAM.

En 2021, le Comité a rendu trois avis en cette qualité, dont deux portent sur l'échange d'informations classifiées[271] et un sur l'avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace en tant qu'autorité conjointement compétente avec le Comité permanent P[272] :

- Avis 005/CPR/2021 du 1er décembre 2021 portant sur une demande d'avis du président de l'Autorité nationale de sécurité concernant le *'projet de loi portant assentiment à l'accord entre le Royaume de Belgique et le Royaume des Pays-Bas concernant l'échange et la protection mutuelle des informations classifiées, fait à Bruxelles le 5 novembre 2019'*.
- Avis 006/CPR/2021 du 1er décembre 2021 portant sur une demande d'avis du président de l'Autorité nationale de sécurité concernant le *'projet de loi portant assentiment à l'accord entre le Royaume de Belgique et le Royaume-Uni de Grande Bretagne et d'Irlande du Nord concernant la protection mutuelle des informations classifiées, fait à Bruxelles le 1 décembre 2020'*.
- Avis commun 001/CPR-CPP/2021 du 8 octobre 2021 sur '*l'avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace*'.

IV.4. LA NOTIFICATION D'UNE POTENTIELLE BRÈCHE DE SÉCURITÉ

Les services contrôlés par le Comité permanent R doivent conserver ou mettre à la disposition du Comité toute une série de données.[273] Le responsable du traitement

---

271 Des avis en ce sens avaient déjà été rendus en 2019 et 2020 sur l'échange d'informations classifiées avec la République de Chypre, la Hongrie, la République de Finlande et le Royaume d'Espagne, la République française et la République italienne.

272 Voir *in extenso* sur le site du Comité permanent R.

273 Chaque service n'est pas tenu de conserver ou tenir à disposition du Comité toutes les données mentionnées ici. La Commission BIM ne doit ainsi pas communiquer d'informations au Comité.

doit ainsi notifier toute brèche de sécurité susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques dans les meilleurs délais et si possible, 72 heures après en avoir pris connaissance (articles 89, 122, 155 et 180 LPD).

En 2021, la presse a fait état d'un piratage du réseau informatique du SPF Intérieur.[274] En réponse, le directeur de l'Unité belge d'information des passagers (BELPIU) a spontanément déclaré que le système informatique distinct des dossiers passagers (PNR) n'avait pas été compromis. C'est ce qu'a révélé une analyse effectuée par le Centre pour la Cybersécurité Belgique (CCB).

IV.5. ÉVALUATION DE LA LOI RELATIVE À LA PROTECTION DES DONNÉES

L'article 286 LPD dispose que la Loi relative à la protection des données doit être soumise à une évaluation conjointe des ministres compétents dans le courant de la troisième année après son entrée en vigueur. Dans ce contexte, le secrétaire d'État Mathieu Michel a écrit au Comité permanent R pour lui demander son aide dans le cadre du comité d'orientation qu'il a mis en place. Le Comité a ensuite fourni plusieurs documents contenant des propositions aussi bien générales que technico-juridiques très spécifiques pour renforcer la protection des données.[275]

[274] H. DECREM et L. BELGHMIDI, www.vrt.be, 26 mei 2021 ('Twee jaar lang 'doelbewuste cyberaanval op overheidsdienst Binnenlandse Zaken: 'Dit is spionage").

[275] Voir à cet égard : COMITÉ PERMANENT R, *Rapport d'activités 2020*, 119-125, ('V.7. Évaluation de la loi relative à la protection des données').

CHAPITRE V.
LE CONTRÔLE DES BANQUES DE DONNÉES COMMUNES

La création de la banque de données commune '*foreign terrorist fighters*' par les ministres de l'Intérieur et de la Justice remonte à 2016. Cette banque de données commune a été modifiée en 2018 : on parle désormais de la banque de données commune '*terrorist fighters*' (BDC TF). Celle-ci comprend, outre la catégorie générale des '*foreign terrorist fighters*', une catégorie visant les '*homegrown terrorist fighters*'. Toujours en 2018, une (nouvelle) banque de données commune distincte a été créée pour les 'propagandistes de haine' (BDC PH). Par un arrêté royal pris fin 2019, deux nouvelles catégories ont encore été ajoutées à la BDC TF, à savoir les 'extrémistes potentiellement violents' (EPV) ainsi que les 'personnes condamnées pour terrorisme' (PCT).

L'article 44/11/3*quinquies*/2 LFP assigne le contrôle du traitement des informations et des données à caractère personnel contenues dans les banques de données communes à l'Organe de contrôle de l'information policière (C.O.C.) et au Comité permanent R (ci-après "les autorités de contrôle"). Un rapport conjoint a été établi dans le cadre de ce contrôle. Il fut discuté début octobre 2021 au sein de la Commission de suivi.[276]

V.1. LA MISSION DE CONTRÔLE ET L'OBJET DU CONTRÔLE

Pour l'année 2020-2021, le Comité permanent R et le C.O.C. ont décidé d'axer leur contrôle conjoint, d'une part, sur la vérification de l'accès direct prévu en faveur de l'Autorité nationale de sécurité (ANS) et, d'autre part, sur le suivi réservé à certaines recommandations formulées dans les rapports des années précédentes.

Par ailleurs, les autorités de contrôle ont procédé à un examen approfondi de la coordination du traitement des informations dans la BDC TF et la BDC PH, avec notamment une attention particulière pour le rôle du *data protection officer* (DPO).

---

[276] C.O.C. et COMITÉ PERMANENT R, *Rapport concernant le contrôle conjoint des Banques de données communes Terrorist Fighters et Prédicateurs de haine par le Comité permanent R et l'Organe de contrôle de l'information policière*, 2020, 33 p. (Diffusion restreinte - A.R. 20 mars 2000). Le rapport a été approuvé par les autorités de contrôle le 12 août 2021.

À cet égard, le nombre croissant de services disposant d'un accès à la BDC TF et la BDC PH a également été pris en compte.

Sur le plan méthodologique, compte tenu de la crise sanitaire et afin de permettre aux services de disposer d'un recul suffisant pour la mise en œuvre des recommandations formulées au terme du rapport relatif au contrôle pratiqué en 2019, il a été décidé de prévoir le déroulement de l'enquête durant le quatrième trimestre de l'année 2020. Plusieurs services ont été questionnés, parmi lesquels l'ANS, l'OCAM (responsable opérationnel des banques de données communes), la Police fédérale (gestionnaire technique) ainsi que les *data protection officers* (DPO). L'enquête s'est clôturée par une rencontre avec le Directeur f.f. de l'OCAM ainsi que le DPO des banques de données communes.

V.2. LES CONSTATATIONS DE L'ENQUÊTE

V.2.1. L'ABSENCE D'ACCÈS DE L'ANS

Au moment du contrôle, le C.O.C. et le Comité permanent R ont constaté que l'ANS n'était pas reliée aux banques de données communes (BDC) et qu'elle n'avait entrepris aucune démarche en ce sens.

Le C.O.C. et le Comité permanent R ont estimé que l'ANS faisait preuve d'une nonchalance manifeste et irresponsable. Son abstention, qui contrevient à la réglementation en vigueur, a fait courir des risques de sécurité non seulement en ce qui concerne le caractère systématique de la consultation des BDC, mais aussi en ce qui concerne l'alimentation de celle-ci. La Police fédérale a indiqué qu'elle ne procédait pas à l'alimentation des BDC dans le cadre des vérifications de sécurité (ni des habilitations de sécurité). Rien n'indiquait que cette alimentation était systématiquement effectuée par les services de renseignement en ce qui concerne les habilitations de sécurité. De ce fait, différentes informations intéressantes, voire cruciales, ont potentiellement pu échapper aux services.

D'autre part, compte tenu du fait que l'ANS ne dispose pas d'une compétence exclusive en qualité d'autorité de sécurité, et afin d'assurer la complétude des BDC, le C.O.C. et le Comité permanent R recommandaient aux différentes autorités de sécurité visées aux articles 15, al.2 et 22*ter*, al.2 L.C&HS et 9, al.1, 9° de la Loi du 28 février 2007[277] de s'assurer de la consultation effective des BDC dans les différents processus pour lesquels elles sont compétentes et d'alimenter les BDC concernant leurs décisions, soit sur base de leur accès direct aux BDC soit en prenant contact avec un service de base à cette fin (dans le cas où elles ne disposent pas de l'accès direct).

[277] Loi du 28 février fixant le statut des militaires et candidats militaires du cadre actif des Forces armées, inséré par la Loi du 31 juillet 2013 modifiant ladite Loi, *M.B.* 20 septembre 2013.

Le C.O.C. et le Comité permanent R ont indiqué que ces différents aspects seront vérifiés lors des contrôles ultérieurs.

V.2.2. LE SUIVI DES RECOMMANDATIONS ANTÉRIEURES

V.2.2.1. Les recommandations suivies d'effet

La disponibilité et l'indépendance du DPO

Le contrôle a démontré que le DPO des BDC disposait des connaissances juridiques requises pour assurer la fonction. Le travail effectué est satisfaisant, ceci d'autant plus que les circonstances (crise sanitaire) n'ont pas facilité l'accomplissement de toutes les missions. Les problématiques de la charge de travail et de la disponibilité du DPO avaient été précédemment identifiées.[278] Dans le cadre du contrôle, il est apparu que le DPO avait depuis demandé un '*réajustement du temps de travail*'. Cette demande a été analysée par le service RH de l'OCAM. Le C.O.C. et le Comité permanent R ont insisté sur le fait que le DPO doit disposer de toute la liberté requise car, en raison du nombre élevé d'utilisateurs et de la technicité de la matière, sa mission est délicate et complexe. La détermination ou la validation des priorités (contenues dans une lettre de mission) par les responsables de traitement était également un facteur critique de succès. En ce qui concerne le risque de conflit d'intérêts, le contrôle effectué a permis de l'écarter : différents avis transmis par le DPO des BDC ont démontré qu'il dispose de l'indépendance requise.

V.2.2.2. Les recommandations non suivies d'effet

Le signalement des incidents de sécurité

Le C.O.C. et le Comité permanent R ont réitéré, à l'attention de la Police fédérale, leur recommandation de leur signaler formellement les incidents de sécurité. Le contrôle pratiqué a révélé un incident de sécurité n'ayant pas fait l'objet d'un signalement immédiat. Ce signalement relève de la responsabilité de la Police fédérale, en sa qualité de gestionnaire technique des BDC. Les autorités de contrôle ont, en outre, attiré l'attention de la Police fédérale sur le fait que la notion '*d'incident de sécurité*' vise non seulement la confidentialité, mais également la disponibilité et l'intégrité des BDC.

En ce qui concerne le suivi de la seconde recommandation (information adéquate des services utilisateurs quant au rapportage d'incidents constatés), le

[278] Voir à ce propos COMITÉ PERMANENT R, *Rapport d'activités 2019*, ('XI.2.4. Évaluation des conflits d'intérêts et de l'emploi du temps du délégué à la protection des données'), 133.

C.O.C. et le Comité permanent R ont posé le constat qu'il n'y avait pas eu d'avancée significative en 2020. Cette recommandation a également été réitérée.

V.2.2.3. Les recommandations partiellement suivies d'effet

L'exécution de développements informatiques

Le C.O.C. et le Comité permanent R ont constaté que leur recommandation relative à l'exécution de développements informatiques (en vue d'assurer le suivi des délais de conservation des données dans les BDC) semblait être en cours d'exécution. Un suivi était annoncé par la Police fédérale au début du second semestre 2021. Ils ont insisté pour que cet aspect, régulièrement rappelé depuis le début des contrôles conjoints, soit définitivement réglé dans le délai annoncé par la Police.

Le contrôle des loggings

D'autre part, le C.O.C. et le Comité permanent R ont constaté que leur recommandation en matière de contrôle de loggings était en cours d'exécution. La Police fédérale avait pris une initiative visant à encourager le contrôle des loggings par les services de police. Le C.O.C. et le Comité permanent R souhaitaient que le DPO des BDC, dans sa mission de stimulation de la sécurité de l'information, veille à ce que cette initiative soit étendue à tous les (DPO des) utilisateurs, ceci d'autant plus que certains d'entre eux n'ont pas l'habitude de traiter des informations sensibles. Lors du contrôle, il a été mentionné que la fonctionnalité de contrôle des loggings était prévue dans la version '3.0' des BDC. Le C.O.C. et le Comité permanent R ont insisté sur le fait que tous les services soient en mesure, lors d'un prochain contrôle, de démontrer qu'ils ont exécuté un contrôle des loggings.

L'exception à l'obligation d'alimenter les BDC et les informations policières

Les contrôles antérieurs ont révélé que les informations policières issues de « RIR, code 01 ou code 00 » n'étaient pas reprises dans les BDC.[279] Les autorités de contrôle avaient demandé à la Police fédérale d'analyser la réglementation relative à l'alimentation des BDC de manière approfondie. Le C.O.C. et le Comité permanent R estimaient que l'analyse de la Police fédérale n'était que partiellement satisfaisante. Une analyse plus approfondie et réalisée en concertation avec les autorités judiciaires a été demandée.

[279] Un « RIR 01 » concerne des informations policières qui ne peuvent être utilisées qu'avec l'accord du rédacteur. Un « RIR 00 » concerne des informations policières qui ne peuvent en aucun cas être utilisées.

La transmission des listes

Le C.O.C. et le Comité permanent R ont noté que des initiatives avaient été prises, d'une part, en vue de mettre fin (partiellement) à la transmission de listes qui ne répondait pas à la réglementation et, d'autre part, en vue de définir les principes clairs et d'élaborer des protocoles d'accord portant sur les finalités, les modalités et les aspects de sécurité de cette transmission. Ils ont salué les initiatives particulières prises par le DPO des BDC. Compte tenu de la réglementation (et sous réserve d'une modification de celle-ci suite à l'enquête menée par l'OCAM), la signature de protocoles s'impose pour tous les services qui ne disposent pas d'un accès direct aux BDC, avec une priorité à accorder aux services qui ne disposent d'aucun accès. Le C.O.C. et le Comité permanent R ont recommandé une analyse et une mise en œuvre rapide des propositions de protocoles d'accord du DPO.

La consultation du Ministère public par l'OCAM concernant les mesures judiciaires

La réglementation tient compte du statut indépendant du Ministère public puisqu'il n'y a aucune obligation (mais une possibilité) pour ce service partenaire d'alimenter la BDC TF et la BDC PH et ce, même s'il a un accès direct. Le législateur a jugé que les données judiciaires proviennent principalement de la police. En ce sens, l'obligation pour les services de police d'alimenter la banque de données commune suffit, de sorte que les données pertinentes de la Police judiciaire sont enregistrées.[280] Afin de s'assurer que les banques de données TF et PH soient correctement alimentées, les autorités judiciaires ont envoyé des instructions. Il n'est pas apparu pas que l'OCAM mettait en œuvre les principes énoncés par la COL 18/2020. Le C.O.C. et le Comité permanent R ont dès lors recommandé à l'OCAM la mise en œuvre des principes contenus dans cette COL, de manière à aboutir à une alimentation et à une mise à jour systématique des BDC.

En outre, sans préjudice du principe de séparation des pouvoirs et de l'autonomie des autorités judiciaires, le C.O.C. et le Comité permanent R ont invité le ministre de la Justice à faire adapter par le Collège des Procureurs généraux la circulaire COL 18/2020 quant à la communication des mesures judiciaires portant sur les extrémistes potentiellement violents (EPV).

V.2.3. DE NOUVELLES RECOMMANDATIONS

Suite à un incident de sécurité – le Service des Cultes et de la Laïcité du SPF Justice disposait d'un accès plus large à la BDC PH que ce que prescrit l'AR PH

[280] Le C.O.C. et le Comité permanent R ont cependant noté que ce raisonnement ne s'applique pas aux jugements et aux arrêts dont les services de police n'ont pas connaissance.

– le C.O.C. et le Comité permanent R ont interpellé les responsables de traitement. Ces derniers ont été invités à mettre un terme aux accès irréguliers. Les autorités de contrôle ont recommandé à la Police fédérale d'apporter les solutions techniques nécessaires pour mettre l'accès de ce service en conformité avec la législation en vigueur (soit accès indirect à la BDC PH uniquement). Le C.O.C. et le Comité permanent R souhaitaient être tenus impérativement et précisément informés à ce propos.

Par ailleurs, ils ont recommandé aux responsables de traitement d'évaluer, sur les plans juridique et opérationnel, si la règlementation de l'accès du Service des Cultes et de la Laïcité devait (ou non) être révisée.

V.3. LA MISSION D'AVIS

La Loi sur la fonction de police (LFP) prévoit également l'obligation de recueillir l'avis conjoint du Comité permanent R et du C.O.C. dans différentes hypothèses.

Ainsi, préalablement à sa création, les ministres de l'Intérieur et de la Justice doivent déclarer la banque de données commune ainsi que les modalités de traitement, dont celles relatives à l'enregistrement des données, et les différentes catégories et types de données à caractère personnel et d'informations traitées, au Comité permanent R et au C.O.C. À leur tour, le Comité et le C.O.C. doivent émettre conjointement un avis (art.44/11/3*bis* § 3 LFP). Par ailleurs, pour chaque banque de données commune, un Arrêté royal délibéré en Conseil des ministres détermine, après avis des deux instances précitées, les règles de responsabilités en matière de protection des données à caractère personnel des organes, services, autorités et organismes traitant des données, les règles en matière de sécurité des traitements, les règles d'utilisation, de conservation et d'effacement des données (art.44/11/3*bis* § 4 LFP). En outre, des modalités complémentaires de gestion des banques de données communes peuvent être déterminées par un arrêté royal délibéré en Conseil des ministres, toujours après un avis du Comité permanent R et du C.O.C. (art.44/11/3*bis* § 8 LFP). Enfin, la fonction d'avis s'exerce également en ce qui concerne tout projet d'Arrêté royal instaurant ou modifiant les accès aux banques de données communes (art.44/11/3*ter* §§ 2 à 4).

Le Comité permanent R et le C.O.C. n'ont pas été sollicités en 2021 dans ce contexte.

CHAPITRE VI.
AVIS

L'article 33 de la Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (L.Contrôle) stipule que le Comité « *ne peut rendre un avis sur un projet de loi, d'arrêté royal, de circulaire, ou sur des documents de toutes natures exprimant les orientations politiques des ministres compétents, qu'à la demande de la Chambre des représentants ou du Ministre compétent* ».

En 2021, l'avis du Comité permanent R a été sollicité à six reprises.[281] La Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières Administratives a adressé deux demandes d'avis au Comité concernant la création d'une agence fédérale de renseignement (VI.1.) et concernant les incriminations visant à promouvoir la résilience démocratique (VI.5.). La Chambre des représentants a également introduit une demande d'avis auprès du Comité (sur l'obligation de notification (VI.2.)). Le ministre de la Justice a, à son tour, sollicité deux fois l'avis du Comité (sur la rétention des données (VI.3.) et sur les modifications de la Loi organique des services de renseignements (VI.4.)). Enfin, conjointement avec le Comité permanent P, un avis a été émis à la demande du ministre de l'Intérieur (relatif aux modifications de la L.OCAM (VI.6.)).[282] Les avis sont résumés, en ordre chronologique, dans le présent chapitre. Ils sont consultables, dans leur intégralité, sur le site internet du Comité.[283]

Par ailleurs, le Comité doit rendre des avis en tant qu'autorité de contrôle compétente (ACC) dans le cadre des traitements de données à caractère personnel ainsi que dans le cadre de la réglementation relative aux banques de données communes, et ce conjointement avec l'Organe de contrôle de l'information policière (C.O.C.). Ces deux compétences d'avis sont traitées respectivement au Chapitre IV. et au Chapitre V.

---

281 Le Comité est de plus en plus sollicité sur la base de l'article 33 L.Contrôle; le temps consacré à la formulation d'avis a, par conséquent, considérablement augmenté.

282 Les Comités permanents R et P ont formulé cet avis tant en leur qualité d'organes de contrôle de l'OCAM en vertu de la L.Contrôle qu'en leur qualité d'autorités de protection des données à l'égard des traitements de données à caractère personnel par l'OCAM.

283 www.comiteri.be.

VI.1. AVIS RELATIF À LA CRÉATION D'UNE AGENCE FÉDÉRALE DU RENSEIGNEMENT

Le Comité permanent R a été sollicité en décembre 2020 par la Commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives de la Chambre des représentants pour rendre un avis dans le cadre de l'examen de la proposition de résolution visant à la création d'une agence fédérale du renseignement.[284]

Cette proposition de résolution visait à demander au gouvernement fédéral de :

- procéder à un audit des services de renseignement et d'un service de la police fédérale (DR3) portant sur la circulation de l'information au sein et entre ces services ;
- créer, sur la base de cet audit, une agence nationale de renseignement regroupant les services de renseignement existants sous la tutelle du Premier ministre ;
- mettre à la disposition de cette agence des moyens humains et techniques nécessaires à l'exécution de ses missions.

Dans son avis, le Comité permanent R s'est dit prêt à participer (en collaboration avec le Comité permanent P et l'Organe de contrôle de l'information policière (C.O.C.) également compétents) à cet audit, dont la portée se devait cependant d'être mieux précisée. À cet égard, il a rappelé la pluralité des acteurs et partenaires belges compétents dans le cadre de la lutte contre la menace terroriste. Il a également souligné qu'il était prématuré de tirer des conclusions quant à la nécessité de créer une nouvelle institution regroupant un seul service de renseignement et un seul service de la Police fédérale (et des moyens à mettre à disposition de cette agence) sans disposer des résultats de l'audit sollicité.

VI.2. AVIS RELATIF À L'INSTAURATION D'UNE OBLIGATION DE NOTIFICATION POUR LES SERVICES DE RENSEIGNEMENT

Fin janvier 2021, une proposition de loi a été déposée visant à modifier la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) en vue de l'instauration d'une obligation de notification active pour certaines méthodes spécifiques de collecte de données.[285] Cette proposition de loi visait

---

[284] Ce projet de résolution a été déposé à la Chambre en septembre 2019. En avril 2022, il était toujours pendant (*Doc.Parl.* Chambre 2019-2020, 55-0287).

[285] *Doc.Parl.* Chambre 2020-2021, 55-1763/001. Le Comité a reçu la demande d'avis de la Chambre des représentants le 6 mai 2021 et a rendu son avis le 31 mai 2021. Le président du Comité a présenté cet avis en Commission Justice le 2 juin 2021. En avril 2022, le projet était toujours pendant à la Chambre.

à introduire, dans le chef des services de renseignement belges, d'une part et principalement une obligation de notification active, et d'autre, une obligation de notification passive.

Une *obligation de notification active* signifie que, sous certaines conditions, les services de renseignement informent de leur propre chef une personne visée qu'elle a fait l'objet d'une méthode de renseignement donnée dans le passé.

Une *obligation de notification passive* signifie qu'à la requête de toute personne ayant un intérêt personnel et légitime qui relève de la juridiction belge, le service de renseignement concerné doit informer celle-ci, moyennant certaines conditions et modalités, qu'elle a fait l'objet d'une méthode de renseignement dans le passé.

VI.2.1. LA NOTIFICATION ACTIVE

La question de savoir si un pays européen est tenu d'instaurer une obligation de notification active, trouve sa réponse dans la Convention européenne des droits de l'homme (CEDH), la jurisprudence de la Cour européenne des droits de l'homme, la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (modernisée en Convention 108+)[286] et, le cas échéant, dans la Constitution et la jurisprudence applicable de la Cour constitutionnelle du pays concerné.

Le Comité a constaté dans son avis que ni la CEDH ni la jurisprudence de la Cour européenne ne contenaient une obligation explicite pour les États parties d'instaurer à tout moment une telle obligation active de notification. Selon la Cour, le poids d'une telle obligation doit être mis en balance avec l'ensemble des garanties juridiques existantes. C'est donc l'ensemble des règles pertinentes du droit national, y compris celles régissant la transparence à l'égard de la personne concernée, qui doit être évalué.

S'appuyant sur deux arrêts de la Cour constitutionnelle[287] et sur la jurisprudence de la Cour européenne, l'exposé des motifs de la proposition de loi indiquait qu'il était nécessaire d'introduire la notification active. Le Comité a cependant estimé

---

[286] Convention du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel Convention 108), amendée par le Protocole n° 223 du 18 mai 2018 (Convention 108+). Lorsque l'avis a été remis, la Convention 108+ n'était pas encore en vigueur en Belgique (raison pour laquelle le « + » a été mis entre parenthèses dans la suite des développements). Voir https://www.coe.int/fr/web/data-protection/convention108-and-protocol.

[287] Une obligation de notification avait déjà été introduite en 2010 et 2017 par le législateur à l'article 2 § 3 L. R&S. La Cour constitutionnelle a cependant annulé l'article 2 § 3 L. R&S à deux reprises, considérant que les garanties juridiques procédurales existantes étaient insuffisantes pour justifier l'absence d'une obligation de notification active pour les services de renseignement.

que cette affirmation devait être nuancée dès lors que depuis les lois de 2010 et 2017[288], le législateur avait mis en place de nouvelles garanties procédurales.[289]

La protection juridique des citoyens – et notamment le droit à la vie privée, le droit à la protection des données à caractère personnel et le droit à un recours effectif – a été largement modifiée et rehaussée grâce à la Loi du 30 mars 2018 relative à la protection des personnes physiques à l'égard des traitements des données (LPD). Avec cette loi, le législateur a non seulement élargi et clarifié le cadre réglementaire des services de renseignement (articles 72 à 104 LPD[290]), mais il a également introduit un mécanisme de contrôle correctif renforcé en désignant le Comité permanent R comme l'autorité compétente en matière de protection des données (DPA) dans le domaine de la 'sécurité nationale'.[291] Depuis la LPD, tout acte de collecte, de traitement, d'analyse et de transmission d'informations, ainsi que toute conservation de données, est soumis au contrôle correctif du Comité lorsqu'il s'agit de traitement de données à caractère personnel.[292] Ce qui est significatif à la lumière du droit à un recours effectif, c'est que, contrairement à une plainte MRD[293] dans laquelle le requérant doit énoncer ses griefs et démontrer son intérêt personnel et légitime, aucune condition formelle de ce type n'est requise lors de l'introduction de la demande visée à l'article 51/2 de la L.Contrôle : « *Pour être recevable, la requête est écrite, datée, signée et motivée, et justifier de l'identité de la personne concernée* ». Et dans la pratique, le Comité adopte une approche très souple quant à l'exigence de motivation. Contrairement à la situation antérieure

---

288 Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité, *M.B.* 10 mars 2010 et Loi du 30 mars 2017 modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal, *M.B.* 28 avril 2017.

289 En sus, le Comité a souhaité faire remarquer que ni l'exposé des motifs de la Loi du 30 mars 2017 ni la Cour constitutionnelle ne faisaient référence aux garanties procédurales prévues par la Loi du 11 avril 1994 relative à la publicité de l'administration (LPA). Pourtant la problématique de la notification active pourrait également être analysée dans le cadre du droit d'accès aux documents administratifs et aux informations des services de renseignement dès lors que, dans une certaine mesure, cette législation permet l'information de la personne concernée. Tant le Conseil d'État que la Commission d'accès aux documents administratifs ont en effet confirmé à maintes reprises que la LPA s'applique à la VSSE et au SGRS.

290 Le sous-titre 1er titre 3 de la LPD (artt. 72 à 104 LPD) règle le traitement des données à caractère personnel par la VSSE et le SGRS dans le cadre de l'exécution de leurs missions, à l'exception des traitements de données à caractère personnel dans le cadre de la Loi du 11 décembre 1998 relative à la Classification. Ce dernier point est traité au sous-titre 3 du titre 3 de la LDP (artt. 106 à 137 LPD).

291 COMITÉ PERMANENT R, *Rapport d'activités 2019*, 75-80.

292 Compte tenu de l'interprétation large donnée par les traités à la notion de 'traitement de données à caractère personnel' (*cf.* article 8 de la CEDH, *i.o.* Convention n° 108(+)) tous les traitements de données à caractère personnel effectués par les services de renseignement sont soumis au contrôle APD du Comité. En sa qualité d'autorité de protection des données, le Comité permanent R agit soit d'initiative, soit à la demande d'une autre autorité de protection de données, ou encore à la requête de toute personne concernée.

293 Visé à l'article 43/4, alinéa 1er, troisième tiret L.R&S.

à la Loi sur la protection des données, le droit à un recours effectif est donc sensiblement amélioré.

Le Comité a indiqué que le renforcement de ses attributions consécutif à l'adoption de la LPD en 2018, conjugué à la mise en place d'un système de notification passive[294] prévue par ladite proposition, permettait à ses yeux de rencontrer l'exigence de transparence issue du droit international. À la lumière de cette constatation, le Comité a considéré que le législateur fédéral n'avait pas d'obligation conventionnelle d'instaurer une obligation de notification active, pour autant que la proposition introduise bien une obligation de notification passive tenant compte des commentaires du Comité (*infra*).

Néanmoins, le Comité a souhaité ajouter et souligner que le législateur fédéral était libre d'instaurer un tel mécanisme.[295] Et dans l'éventualité où le législateur faisait ce choix, le Comité a formulé un certain nombre de commentaires sur les différents articles relatifs à l'obligation de notification active. Les remarques avaient notamment trait :

- au choix (inexpliqué) opéré dans la proposition de loi de limiter le champ d'application à certaines MRD ;
- à la différence observée avec l'obligation de notification active qui existe dans la procédure pénale (article 90*novies* CIC) ;
- aux motifs d'exception qui devraient s'aligner davantage sur ceux déjà contenus dans plusieurs réglementations (LPA, L.C&HS, L.R&S et L.Organe de recours) ;
- aux personnes à notifier ;
- au délai de notification ;
- à l'autorité de contrôle, le Comité étant d'avis qu'une instance de contrôle suffit.

Par ailleurs, le Comité a recommandé que des moyens supplémentaires soient alloués aux deux services de renseignement en cas d'instauration d'une telle obligation. Sans ces ressources supplémentaires, l'introduction d'une telle obligation de notification active affecterait les priorités stratégiques et opérationnelles de la VSSE et du SGRS.

VI.2.2. LA NOTIFICATION PASSIVE

Tout en accueillant positivement la proposition de réintroduire la notification passive, le Comité a relevé que différents systèmes, compétences et procédures existaient déjà en matière de transparence des informations en possession des services de renseignement. À cet égard, le Comité a souligné que les possibilités d'action étaient complexes à cerner et à mettre en œuvre pour le citoyen et que le

294 Prenant en considération les observations formulées dans l'avis rendu.

295 Le Comité a relevé dans son avis qu'une décision d'introduire (une certaine forme) d'obligation de notification active avait été prise dans 6 des 47 États membres du Conseil de l'Europe.

choix d'une procédure avait actuellement un impact sur ses possibilités d'accès (ou non) à de l'information. Aux yeux du Comité, une harmonisation des procédures d'accès à l'information et des exceptions à la communication d'information – et donc une harmonisation du résultat des différentes procédures – était dès lors souhaitable.

Dans le même ordre d'idées, le Comité a souhaité attirer l'attention du législateur sur la nécessité d'expliciter et de préciser davantage dans l'exposé des motifs la manière dont le système de notification passive s'articulerait avec les procédures existantes.

VI.3. AVIS RELATIF À LA RÉTENTION DES DONNÉES

Le Comité permanent R a été sollicité par le ministre de la Justice pour rendre un avis sur le projet de loi 'relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités' (ci-après : le projet de loi).[296] [297] Suite à l'annulation par la Cour constitutionnelle des articles 2, b), 3 à 11 et 14 de la Loi du 29 mai 2016 'relative à la collecte et à la conservation des données dans le secteur des communications électroniques'[298], le projet de loi visait à instaurer un système de conservation des données de communication qui respecte les exigences imposées par la Cour de justice de l'Union européenne (CJUE). Pour ce faire, il entendait modifier plusieurs lois parmi lesquelles la Loi du 13 juin 2005 relative aux communications électroniques (Loi LCE) et la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S).

Le Comité permanent R a discuté, dans son avis, les modifications proposées dans la L.R&S, et les modifications proposées dans la Loi LCE relevant de sa compétence.[299]

---

296 Le Comité permanent R a reçu la demande le 7 mai 2021 et a rendu son avis le 15 juin 2021.

297 L'avant-projet a été approuvé en deuxième lecture par le Conseil des ministres en décembre 2021 et déposé à la Chambre en mars 2022. Toujours en mars 2022, 18 amendements ont été approuvés par le Conseil des ministres (suite à l'arrêt n° 158/2021 pris par la Cour constitutionnelle le 18 novembre 2021). Les avis du Conseil d'État et de l'APD sur ces amendements ont été sollicités. L'APD a remis un avis le 1er avril 2022 (Voir avis n°66/2022 de l'APD).

298 Cette loi avait été annulée en raison de sa contrariété avec le droit européen et la jurisprudence de la CJUE.

299 Le Comité ne s'est pas prononcé quant à la question de savoir si les modifications apportées à la Loi LCE par le projet rencontraient ou non les exigences consacrées dans les jurisprudences de la CJUE et de la Cour constitutionnelle belge. Cf. l'avis de l'autorité de protection des données rendue sur le projet de loi https://www.autoriteprotectiondonnees.be/publications/avis-n-108-2021.pdf

VI.3.1. MODIFICATIONS À LA LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT

VI.3.1.1. Conservation ciblée des données de trafic et de localisation

Le gouvernement proposait d'inclure dans la L.R&S une nouvelle méthode ordinaire de conservation ciblée des données de trafic et de localisation dans le secteur des communications électroniques.

Le Comité a relevé une divergence inexpliquée dans le niveau de protection juridique qu'offrait le projet de loi dans le cadre de la conservation ciblée selon que cette dernière était opérée dans le cadre d'une procédure pénale ou d'une procédure de renseignement.

Il notait par ailleurs que le mécanisme de contrôle proposé dans le cadre de la procédure de renseignement – à savoir une notification mensuelle des méthodes utilisées (donc après la mise en œuvre de plusieurs méthodes) – n'était pas suffisant et ne répondait pas à l'exigence de la CJUE qui estime que la conservation ciblée des données de trafic et de localisation nécessite que la décision de l'autorité compétente soit soumise à un contrôle juridictionnel effectif.

Le Comité a également pointé un pouvoir de délégation inapproprié dans le cadre de cette nouvelle méthode ordinaire de conservation ciblée qui concerne les données de trafic et de localisation relatives aux communications électroniques. Le gouvernement proposait que le pouvoir de réquisition de ces données puisse être exercé par « *le dirigeant de service ou son délégué* ». À l'instar de la Cour constitutionnelle et de la Cour EDH, le Comité est d'avis que de telles données sont très intrusives. Il ne perçoit pas de justification à l'instauration d'un pouvoir de délégation supplémentaire que celui déjà inscrit dans la L.R&S[300], et a invité par conséquent le gouvernement à motiver ce choix.

VI.3.1.2. Accès aux données de trafic et de localisation

Le projet de loi visait à rétablir l'article 18/8 L.R&S, qui a été en grande partie annulé par la Cour constitutionnelle[301] et qui réglait l'accès aux données relatives au trafic et à la localisation des communications électroniques par les services de renseignement.

Le Comité a rappelé que la Cour constitutionnelle avait annulé l'intégralité de l'article 18/8 L.R&S. De l'avis du Comité, il était prématuré de conclure que seule

---

300 La définition juridique de la notion de dirigeant du service contient déjà un pouvoir de délégation : en cas d'empêchement de l'Administrateur général de la VSSE ou du Chef du SGRS, les dirigeants des service respectifs ont la possibilité de déléguer leur pouvoir de décision à, respectivement, l'Administrateur général ou au chef de service faisant fonction. Cette délégation n'est pas limitée à l'Administrateur général adjoint de la VSSE et au Chef adjoint du SGRS. En cas d'empêchement de ces derniers, une nouvelle délégation peut être faite à un niveau inférieur de la hiérarchie.

301 C.C., 22 avril 2021, n° 57/2021.

l'annulation du paragraphe 2 s'imposait à la lumière de jurisprudence de la Cour constitutionnelle et de la Cour EDH. Ce sont les garanties juridiques procédurales dans leur ensemble qui doivent être prises en considération.

VI.3.1.3. Conservation généralisée et indifférenciée des données de trafic et de localisation

Le projet de loi proposait d'inscrire dans la L.R&S une nouvelle méthode exceptionnelle dans le cadre de la conservation des données relatives au trafic et à la localisation dans le secteur des communications électroniques lorsqu'il existe une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Dans ce cas, le projet prévoyait la possibilité pour les services de renseignement de requérir le concours des opérateurs pour procéder à la conservation généralisée et indifférenciée des données de trafic et de localisation de moyens de communications électroniques générées et traités par eux.

Le Comité souscrivait pleinement à la proposition de soumettre l'utilisation de cette compétence à tous les mécanismes de contrôle inhérents aux méthodes exceptionnelles.

Il recommandait de renforcer le lien entre la disposition réglant l'accès et celle réglant la conservation généralisée. Tel que le projet était rédigé, il était possible qu'une menace bien définie (par exemple, le terrorisme) puisse justifier l'imposition d'une conservation généralisée et indifférenciée aux opérateurs de télécommunications, sans aucune limitation ultérieure, et que l'accès à ces données puisse également être utilisé à d'autres fins (par exemple, dans le cadre de la lutte contre d'autres menaces).

Par ailleurs, dans l'exposé des motifs, il était indiqué que : « *l'autorisation prise par le dirigeant du service concerné de mettre en œuvre cette méthode exceptionnelle est transmise au ministre compétent pour information. Il convient de préciser que le but est donc d'informer le ministre compétent qu'une conservation indifférenciée est déclenchée* ».[302] Le Comité recommandait que le ministre concerné soit informé non seulement de 'l'autorisation' définitive du dirigeant du service, mais aussi du 'projet d'autorisation'. Ni la notification du projet d'autorisation ni la notification de l'autorisation ne sont prévues dans la procédure MRD pour les méthodes exceptionnelles. Toutefois, le Comité estimait que si les services de renseignement ordonnent aux opérateurs de télécommunications une conservation généralisée et indifférenciée[303] des données de trafic et de localisation, l'impact en termes

[302] Avant-projet de Loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités, pp.111-112.

[303] Par opposition aux autres méthodes exceptionnelles qui sont ciblées (cf. art. 18/10, §2, 2° L.R&S).

d'ingérence dans la vie privée des citoyens belges et des résidents sur le territoire belge est tel que pareilles exigences de forme divergentes se justifient.[304]

Le Comité a également pointé l'absence de motivation justifiant des délais de conservation des données[305] et de rapportage[306] différents de ceux d'application dans le cadre des méthodes exceptionnelles.

Le Comité recommandait encore de clarifier le rapport entre cette mesure et le régime de protection particulier pour les avocats, les médecins et les journalistes prévu par la L.R&S.[307]

VI.3.1.4. Notification obligatoire des décisions du Comité aux opérateurs

Le Comité recommandait aussi de créer une obligation pour les services de renseignement d'informer les opérateurs concernés lorsque le Comité permanent R avait ordonné la cessation d'une conservation généralisée et indifférenciée ou d'une conservation ciblée.

VI.3.2. MODIFICATIONS À LA LOI TÉLÉCOM (LCE)

Le Comité a également formulé plusieurs remarques quant aux modifications proposées dans la Loi LCE. Tout d'abord, le projet de loi proposait, dans le cadre de la conservation ciblée de données en cas de menace grave, réelle et actuelle pour la sécurité nationale, que celle-ci s'opère pour toutes les 'zones' dont le niveau de la menace évaluée par l'OCAM soit au moins de niveau 3, et aussi longtemps qu'un niveau 3 perdure pour ces 'zones'. Le Comité invitait à préciser la notion de 'zones' afin de clarifier à quoi celles-ci se référaient.

Le projet chargeait les services de renseignement d'établir une liste annuelle « *(d)es bâtiments affectés aux personnes morales dont le potentiel économique et/ou scientifique doit être protégé* », devant être approuvée par le Conseil national

---

304 La notification du projet d'autorisation au ministre compétent n'aurait pas pour but de porter le pouvoir décisionnel au niveau ministériel, mais de rendre obligatoire l'information du gouvernement sur le fait que, selon le service de renseignement concerné, il existe un danger pour la sécurité nationale d'un niveau si élevé qu'une mesure aussi intrusive de conservation généralisée et indifférenciée des données de communication en question semble justifiée.

305 Le projet proposait une durée de conservation de maximum six mois au lieu de deux mois prolongeable.

306 Le projet proposait un rapport tous les deux mois, ce qui s'écarte du rapportage une fois toutes les deux semaines qui est imposé pour les autres méthodes exceptionnelles.

307 En vertu de l'article 18/9, § 4 L.R&S, des méthodes exceptionnelles ne peuvent être utilisées contre l'une de ces professions protégées ou, entre autres, contre les moyens de communication utilisés à des fins professionnelles, que si le service de renseignement dispose au préalable d'indices sérieux révélant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement d'une menace potentielle grave. Le cas échéant, il y a lieu de suivre une procédure particulière.

de sécurité. À cet égard, le Comité a rappelé l'existence du Plan d'action du gouvernement fédéral pour la sauvegarde du potentiel scientifique et économique[308]. Ce plan d'action contient également une liste d'entités. Le Comité constatait que la liste établie en 2007 n'avait pas été actualisée depuis et se demandait, par conséquent, si la mise à jour annuelle prévue par le projet de loi était réaliste.

Le Comité relevait encore que le projet ne prévoyait pas d'obligation de notification aux autorités de protection des données vis-à-vis de l'OCAM (à savoir le Comité permanent R et le Comité permanent P) en cas de conservation géographique ciblée effectuée sur la base du niveau de menace général tel que déterminé par l'OCAM. Il recommandait d'établir une obligation de notification pour le Comité permanent R et d'interroger le Comité permanent P à cet égard.

VI.4. AVIS CONCERNANT L'AVANT-PROJET DE LOI MODIFIANT LA LOI ORGANIQUE DES SERVICES DE RENSEIGNEMENT

À la demande du ministre de la Justice, le Comité permanent R a rendu un avis concernant l'avant-projet de loi 'modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité'.[309] [310] Le projet de loi prévoyait notamment, pour les agents des services de renseignement, un élargissement des possibilités de commettre des infractions ainsi qu'une procédure spécifique pour l'utilisation des identités fictives. Il introduisait également la possibilité pour les sources humaines de commettre certaines infractions ainsi que la possibilité de réaliser des MRD pour contrôler la fiabilité d'une soucre. Le projet visait également à introduire une nouvelle compétence pour le SGRS en cas de crise nationale de cybersécurité. Un remaniement de la méthode de collecte déjà existante auprès des institutions bancaires et financières était également proposé.

VI.4.1. UNE RÉGLEMENTATION TROP COMPLEXE

De manière générale, le Comité constatait dans son avis que les modifications législatives proposées rendaient beaucoup plus complexe et incohérente la réglementation qui s'applique à la VSSE et au SGRS. Le Comité déplorait que le

308 Ce plan a été approuvé le 16 mars 2007 par le Comité ministériel du renseignement et de la sécurité (aujourd'hui, le Conseil national de sécurité).

309 Le ministre a fait sa demande le 31 mai 2021; le Comité a rendu son avis le 15 juin 2021. C'était le deuxième avis du Comité dans ce contexte. À la demande du ministre de la Justice, le Comité avait déjà rendu un avis le 16 novembre 2018 sur un projet de loi dans lequel les mesures proposées étaient (en grande partie) les mêmes.

310 En avril 2022, cet avant-projet n'avait pas (encore) été approuvé en deuxième lecture par le Conseil des ministres.

projet de loi s'inscrivait dans l'évolution de ces dernières années d'abandonner la structure logique - mise en place par le législateur MRD en 2010 - dans la L.R&S en ce qui concerne les compétences (d'enquête) des services de renseignement.
Le Comité notait en outre que certains choix opérés dans le projet de loi étaient inutilement compliqués et incomplets, ce qui n'allait pas favoriser, selon le Comité, une bonne application de la législation en question.

VI.4.2. CYBERSÉCURITÉ - MISSION DU SGRS

Le projet de loi conférait au SGRS la nouvelle compétence de « *neutraliser, dans le cadre d'une crise nationale de cybersécurité, une cyberattaque de systèmes informatiques et de communications non gérés par la Défense et d'en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit international* ».
Le Comité constatait que cette nouvelle mission complétait la mission de cybersécurité existante[311], en offrant la possibilité au SGRS d'agir contre une cyberattaque menée contre les systèmes informatiques et de communications qui ne sont pas gérés par le ministre de la Défense. La compétence matérielle du SGRS dans le cadre de cette mission, était déterminée par la proposition de définition du concept de « *crise nationale de cybersécurité* », à savoir « *tout incident de cybersécurité qui, par sa nature ou ses conséquences :*
- *menace les intérêts vitaux du pays ou les besoins essentiels de la population ;*
- *requiert des décisions urgentes ;*
- *et demande une action coordonnée de plusieurs départements et organismes* ».[312]

De l'avis du Comité, les entités à protéger étaient définies de manière trop large dans le projet de loi, l'expression 'les intérêts vitaux du pays ou les besoins essentiels de la population' n'étant pas suffisament définie. Le Comité recommandait de délimiter le champ d'action aux 'infrastructures critiques' (cf. la Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques).

Outre la compétence de 'neutraliser' une cyberattaque, le projet octroyait au SGRS la compétence de réagir par 'une propre cyberattaque'. Le Comité s'interrogeait, dans son avis, sur le cadre juridique à respecter dans la mise en œuvre d'un tel pouvoir d'attaque qui s'inscrit dans le droit de la guerre. Des

311 Cette compétence est définie à l'article l'article 11, § 1er, 2° L.R&S et permet SGRS d'agir contre une cyberattaque de systèmes informatiques et de communications gérés par le ministre de la Défense.

312 L'exposé des motifs précisait que la définition du mot « crise » avait été reprise de l'article 2 de l'Arrêté royal du 18 avril 1988' portant création du Centre gouvernemental de Coordination et de Crise'.

éclaircissements quant la manière dont le droit de la guerre s'articulerait dans pareil cas avec le droit penal étaient nécessaires.[313]

VI.4.3. LA COMMISSION D'INFRACTIONS D'APPUI

VI.4.3.1. Généralités

Le projet de loi permettait la commission d'infractions en appui à l'exécution de différents types de missions de la VSSE et du SGRS. Le Comité recommandait de supprimer la possibilité de commettre des infractions par le SGRS dans le cadre de ses missions du maintien de la sécurité militaire et la protection du secret. Le Comité n'en voyait pas la nécessité, et aucun motif n'était développé pour en justifier le besoin.

Le projet de loi contenait également une liste d'infractions ne pouvant pas être commises par les agents des services de renseignement ou par les sources humaines (HUMINT). Le Comité constatait que cette liste n'était pas exhaustive et il proposait d'y ajouter plusieurs infractions.

Par ailleurs, le Comité déplorait que le projet de loi ne permettait pas à la Commission BIM d'imposer une interdiction d'exploitation et une ordonnance de destruction des données collectées lorsque des infractions d'appui étaient commises illégalement dans le cadre de l'utilisation de méthodes ordinaires. Il recommandait de donner à la Commission BIM les mêmes compétences de contrôle et de sanction que celles dont elle dispose pour le contrôle des méthodes exceptionnelles (cf. article 18/10, § 6 L.R&S). En conséquence, la 'commission d'infractions' ne deviendrait pas une méthode exceptionnelle, mais elle serait contrôlée comme les méthodes exceptionnelles. Le même niveau de protection juridique s'appliquerait donc.

VI.4.3.2. Lacune dans la procédure pénale

Le Comité attirait également l'attention sur l'absence d'une procédure de contrôle sur la régularité de l'enquête de renseignement au cours de la procédure pénale, à l'instar de la mission de contrôle dont est animée la chambre des mises en accusation dans l'enquête judiciaire (cf. art. 235*bis* et suiv. CIC). En dehors d'une

313 Sachant qu'une cyberattaque contre les infrastructures IT belges constitue en soi une infraction, la question se posait de savoir si une telle cyberattaque n'interfèrerait pas avec les missions judiciaires. Une situation dans laquelle une infraction avec une dimension purement nationale serait commise devrait être traitée par le droit pénal.

procédure à portée limitée[314], il n'existe pas de procédure comparable. Ce contrôle est pourtant nécessaire, puisqu'un dossier pénal peut également contenir des notes des services de renseignement.

Le Comité recommandait par conséquent de généraliser la 'procédure d'avis préjudiciel en matière pénale'. Les tribunaux pénaux devraient ainsi avoir la possibilité d'interroger le Comité permanent R sur la légalité des données de renseignement contenues dans le dossier pénal.

VI.4.3.3. La commission d'infractions par des agents

Afin d'assurer le suivi de la commission d'une infraction ayant été autorisée par la Commission BIM pour un agent, le Comité recommandait que soit indiqué, dans la demande écrite d'autorisation, le nom de la personne chargée du contrôle de l'utilisation de cette mesure.[315]

Pour garantir la protection des agents, le Comité recommandait également de prévoir la possibilité d'un recours juridictionnel auprès du Comité contre une décision négative de la Commission BIM devant statuer – dans le cadre d'une procédure exceptionnelle lors de laquelle elle n'avait pas été invitée *a priori* à autoriser la commission d'infraction – sur le caractère imprévisible et strictement nécessaire de l'infraction commise.

VI.4.3.4. La commission d'infractions par des informateurs

Quant aux infractions commises par des sources humaines, le Comité recommandait de préciser que celles-ci n'étaient autorisées que dans le cadre des missions de renseignement. Il estimait ensuite que le champ d'application matériel de cette exemption de peine n'était pas suffisamment clair vu l'absence de définition légale du concept de 'sources humaines'.

Pour assurer un contrôle efficace, le Comité recommandait que soit inscrit, dans la demande d'autorisation, le nom de l'agent traitant de la source humaine concernée. Le Comité estimait également que les organes de contrôle concernés devaient être habilités à prendre connaissance de l'identité de l'informateur.[316]

---

314 Il s'agit de la procédure dite « d'avis préjudiciel » (cf. art. 131*bis*, 189*quater* et 279*bis* CIC) dans laquelle un tribunal pénal peut interroger le Comité permanent R quant à la régularité des méthodes qui ont conduit à la rédaction d'un « procès-verbal non classifié » (cf. art. 19/1 L.R&S). Ce procès-verbal est établi par la Commission BIM lorsque des indices d'infractions sont mis en évidence par l'utilisation de MRD.

315 Le Comité admet qu'il n'est pas toujours possible de connaître à l'avance le nom de l'agent chargé de mettre en œuvre une méthode de renseignement ou une mesure de protection et d'appui. Mais ce n'est pas le cas de la personne chargée du suivi de la mesure.

316 Donner à un informateur (c'est-à-dire une personne privée) l'autorisation de commettre des délits sans que la Commission BIM ne sache à qui cette autorisation est donnée rend impossible un contrôle efficace.

VI.4.3.5. Dommages subis ou causés par une source humaine

Le projet instaurait une procédure – ainsi qu'un système d'indemnisation – pour régler les cas de dommages subis ou causés par une source humaine pendant sa mission. Le Comité soulignait le manque de clarté dans la description de la procédure.

VI.4.3.6. Protection juridique insuffisante de la source humaine

Le Comité constatait que le projet de loi ne prévoyait pas un degré adéquat de protection juridique pour la source humaine ayant obtenu l'autorisation de commettre certaines infractions. La question de savoir comment les autorités judiciaires concernées pouvaient savoir avec certitude qu'une personne verbalisée avait été autorisée par la Commission BIM à commettre certaines infractions demeurait sans réponse.[317] Le Comité recommandait diverses mesures pour y remédier.[318]

VI.4.4. IDENTITÉ ET QUALITÉ FICTIVES COMME MESURE D'APPUI À UNE MÉTHODE DE RENSEIGNEMENT OU UNIQUEMENT POUR DES RAISONS DE SÉCURITÉ

Le projet de loi modifiait la procédure – établie à l'article 13/2 L.R&S – pour la création et l'utilisation d'une identité fictive et créait une nouvelle compétence en matière d'utilisation d'une identité fictive à des fins de collecte d'informations.

Le Comité recommandait de permettre à la Commission BIM de réaliser un contrôle dans tous les cas de figure où celle-ci est d'avis que l'identité fictive est utilisée pour la collecte d'informations (et ce, même si le service concerné avance d'autres motifs pour justifier le recours à l'identité fictive). Le Comité invitait également à préciser dans la loi la signification exacte de 'l'identité fictive' et de la 'qualité fictive'.[319]

---

317 Ceci est problématique puisque le parquet, la juridiction d'instruction ou, en dernière instance, la juridiction de jugement sont les autorités compétentes pour juger de l'existence concrète d'une exemption de peine dans le chef de la personne verbalisée.

318 Telles que la possibilité pour la Commission BIM de rédiger, dans certains cas, un acte décrivant son autorisation pour la commission de certaines infractions ; la conclusion d'un protocole d'accord entre les services de renseignement, la Commission BIM et le Collège de procureurs généraux visant à garantir un canal de communication effectif entre ces acteurs relatif à cette question.

319 Le Comité s'interrogeait notamment sur le fait de savoir si le simple fait d'omettre délibérément de révéler à un interlocuteur la qualité d'un membre d'un service de renseignement lors de la collecte de données revenait à utiliser une qualité fictive.

VI.4.5. INFILTRATION DANS LE MONDE RÉEL ET VIRTUEL

Le projet de loi optait pour une exécution indirecte du contrôle de la compétence d'infiltration via le contrôle de la commission d'infractions et/ou l'utilisation d'une identité fictive. La procédure qui en découlait était inutilement compliquée, incomplète et ne répondait en aucun cas aux garanties juridiques nécessaires dans le cadre d'un pouvoir d'investigation d'une telle ampleur. Un avis négatif a donc été rendu par le Comité quant à l'exécution de ce contrôle. Il estimait en effet que le projet de loi ne répondait pas aux exigences fixées par la Commission d'enquête parlementaire « Attentats » en termes de protection juridique.[320]

Le projet de loi considérait cette nouvelle compétence comme une méthode ordinaire. Compte tenu de la manière dont l'infiltration est organisée dans la procédure pénale, le Comité recommandait de considérer 'l'infiltration dans le monde réel' comme une méthode exceptionnelle et 'l'infiltration dans le monde virtuel' comme une méthode spécifique.

Par ailleurs, le Comité constatait que la procédure d'autorisation prévue donnait l'impression – erronée – d'être identique à celle prévue pour les méthodes exceptionnelles. Divers mécanismes de contrôle applicables aux méthodes exceptionnelles n'étaient pas d'application.

Considérer le pouvoir d'infiltration comme une MRD – comme l'a suggéré le Comité dans son avis – présenterait également l'avantage de rendre possible un contrôle structuré des résultats d'enquête par la Commission BIM.[321]

VI.4.6. MÉTHODES ORDINAIRES PLUS

Dans son avis, le Comité soulignait que les garanties procédurales pour les méthodes ordinaires (MPLUS) plus n'étaient pas suffisantes et que le contrôle n'offrait pas un niveau de protection juridique adéquat. Il recommandait, par conséquent, un renforcement du contrôle des méthodes ordinaires plus (MPLUS), en traitant toutes les MPLUS de la même manière et en créant une obligation pour les services de renseignement de faire précéder chaque utilisation d'une MPLUS d'une décision

---

320 L'exposé des motifs faisait à juste titre référence au Troisième rapport intérmédiaire de la Commission d'enquête parlementaire sur les attentats terroristes, qui recommande la création d'une compétence d'infiltration pour les services de renseignement. Mais la recommandation indique également que « *(l)a réglementation légale à adopter en la matière devra toutefois prévoir les garanties nécessaires, tant en termes de protection juridique des citoyens qu'en termes de sécurité des agents de la VSSE chargés de missions d'infiltration* ». *Doc. Parl.*, Chambre, 2016-17, n° 54-1752/008.

321 Si par le passé, la procédure d'autorisation MRD n'était peut-être pas suffisamment adaptée à l'exercice d'un pouvoir d'infiltration, le législateur a depuis créé un certain nombre d'instruments dans la L.R&S pour passer outre ces obstacles.

écrite et motivée, et de communiquer chaque décision spontanément et dans les meilleurs délais au Comité.[322]

VI.4.7. RÉCLAMATION DE DONNÉES FINANCIÈRES

Le projet introduisait une nouvelle méthode ordinaire, créant une obligation pour les institutions financières, au sens large du terme, de coopérer afin d'identifier les produits ou services financiers dont dispose une personne ou, inversément, d'identifier quelle personne peut être liée à certains produits ou services financiers. Il s'agit pour l'heure d'une méthode exceptionnelle.

Le Comité recommandait de considérer cette méthode comme une méthode spécifique ne pouvant se rallier à la conclusion dans l'exposé des motifs selon laquelle « *le caractère intrusif d'une telle méthode est (...) faible à très faible* ».

VI.4.8. MOYENS EN PERSONNEL ET MOYENS FINANCIERS

Enfin, estimant que la mise en œuvre des différentes mesures élaborées dans le projet de loi créait non seulement une charge de travail supplémentaire pour les services de renseignement mais aussi pour les organes de contrôle concernés, le Comité plaidait pour que l'approbation du projet de loi soit accompagnée d'une augmentation des effectifs de la Commission BIM et du Comité permanent R.

VI.5. AVIS SUR DES PROPOSITIONS DE LOI À PROPOS D'INCRIMINATIONS VISANT À PROMOUVOIR LA RÉSILIENCE DÉMOCRATIQUE

En septembre 2021, le Comité permanent R a rendu un avis, à la demande du Président de la Commission de l'lnterieur, de la Sécurité, de la Migration et des Matières Administratives concernant trois propositions de loi:

– la proposition de loi incriminant l'appartenance ou la collaboration avec un groupement qui prône la discrimination ou la ségrégation ;

[322] En ne considérant pas les méthodes MPLUS comme des MRD, le législateur a choisi de ne pas faire effectuer de contrôle par la Commission BIM. Il a confié cette mission au Comité permanent R. Dans le cadre de son contrôle des MPLUS, le Comité, en tant que régulateur de la sécurité nationale en matière de protection des données dans ce domaine, a également le pouvoir de prendre des mesures correctrices contraignantes à l'égard de tous les traitements de données à caractère personnel effectués par les services de renseignement. En conséquence, le Comité a le pouvoir, par exemple, d'imposer une interdiction de traitement ou un effacement des données dans le cadre de son contrôle des MPLUS.

– la proposition de loi modifiant la loi du 29 juillet 1934 interdisant les milices privées en vue d'interdire les groupements non démocratiques ;
– la proposition de loi modifiant la loi du 29 juillet 1934 interdisant les milices privées, afin que les interdictions prévues par cette loi soient élargies pour viser les associations incitant à la haine, à la discrimination ou à la violence, et permettant leur dissolution par le pouvoir exécutif.[323] [324]

Les propositions législatives soumises à l'avis du Comité visaient à introduire de nouvelles dispositions pénales avec l'objectif général de promouvoir la résilience démocratique. Le Comité a limité son avis aux aspects des propositions de loi concernées qui ont ou peuvent avoir un impact sur les missions et le fonctionnement des services de renseignement et de sécurité.

VI.5.1. OBSERVATION PRÉALABLE

Le Comité a tout d'abord constaté que les actes punissables proposés pouvaient, dans certains cas, être également considérés comme des menaces pour la sécurité nationale, en ce qu'ils correspondent aux activités qui doivent être contrôlées par la VSSE, le SGRS et l'OCAM. De manière significative, l'incrimination de menaces à la sécurité nationale affecte le fonctionnement des services de renseignement et de sécurité.

En effet, la VSSE a notamment pour mission de rechercher, d'analyser et de traiter le renseignement relatif aux activités extrémistes qui menacent ou pourraient menacer la sécurité nationale. Le SGRS a lui aussi pour mission légale d'enquêter sur les activités extrémistes si celles-ci comportent un aspect militaire.

VI.5.2. COOPÉRATION ET ÉCHANGE D'INFORMATIONS AVEC LES ACTEURS JUDICIAIRES

Le Comité est d'avis qu'un élargissement (indirect) de l'arsenal pénal dans le cadre de la sécurité nationale accroit la nécessité de prévoir, de manière générale et formalisée, une coopération opérationnelle entre le Ministère Public, la Police judiciaire, la VSSE, le SGRS et l'OCAM.

Actuellement cette coopération opérationnelle et cet échange d'informations au sein de l'arrondissement judiciaire de Bruxelles sont largement organisés par

---

323 *Doc. parl.* Chambre 2021-2022, 55 n° 450/001, 55 n° 943/001 et 55 n° 2024/001.

324 Ces trois propositions de loi, encore pendantes à la Chambre en avril 2022, ont fait l'objet de débats en Commission Intérieur en juin et juillet 2021. Les rapports d'auditions ont été publiés en avril 2022.

le biais du système Joint Intelligence Centre (JIC)/ Joint Decision Centre (JDC)[325] en vue d'un échange et d'une évaluation commune des informations relatives à le menace terroriste. Dans son avis, le Comité recommandait d'examiner dans quelle mesure le système JIC/JDC devrait être étendu au suivi des menaces autres que le terrorisme, et plus particulièrement au suivi des infractions pénales proposées. Le Comité indiquait ensuite que le système JIC/JDC n'est applicable que dans l'arrondissement judiciaire de Bruxelles. Le Comité conseillait d'examiner l'utilité opérationnelle d'étendre ce système aux autres arrondissements et au suivi des infractions pénales proposées. Enfin, le Comité rappelait la recommandation de la Commission d'enquête parlementaire 'Attentats' de créer une Banque Carrefour de sécurité.

VI.5.3. COOPÉRATION ET ÉCHANGE D'INFORMATIONS AVEC LES ACTEURS ADMINISTRATIFS

Dans son avis, le Comité a également relevé que les mesures d'incrimination proposées affectent de manière significative la liberté d'expression, la liberté d'association et la liberté de réunion.

Le Comité a rappelé les obligations légales de la VSSE, du SGRS et de l'OCAM dans l'établissement des listes conjointes de 'phénomenes et de groupements à suivre' par la police : conformément à l'article 44/5, § 2 de la Loi sur la fonction de police (LFP), la VSSE, le SGRS et l'OCAM – en toute logique avec la Police fédérale – sont chargés d'établir annuellement pour le ministre de l'Intérieur 'une proposition conjointe' de listes de 'phénomènes de police administrative' et de 'groupements nationaux et internationaux susceptibles de porter atteinte à l'ordre public' et qui requièrent un suivi par la police. Le ministre de l'lntérieur établit ces listes annuellement. Dans son avis, le Comité recommandait d'examiner dans quelle mesure ces listes devaient être utilisées dans le suivi des organisations et groupements interdits visés dans les propositions de loi soumises pour avis.

[325] Le *Joint Intelligence Center* (JIC), composé de la Police judiciaire fédérale (PJF Bxl), du Service central de lutte contre le Terrorisme au sein de la Police fédérale (DJSOC/Terro), de la VSSE, du SGRS et de l'OCAM, est chargé de l'échange d'informations structurel dans le cadre de la lutte contre le terrorisme. Le JIC est également chargé d'évaluer conjointement tout nouveau renseignement relatif à la menace terroriste recueilli par l'un des services partenaires et de formuler une proposition de suivi approprié (suivi judiciaire/renseignement/autre). Le *Joint Decision Center* (JDC), composé des représentants du JIC, du ministère public et du directeur-coordinateur administratif de la police de Bruxelles, décide ensuite du suivi de manière collégiale.

VI.6. AVIS COMMUN SUR L'AVANT-PROJET DE LOI MODIFIANT LA LOI OCAM

En août 2021, les Comités permanents R et P ont été saisis par le ministre de l'Interieur et l'Autorité de protection des données afin de rendre un avis commun sur l'avant-projet de loi modifiant la loi du 10 juillet 2006 relative à l'analyse de la menace (L.OCAM).[326] Sur certains points, le Comité permanent R a formulé des observations en son nom seul.

VI.6.1. EXTENSION DE LA LISTE DES SERVICES D'APPUI

L'avant-projet de loi visait tout d'abord à conférer un ancrage légal (dans la L.OCAM) aux quatre services publics désignés en tant que services d'appui de l'OCAM par l'Arrêté royal du 17 août 2018.[327]

En effet, alors que la L.OCAM prévoit que les services d'appui désignés par arrêté royal soient confirmés par une loi adoptée dans un delai d'un an à compter de la date d'entrée en vigueur de cet arrêté royal, les Comités permanents R et P observaient que cela n'avait pas été le cas. Ils notaient que l'avant-projet de loi venait remédier à cette situation, sans toutefois qu'il soit précisé dans l'exposé des motifs les raisons de l'intervention tardive du gouvernement.

Le Comité permanent R jugeait dès lors nécessaire de procéder à une évaluation de la possibilité juridique de désigner un service public comme service d'appui par le biais d'un arrêté royal. En effet, la question se pose de savoir si une évaluation de la menace établie par l'OCAM (et toute mesure fondée sur cette évaluation) est illégale si elle se fonde (entre autres) sur des informations provenant d'un service d'appui désigné par arrêté royal et transmises après le délai dans lequel cette désignation devait être légalement confirmée. Selon le Comité permanent R, il y a également lieu de s'interroger sur la question de savoir si le traitement de données à caractère personnel par un service d'appui qui devait encore faire l'objet d'une confirmation juridique est toujours compatible avec l'article 22 de la Constitution.

Le Comité permanent R a également formulé plusieurs observations spécifiques à propos du service Belgian Passenger Information Unit (BelPIU), cette unité

---

326 Le projet de loi a été déposé à la Chambre en février 2022, et adopté en Commission Intérieure – en deuxième lecture – le 3 mai 2022 (*Doc.Parl.* Chambre 2021-2022, 55-2443).

327 Cet arrêté royal a été pris en exécution de l'article 2, 1er alinéa, 2°, g), de la L.OCAM. Il désigne les services d'appui suivants : le service des Cultes et de la Laïcité de la Direction générale Législation, libertés et droits fondamentaux du SPF Justice, la Direction générale des Établissements pénitentiaires du SPF Justice, la Direction générale du Centre de crise du SPF Intérieur et l'Administration générale de la Trésorerie du SPF Finances.

placée par l'A.R. du 21 décembre 2017 sous la direction de la Direction générale Centre de crise du SPF lnterieur.[328]

Le Comité permanent R a souligné que le fait de placer le service BelPIU sous l'égide du Centre de crise n'a aucune influence sur le cadre juridique existant concernant le traitement des données des passagers par ce service. Malgré la désignation du Centre de crise comme service d'appui de l'OCAM, BELPIU ne peut être (indirectement) soumis aux modalités de coopération telles que décrites dans la L.OCAM.

S'il existe une nécessité de désigner le service BelPIU comme service d'appui de l'OCAM, il faut alors adapter la L.OCAM ainsi que la Loi du 25 decembre 2016 relative au traitement des données des passagers.

En outre, le croisement entre les informations de voyage détenues par BELPIU et les données de les BDC illustre la problématique plus large de la relation entre les activités de l'OCAM en sa qualité de gestionnaire opérationnel des BDC et l'OCAM en sa qualité d'organe d'évaluation de la menace, d'autre part (voir *infra*).

VI.6.2. MODIFICATION DES CONDITIONS DE NOMINATION DU DIRECTEUR ET DU DIRECTEUR ADJOINT

Le projet de loi visait aussi à supprimer l'une des conditions à remplir pour être designé directeur et directeur adjoint de l'OCAM, à savoir le statut requis de magistrat.

Le Comité permanent R indiquait dans son avis que cette suppression augmenterait certes le nombre de candidats possibles, mais posait un certain nombre de questions au regard de l'environnement légal complexe dans lequel l'OCAM évolue. La question se pose de savoir si la condition de nomination en remplacement d'une 'expertise juridique complémentaire' n'est pas plus théorique que réellement suffisante pour compenser la suppression du statut de magistrat au regard du respect d'un équilibre entre les besoins opérationnels de l'OCAM et l'importance du respect et de la connaissance des règles en vigueur. Le Comité permanent R constatait également que le projet de loi n'ajoutait aucune disposition pour protéger l'indépendance et l'impartialité de la direction de l'OCAM (tenant compte de la suppression proposée de la condition de nomination d'être un magistrat). Un tel cadre est toutefois nécessaire, notamment en ce qui concerne la réalisation d'évaluations de la menace et la définition du niveau de menace pertinent.

---

328 Article 2 de l'Arrêté royal relatif à l'exécution de la Loi du 25 decembre 2016 relative au traitement des données des passagers, reprenant diverses dispositions concernant l'Unité d'information des passagers et le délégué à la protection des données.

VI.6.3. EXTENSION DES MISSIONS DE L'OCAM

L'avant-projet de loi visait également à inscrire (à l'article 8 de la L.OCAM) des nouvelles missions pour l'OCAM.

VI.6.3.1. La coordination de l'approche globale des menaces

Le projet de loi prévoyait tout d'abord un rôle de coordination pour l'OCAM dans l'approche globale des menaces visées dans l'article 3 de la L.OCAM. L'exposé des motifs indiquait qu'il s'agissait de consolider une pratique déjà existante.

Les Comités permanents R et P constataient toutefois que le contenu de ce rôle de coordination n'était pas davantage precisé. L'exposé des motifs se limitait à une énumeration non exhaustive d'exemples tels que l'interaction entre les Local Task Force (LTF) et les Cellules de Securité lntegrale Locale en matière de radicalisme, d'extrémisme et de terrorisme (CSIL-R) et l'optimalisation des BDC. Les Comités recommandaient de préciser la mission de l'OCAM en matière de coordination de l'approche globale des menaces. En effet, l'OCAM ne dispose pas d'un arsenal opérationnel pour approcher les menaces de façon effective et globale.

Le Comité permanent R pointait en outre la définition excessivement vague et large de l'objet de la mission de coordination. Cela soulève d'abord la question des services qui relèveraient ou non de la coordination de l'OCAM. Se pose également la question de savoir quelle 'approche' doit etre coordonnée : s'agit-il de la coordination de l'approche globale du terrorisme, de l'extrémisme et de la radicalisation ou uniquement de la coordination de l'approche 'administrative' ? Cela concerne-t-il uniquement la coordination de l'approche 'strategique' ou également la coordination de l'approche 'opérationnelle' ? Enfin, se pose la question des instruments (contraignants ?) dont dispose l'OCAM pour concrétiser cette mission de coordination.

Le Comité permanent R constatait également que le projet créait une confusion entre plusieurs réglementations légales qui encadrent les missions de l'OCAM.[329] Le Comité indiquait qu'il conviendrait de clarifier la relation entre l'obligation d'alimenter les BDC dans le chef des 'services de base' et des 'services partenaires'[330] et l'obligation de notification à l'OCAM pour les 'services d'appui de l'OCAM'. En

---

329 En particulier, la L.OCAM, la réglementation autour des banques de données communes et la loi portant création des CSIL-R.

330 Les articles 44/2, § 2 et 44/11/3ter, § 4 LFP, *i.o.* article 7, § 1er de 'I' Arrete royal du 21 juillet 2016 AR Terrorist Fighters et article 7, § 1er AR Propagandistes de haine. Voir egalement la Circulaire du 22 mai 2018 du ministre de la Sécurité et de l'lntérieur et du ministre de la Justice 'relative à l'échange d'informations et au suivi des terrorist fighters et des propagandistes de haine' (Circulaire Terrorist fighters et Propagandistes de haine). Le Collège des procureurs fédéraux et le Ministère public ont eux aussi émis quelques circulaires en la matière : COL 10/2015 'concerne : Approche judiciaire en matière des foreign terrorist fighters', COL 21/2016 'concerne : Approche judiciaire des prédicateurs de haine' et COL 22/2016 'concerne : Banque de données commune relative aux Foreign Terrorist Fighters'.

effet, l'extension de l'obligation de notification à toutes les nouvelles missions de l'OCAM crée une ambiguité.

Le Comité permanent R invitait par ailleurs à clarifier si l'obligation de notification s'appliquait aux membres des CSIL-R également et, le cas échant, s'ils sont autorisés à fournir à l'OCAM des données à caractère personnel.

VI.6.3.2. De nouvelles missions confiées à l'OCAM par le Conseil national de sécurité ?

L'avant-projet de loi prévoyait ensuite que l'OCAM pouvait se voir attribuer, le cas échéant, de nouvelles missions dans la sphère de ses compétences par le Conseil national de sécurité au moyen d'un arrêté royal. Si l'extension de la liste des services d'appui par A.R. doit être confirmée dans une loi, une telle confirmation n'était pas exigée en ce qui concerne l'extension des missions de l'OCAM qui devait, selon l'avant-projet, uniquement faire l'objet d'un arrêté royal délibéré en Conseil des ministres. L'avis mettait en lumière cette différence d'approche instaurée au sein de la même loi.

Le Comité permanent R conseillait par ailleurs de clarifier davantage l'expression 'sphère de compétence de l'OCAM' dans la disposition concernée. En effet, il n'existe pas de sphère de compétence de l'OCAM qui soit uniforme pour toutes ses missions.[331]

Il était également proposé d'étendre l'obligation de notification des services d'appui à toutes les nouvelles missions de l'OCAM. Selon cette logique, les services d'appui seraient obligés de transmettre toutes les informations dont ils disposent à l'OCAM lorsque ces informations sont pertinentes pour des missions de l'OCAM fixées par arrêté royal. Cela inclut également les données à caractère personnel. Compte tenu du droit fondamental à la vie privée consacré par l'article 22 de la Constitution, l'avis rappelait que la transmissionet le traitement de données à caractère personnel doivent toujours être ancrés dans une loi formelle afin d'en fixer les règles et objectifs de base.

VI.6.4. COMMUNICATION ET CONSULTATION DES ÉVALUATIONS

L'avant-projet de loi visait également à modifier les conditions et modalités de communication, par l'OCAM, des évaluations stratégiques, ponctuelles ou effectuées à la demande d'un service d'appui. A ce propos, les Comités permanents

331 Ainsi, par exemple, la L.OCAM porte sur le terrorisme et l'extrémisme, y compris le processus de radicalisation tandis que la Loi sur la fonction de police (LFP) traite du terrorisme et de l'extrémisme pouvant mener au terrorisme.

P et R pointaient certaines incohérences (notamment linguistiques) dans le texte et suggèraient des formulations alternatives.

VI.6.5. COMMUNICATION ET CONSULTATION DE RENSEIGNEMENTS DE NATURE JUDICIAIRE SOUS EMBARGO[332]

L'avant-projet de loi visait aussi à modifier la L.OCAM en prévoyant notamment que les renseignements de nature judiciaire sous embargo ne soient plus uniquement transmis au directeur de l'OCAM mais également aux membres habilités de l'OCAM désignés pour réaliser l'évaluation *ad hoc* des renseignements sous embargo.

Les Comités permanents R et P conseillaient de prévoir expressément dans l'avant-projet de loi que la connaissance de ces renseignements sous embargo par les membres du personnel de l'OCAM désignés soit strictement indispensable pour l'exercice de leur fonction dans le cadre des missions de l'OCAM.[333] Les Comités recommandaient par ailleurs de reprendre expressément dans le texte de l'avant-projet de loi que le directeur de l'OCAM doit tenir la liste des membres du personnel désignés ayant accès à ces informations à la disposition des Comités permanents R et P.

VI.6.6. COMMUNICATION ET CONSULTATION DE RENSEIGNEMENTS VISÉS À L'ARTICLE 12, 1ER ALINÉA L.OCAM

L'avant-projet de loi prévoyait les mêmes adaptations en ce qui concerne les renseignements sous embargo fournis, par les services de renseignement et de securité, l'Administration des douanes et accises du SPF Finances et le SPF Affaires étrangères, provenant d'un service étranger homologue qui a explicitement demandé de ne pas les transmettre à d'autres services ou dont la transmission peut compromettre la securité d'une source humaine.

À l'instar de ce qui a été discuté *supra,* les Comités invitaient à reprendre expressément dans le texte que cet accès doit être déterminé selon le principe du besoin d'en connaitre et que le directeur de l'OCAM doit tenir la liste des membres du personnel designés ayant accès à ces informations à la disposition des Comités permanents R et P.

---

332 Voir egalement : COMITÉ PERMANENT R, *Rapport d'activites 2008*, 110.

333 Autrement dit, qu'ils aient strictement le besoin d'en connaitre.

CHAPITRE VII.
LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Le service d'Enquêtes R du Comité effectue également sur ordre des autorités judiciaires des enquêtes sur les membres des services de renseignement et de sécurité et de l'Organe de coordination pour l'analyse de la menace (OCAM)[334] suspectés d'avoir commis un crime et/ou un délit. Cette compétence est décrite à l'article 40, alinéa 3 de la L.Contrôle.

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le directeur du service d'Enquêtes R sont soumis à l'autorité du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a aucune autorité sur eux. Le président du Comité doit cependant veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle. La raison en est évidente : le Comité a beaucoup d'autres missions légales. Celles-ci pourraient être mises en péril si les dossiers judiciaires nécessitaient un investissement trop conséquent. Le président peut, le cas échéant, se concerter avec les autorités judiciaires quant à la participation des membres du service d'Enquêtes R à des enquêtes pénales (art. 61*bis* L.Contrôle).

Lorsque le service d'Enquêtes R effectue des enquêtes pénales, le directeur doit remettre un rapport au Comité permanent R au terme de celles-ci. Dans ce cas, '*le rapport se limite aux informations qui sont nécessaires à l'accomplissement par le Comité permanent R de ses missions*' (art. 43, alinéa 3, L.Contrôle).

En 2021 le service d'Enquêtes R a effectué des devoirs d'enquête dans le cadre de six dossiers répressifs ; quatre sous l'autorité du Parquet fédéral, un à l'Auditorat du travail de Liège et un auprès du Procureur du Roi de Bruxelles. Cinq de ces dossiers concernaient potentiellement des membres du Service Général du Renseignement et de la Sécurité et un dossier des membres de la Sûreté de l'État. Dans ce cadre, le service d'Enquêtes R a reçu six apostilles et en a clôturées quatre.

Au total, dix procès-verbaux ont été dressés et onze rapports confidentiels ont été rédigés. Les infractions suivantes étaient visées dans le cadre de ces dossiers : 'violation du secret professionnel', 'faux et usage de faux en écriture' et 'consultation irrégulière de bases de données'.

---

[334] En ce qui concerne les membres des autres 'services d'appui' de l'OCAM, cette disposition ne s'applique qu'à l'égard de l'obligation de communiquer des renseignements pertinents à l'OCAM (articles 6 et 14 L.OCAM).

Par ailleurs, l'article 50 L. Contrôle dispose que *'[t]out membre d'un service de police qui constate un crime ou un délit commis par un membre d'un service de renseignement rédige un rapport d'information et le communique dans les quinze jours au chef du Service d'enquêtes R*'. En 2021, le service d'Enquêtes R n'a reçu aucun signalement en ce sens.

CHAPITRE VIII.
EXPERTISE ET CONTACTS EXTERNES

VIII.1. EXPERT DANS DIFFÉRENTS FORUMS

En 2021, les membres du Comité permanent R et son personnel ont été consultés à plusieurs reprises en tant qu'experts par des institutions publiques et privées nationales et étrangères:

- Le greffier faisant fonction du Comité permanent R a été invité, dans le cadre du cours « Intelligence » du Master en relations internationales et diplomatie (Université d'Anvers), à présenter le fonctionnement du Comité. L'intervention s'est déroulée par vidéoconférence ;
- Des articles rédigés par des collaborateurs du Comité ont été publiés dans diverses revues scientifiques[335] ;
- Le président a été invité, en mai 2021, à faire partie du comité de sélection pour la nomination d'un membre suppléant pour la Commission BIM. L'objectif de cette sélection et du comité de sélection était de recueillir des informations utiles sur les candidats afin de pouvoir donner un avis motivé au ministre de la Justice ;
- En juin 2021, le président est intervenu, à la demande de la Rapporteuse spéciale sur les droits de l'homme et la lutte antiterrorisme, en tant que modérateur à *RightsCon*, conférence mondiale sur les droits de l'homme à l'ère numérique. La conférence, organisée en collaboration avec l'Agence AWO, avait pour thème '*When States of Emergency Collide : COVID-19, Counter-Terrorismmand Transnational Data Flows*' ;
- Plusieurs vidéoconférences ont eu lieu entre des juristes du Comité permanent R et des représentants de l'Institut fédéral pour la protection et la promotion des droits humains (*infra*) au sujet de l'obligation de notification active suite à la mise en œuvre de méthodes particulières de recueil de données.

---

335 F. GIVRON et S. LIPSZYC, 'Le contentieux en matière de sécurité et son instance spécifique: l'Organe de recours en matière d'habilitations, attestations et avis de sécurité. La recherche de l'équilibre entre la protection des droits de la défense et la préservation des intérêts majeurs de l'État', *J.T.*, 2021/3, 45-53; W. VAN LAETHEM, 'Problemen met veiligheidsadvies van beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen', *Juristenkrant*, 2021, 439, 8-9 ; B. VERSCHAEVE, 'Het Incident Respons Team van de Staatveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht', *Politie en Recht*, 1, 2022, 3-20.

- Des échanges ont eu lieu avec des personnes issues du monde académique (Université d'Anvers) sur la place croissante qu'occupent les informations issues des services de renseignement dans la motivation (de tout type) de décision(s) administrative(s) ;
- En septembre 2021, le greffier faisant fonction a été invité à faire une présentation sur le cadre théorique des screenings de sécurité en Belgique lors d'une journée d'étude organisée à huis clos. Elle s'adressait aux chercheurs ainsi qu'aux personnes issues du monde du renseignement et des infrastructures critiques. L'ensemble de l'événement s'inscrivait dans le cadre d'une thèse de doctorat sur l''*insider threat*' (Université d'Anvers) ;
- Toujours en septembre, à la demande du ministre du gouvernement de la Fédération Wallonie-Bruxelles compétent pour les Maisons de justice, le Comité a participé à une réunion sur l'échange d'informations entre les Maisons de justice, l'Organe de coordination pour l'analyse de la menace (OCAM) et la Sûreté de l'État (VSSE) ;
- Le Directeur du service d'Enquêtes a participé à une session de formation pour les personnes nouvellement recrutées au sein du Service Général du Renseignement et de la Sécurité (SGRS).
- En octobre 2021, le président du Comité permanent R a pris la parole lors de la troisième 'European Intelligence Oversight Conference ' organisée à Rome.[336]
- Un collaborateur a finalisé sa thèse de doctorat et obtenu le titre de Docteure en Sciences politiques et sociales en décembre 2021 (UCLouvain Saint Louis Bruxelles).[337]

VIII.2. PROTOCOLE DE COOPÉRATION AVEC LES MÉDIATEURS FÉDÉRAUX

La Loi du 15 septembre 2013[338] désigne les Médiateurs fédéraux[339] comme point de contact central des atteintes suspectées à l'intégrité au sein des autorités administratives fédérales. En septembre 2021, le 'Protocole de coopération du 7 octobre 2021 pour les relations entre les Médiateurs fédéraux et le Comité permanent de contrôle des services de renseignement et de sécurité dans le cadre de la loi du 15 septembre 2013' a été conclu. Le protocole vise à réglementer les modalités de coopération entre les Médiateurs fédéraux et le Comité lorsqu'une

336 Le titre de son intervention était : '*European case law on the notification of secret measures and the Belgian response with particular attention to the future rol of the Standing Committee R*'.

337 C. THOMAS, "*Une menace possible et vraisemblable*" *Dire et faire la sécurité : l'Organe de coordination pour l'analyse de la menace et la structuration du champ antiterroriste belge*, Bruxelles, UCLouvain Saint Louis Bruxelles, septembre 2021, 470p.

338 Loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel, *M.B.* 14 octobre 2013.

339 Loi du 22 mars 1995 instaurant des médiateurs fédéraux, *M.B.* 7 avril 1995.

une atteinte suspectée à l'intégrité dans l'un des deux services de renseignement est signalée aux Médiateurs.

Le cas échéant, les Médiateurs fédéraux peuvent demander au Comité permanent R de désigner un membre du service d'Enquêtes pour assister le Centre Intégrité – un point de contact central au sein des Médiateurs fédéraux – en tant qu'expert dans la conduite de l'enquête. Des accords ont également été conclus dans le protocole concernant les moyens d'investigation, le secret professionnel, la confidentialité et l'échange de bonnes pratiques.

VIII.3. COLLABORATION AVEC L'INSTITUT FÉDÉRAL DES 'DROITS DE L'HOMME'

Avec la Loi du 12 mai 2019, l'Institut fédéral pour la protection et la promotion des droits humains (IFDH) a été créé.[340] Par le biais d'un protocole de coopération, toutes les institutions participantes ont accepté d'échanger des pratiques et des méthodes, d'examiner des questions communes et de promouvoir la coopération mutuelle. La contribution des partenaires a été sollicitée pour la rédaction d'un premier plan stratégique. Il a également été demandé au Comité un échange de vues avec les représentants de l'IFDH dans le cadre de la réalisation d'un rapport alternatif pour le Comité contre la Torture (CAT) de l'ONU. Cela concernait notamment les 'restitutions extraordinaires'[341], et relevait donc du mandat du Comité permanent R.

VIII.4. UNE INITIATIVE MULTINATIONALE EN MATIÈRE D'ÉCHANGE D'INFORMATIONS

La multiplication des échanges de données au niveau international entre les services de renseignement et de sécurité pose un certain nombre de défis aux organes de contrôle nationaux. Les organes de contrôle de (au départ) cinq pays européens (la Belgique, le Danemark, les Pays-Bas, la Norvège et la Suisse) se concertent depuis quelques années afin de relever ces défis, en identifiant des méthodes de travail qui leur permettraient de limiter le risque de lacunes dans le contrôle. Un nouveau partenaire a été impliqué ultérieurement dans ce projet, à savoir l'*Investigatory Powers Commissioner's Office (IPCO)* du Royaume-Uni. Le groupe a été rebaptisé '*Intelligence Oversight Working Group*' (IOWG) et, en 2019, a été élargi à trois observateurs, à savoir le *Swedisch Foreign Intelligence Inspectorate*

340 Loi du 12 mai 2019 portant création d'un Institut fédéral pour la protection et la promotion des droits humains, *M.B.* 21 juin 2019.

341 Voir *in extenso*, COMITÉ PERMANENT R, *Rapport d'activités 2006*, 34-41, ('II.2. Les vols CIA').

(Statens inspektion av försvarunderättelse-verksamhet (SIUN)), le *Swedish Board of Inventions (Statens uppfinnarnämnd, (SUN))* et la Commission G10 allemande.

En raison des restrictions liées à la crise sanitaire, les activités internationales sont restées limitées en 2021. En septembre 2021, une réunion virtuelle organisée par l'autorité de surveillance suisse *Autorité de surveillance indépendante des activités de renseignement* (AS-Rens) a eu lieu pour échanger sur l'avenir de l'IOWG. Les discussions ont également porté sur la manière dont les organes de contrôle font face à la pandémie et aux nouveaux développements technologiques dans le domaine du renseignement. Cette coopération sera intensifiée en 2022.

VIII.5. CONTACTS AVEC DES ORGANES DE CONTRÔLE ÉTRANGERS

En octobre 2021 s'est tenue la troisième conférence *European Intelligence Oversight Conference* auprès de l'organe de contrôle italien, la *Procura Generale della Corte di Cassazione*. La conférence a abordé des thèmes tels que '*The developments in the light of European Case Law*', '*Bulk data collection and targeted interceptions*' et '*International cooperation and other oversight developments in the light of the revised Convention 108+*'.

Dans le prolongement d'un questionnaire sur l'"*ex ante oversight*', l'organe de contrôle néerlandais CTIVD (*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten)* a lancé, en juillet 2020, une initiative similaire. Il s'agissait d'un questionnaire portant sur le '*complaint handling*' (traitement des plaintes). L'objectif de cette initiative était de recueillir et analyser les meilleures pratiques en Europe en matière de traitement des plaintes à des fins d'amélioration. Le Comité y a apporté sa contribution.

Le Comité permanent R a expliqué son intention de procéder, avec *l'Autorité de surveillance indépendante des activités de renseignement* (AS-Rens) suisse, à un échange de personnel dans le cadre d'un stage, même de courte durée. Après une suspension du projet en raison de la crise sanitaire, cet échange est prévu dans le courant de l'année 2022.

Le *Danish Intelligence Oversight Board* a partagé avec les organes de contrôle belge et européens ses '*Standards for Danish intelligence oversight activities*'.

Enfin, des informations ont été échangées avec la Cour administrative du Luxembourg concernant la législation relative à l'utilisation de documents classifiés dans le cadre des habilitations de sécurité.

CHAPITRE IX.
L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ[342]

Ce chapitre reprend le rapport d'activités approuvé lors de la réunion du 20 mai 2022 par l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité (ci-après l'Organe de recours) ainsi qu'un certain nombre de remarques et suggestions du président de cette juridiction.

IX.1. LE RAPPORT D'ACTIVITÉS DE L'ORGANE DE RECOURS

IX.1.1. INTRODUCTION

L'Organe de recours[343] est, en Belgique, l'unique juridiction administrative compétente pour les contentieux portant sur des décisions administratives dans divers domaines : les habilitations de sécurité, les attestations de sécurité et, enfin, les avis de sécurité.

L'Organe de recours intervient également en tant que 'juge d'annulation' contre des décisions d'autorités publiques ou administratives, lorsqu'elles imposent des avis ou des attestations de sécurité pour un secteur, un lieu ou un événement donné.[344]

L'Organe de recours est composé du président du Comité permanent R, de la présidente du Comité permanent P et du président de la Chambre contentieuse de l'Autorité de protection des données. Les trois présidents peuvent être remplacés

---

342 Le présent rapport d'activités exécute l'article 13 de la Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité qui stipule que l'organe de recours est tenu de rédiger un rapport annuel.

343 GIVRON, F. et LIPSZYC, S., 'Le contentieux en matière de sécurité et son instance spécifique : l'Organe de recours en matière d'habilitations, attestations et avis de sécurité. La recherche de l'équilibre entre la protection des droits de la défense et la préservation des intérêts majeurs de l'État', *J.T.*, 2021/3, 45-53.

344 Pour plus de détails, voir COMITÉ PERMANENT R, *Rapport d'activités 2006*, 87-120 et *Rapport d'activités 2018*, 111-124.

en cas d'empêchement par un membre-conseiller effectif de l'institution à laquelle appartient le président concerné.

Le président du Comité permanent R assure la présidence de l'Organe de recours. La fonction de greffier est exercée par le greffier du Comité permanent R et le personnel du greffe est le personnel affecté par le Comité. Les activités de l'Organe de recours constituent depuis plus de vingt ans l'exemple parfait de synergie au sein de certaines institutions satellitaires du Parlement. La composition de l'Organe de recours apporte en outre une contribution multidisciplinaire à la délibération de chaque dossier.

Il convient de noter qu'en ce qui concerne les recours, l'administration et le suivi sont entièrement assurés par le Comité permanent R. En effet, le Comité met à disposition toutes les personnes et ressources nécessaires pour assurer l'administration, la correspondance, la tenue des audiences et la rédaction des décisions. Il s'agit, d'une part, de la mise à disposition du président et de ses membres suppléants, de son greffier mais aussi des juristes comme '*greffiers assumés*' et du personnel administratif qui forment le greffe de cette juridiction administrative. D'autre part, le Comité permanent R prend en charge, sur son budget, les frais de locaux et de fonctionnement de l'Organe de recours.

L'Organe de recours a pris toutes les mesures nécessaires pour assurer son fonctionnement nonobstant la pandémie du COVID-19. L'Organe de recours a ainsi maintenu ses audiences au rythme minimum de deux par mois. En 2021, il a tenu 30 audiences.[345]

IX.1.2. LE DÉTAIL DES CHIFFRES

Cette section reprend les chiffres relatifs à la nature des décisions contestées, la qualité des autorités compétentes et des requérants, ainsi que la nature des décisions de l'Organe de recours dans le cadre des différentes procédures de recours. À des fins de comparaison, les chiffres des cinq années précédentes sont également repris.

En 2021, 180 recours ont été introduits, contre 144 en 2020 et 196 en 2019 (*infra*). On constate que ces chiffres suivent la reprise économique et la demande d'avis de sécurité notamment dans le secteur aéroportuaire et pour les candidats à la Défense.

149 décisions finales ont été prises.

[345] Dont 13 audiences en néerlandais et 17 en français.

Tableau 1. Nombre de recours introduits (2016-2021)

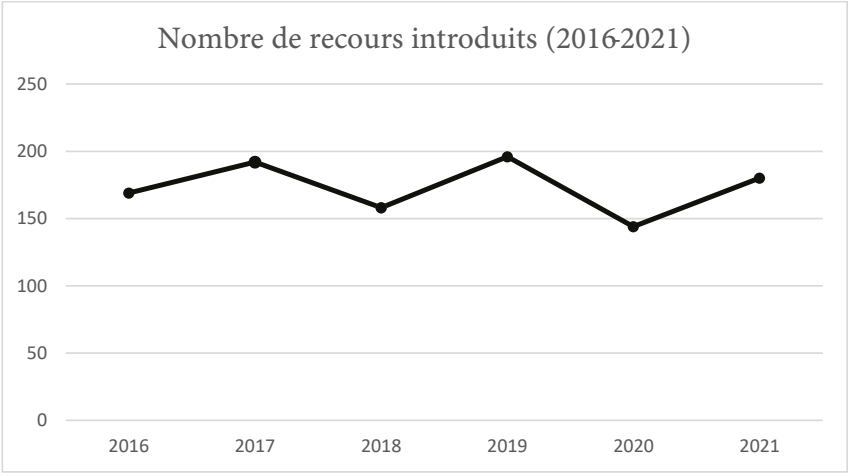


Tableau 2. Nombre de recours introduits *vs* nombre de décisions rendues (2016-2021)

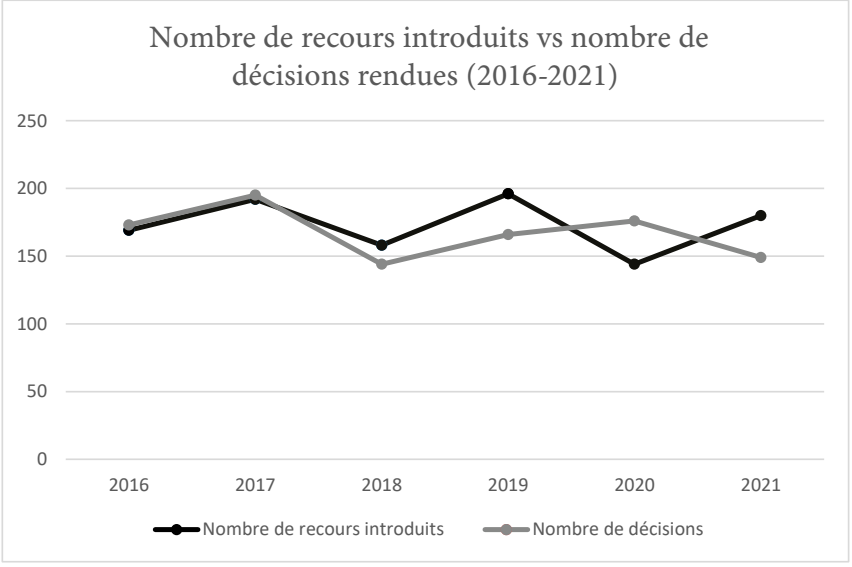


Tableau 3. Autorités de sécurité concernées (2016-2021)

	2016	2017	2018	2019	2020	2021
Autorité nationale de sécurité	92	129	113	114	91	86
Sûreté de l'État	0	0	0	0	0	4
Service Général du Renseignement et de la Sécurité	68	53	32	61	41	84
Agence fédérale de Contrôle nucléaire	8	7	10	17	7	6
Police fédérale	1	3	3	3	4	0
Police locale	0	0	0	1	1	0
TOTAL	**169**	**192**	**158**	**196**	**144**	**180**

Le graphique ci-dessous visualise la répartition des autorités de sécurité concernées en 2021.

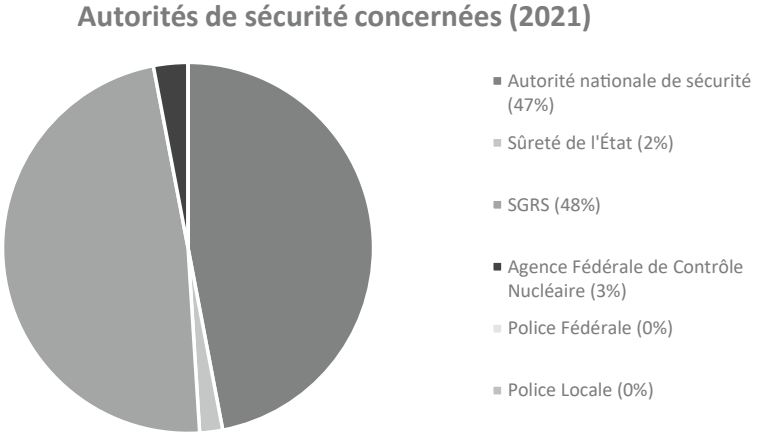


Tableau 4. Nature des décisions contestées

	2016	2017	2018	2019	2020	2021
Habilitations de sécurité (art. 12 et s. L.C&HS)						
Confidentiel	5	1	2	5	0	2
Secret	38	33	31	39	27	50
Très secret	7	6	3	7	5	8
Refus	28	30	26	39	23	37

	2016	2017	2018	2019	2020	2021
Retrait	9	7	4	16	8	17
Refus et retrait	0	0	0	0	0	4
Habilitation pour une durée limitée	4	1	1	3	0	1
Habilitation pour un niveau inférieur	1	0	0	0	0	
Pas de décision dans les délais	7	2	5	0	0	1
Pas de décision dans les nouveaux délais	1	0	0	0	0	0
Autres					1[346]	
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	50	40	36	51	32	60
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)						
Refus	1	3	3	1	0	3
Retrait	0	0	0	0	0	0
Pas de décision dans les délais	0	0	0	0	0	
Attestations de sécurité lieu ou événement (art. 22*bis*, al.2 L.C&HS)						
Refus	9	20	15	12	6	2
Retrait	0	0	0	0	0	0
Pas de décision dans le délai	0	0	0	0	0	1
Attestations de sécurité lieu secteur nucléaire (art. 8*bis* L.C&HS)						
Refus	7	7	11	17	7	6
Retrait	1	0	0	0	0	0
Pas de décision dans le délai	0	0	1	0	0	0
Avis de sécurité (art. 22*quinquies* L.C&HS)						
Avis négatif	101	122	92	115	99	108
Pas d'avis	0	0	0	0	0	0
Révocation d'avis positif	0	0	0	0	0	0
Actes normatifs d'une autorité administrative (art. 12 L. Org.recours)						

346 'Mise en garde du requérant'. Une personne s'était vue octroyer l'habilitation de sécurité pour cinq ans avec une mise en garde. Il est allé en recours contre cette mise en garde.

	2016	2017	2018	2019	2020	2021
Décision d'une autorité publique d'exiger des attestations de sécurité	0	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des attestations de sécurité	0	0	0	0	0	0
Décision d'une autorité administrative d'exiger des avis de sécurité	0	0	0	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des avis de sécurité	0	0	0	0	0	0
SOUS-TOTAL ATTESTATIONS ET AVIS	119	152	122	145	112	120
TOTAL DÉCISIONS CONTESTÉES	**169**	**192**	**158**	**196**	**144**	**180**

Tableau 5. Nature du requérant

	2016	2017	2018	2019	2020	2021
Fonctionnaire	2	4	5	4	8	16
(candidat) Militaire	23	20	8	27	39	81
Particulier	139	164	140	163	95	80
Personne morale	5	4	5	2	2	3

Le graphique ci-dessous visualise la répartition 'nature du requérant' en 2021.

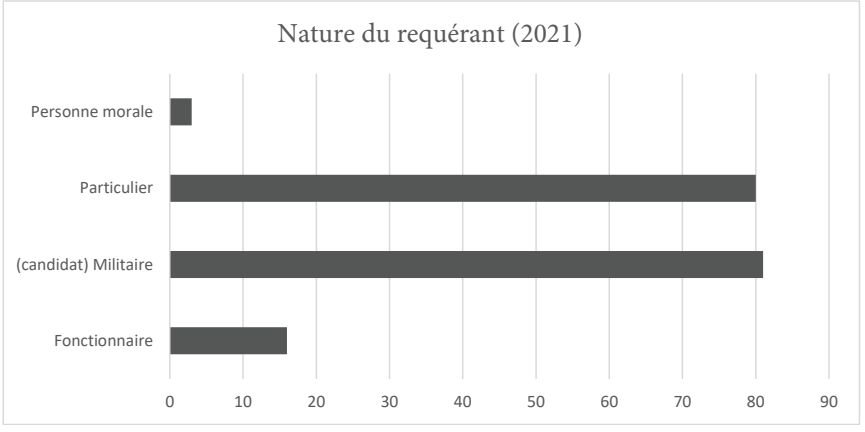


Tableau 6. Langue du requérant

	2016	2017	2018	2019	2020	2021
Français	99	115	83	101	83	86 (1)
Néerlandais	70	77	75	95	61	94 (2)
Allemand	0	0	0	0	0	0
Autre langue	0	0	0	0	0	0

(1) 86 dossiers francophones en 2021 + 29 dossiers francophones des années antérieures mais traités en 2021 = 115 requérants francophones

(2) 94 dossiers néerlandophones en 2021 + 18 dossiers néerlandophones des années antérieures mais traités en 2021 = 112 requérants néerlandophones

Tableau 7. Actes du greffe

	2016	2017	2018	2019	2020	2021
Demande du dossier complet (1)	167	191	154	191	141	180
Demande d'informations complémentaires (2) et rappels adressés aux autorités de sécurité (3)*	23	36	12	39	41	45

(1) L'Organe de recours peut demander l'intégralité du dossier aux autorités de sécurité. Comme ce dossier contient davantage de données que le rapport d'enquête seul, cette requête est systématiquement effectuée par le greffe.

(2) L'Organe de recours peut également demander tout complément d'informations qu'il juge nécessaire pendant la procédure. Dans la pratique, le greffe se charge de demander aux autorités de compléter les dossiers.

(3) L'art. 6 de l'AR Org. recours prévoit les délais pour la communication des dossiers par les autorités de sécurité. Ces délais prennent cours lorsque le greffier transmet une copie du recours à l'autorité de sécurité concernée. Ils varient selon la nature de l'acte attaqué. Ainsi, l'autorité de sécurité doit communiquer son dossier dans les 15 jours en ce qui concerne les habilitations de sécurité, dans les 5 jours en matière d'attestations de sécurité et dans les 10 jours si le recours porte sur un avis de sécurité. Lorsque ces délais ne sont pas respectés, le greffe prend les contacts nécessaires. Ces données sont comptabilisées à partir de 2019.

Tableau 8. Actes juridictionnels interlocutoires pris par l'Organe de recours [347]

	2016	2017	2018	2019	2020	2021
Audition d'un membre d'une autorité (1)	10	0	1	6	1	4
Décision du président (2)	0	0	0	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (3)	54	80	72	77	50	77
Décisions avant dire droit (4)	/	/	/	9	9	19

(1) L'Organe de recours peut décider d'entendre les membres des services de renseignement et de police ou des autorités de sécurité qui ont participé à l'enquête ou à la vérification de sécurité.

(2) Le président de l'Organe de recours peut décider de permettre au membre du service de renseignement de garder secrètes certaines données pendant son audition.

(3) Si le service de renseignement ou de police concerné le demande, l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant.

(4) Il peut s'agir par exemples d'une décision de jonction de deux dossiers ou de demander un complément d'informations à propos de la situation d'un dossier judiciaire. Ces données sont comptabilisées à partir de 2019.

Tableau 9. Manière dont le requérant fait usage de ses droits de défense

	2016	2017	2018	2019	2020	2021
Consultation du dossier par le requérant et/ou l'avocat	87	105	69	96	96	97
Audition du requérant (assisté ou non d'un avocat)[348]	127	158	111	143	135	151

347 Le nombre d'"actes juridictionnels interlocutoires' (tableau 6), les 'manières dont les requérants font usage de leurs droits de défense' (tableau 7), ou encore la 'nature des décisions de l'Organe de recours' (tableau 8) ne correspondent pas nécessairement au nombre de requêtes introduites (voir tableaux 1 à 4). En effet, certains dossiers ont par exemple déjà été ouverts en 2020, alors que la décision n'a été rendue qu'en 2021.

348 La L.Org.recours prévoit l'assistance d'un avocat à l'audience mais pas la représentation par ce dernier. À noter que, dans le cadre de certains dossiers, le requérant (assisté ou non de son avocat) est auditionné à plusieurs reprises.

Tableau 10. Nature des décisions de l'Organe de recours

	2016	2017	2018	2019	2020	2021
Habilitations de sécurité (art. 12 et s. L.C&HS)						
Recours irrecevable	0	3	0	1	1	0
Recours sans objet	7	0	4	3	3	3
Recours non fondé	18	13	12	12	16	11
Recours fondé (avec octroi partiel ou complet)	24	24	12	25	14	17
Devoir d'enquête complémentaire par l'autorité	2	0	1	1	2	1
Délai supplémentaire pour l'autorité	2	1	1	0	3	0
Donne acte de retrait de recours	0	0	3	2	2	11
Attestations de sécurité zone classifiée (art. 22*bis*, al.1 L.C&HS)						
Recours irrecevable	0	1	0	0	0	0
Recours sans objet	0	1	0	0	0	0
Recours non fondé	1	0	1	1	0	2
Recours fondé (avec octroi)	1	1	0	3	0	2
Donne acte de retrait de recours	-	-	-	1	0	0
Attestations de sécurité pour lieux ou événements (art. 22*bis*, al.2 L.C&HS)						
Recours irrecevable	0	1	2	4	2	0
Recours sans objet	0	1	0	0	0	0
Recours non fondé	2	12	2	4	4	1
Recours fondé (avec octroi)	4	7	3	4	1	0
Donne acte de retrait de recours	0	1	2	0	0	0
Attestations de sécurité pour le secteur nucléaire (art. 8*bis* §2 L.C&HS)						
Recours irrecevable	1	1	0	1	0	0
Recours sans objet	1	0	1	0	0	0
Recours non fondé	0	1	1	5	2	2
Recours fondé (avec octroi)	7	5	6	7	4	6
Donne acte de retrait de recours	-	-	2	0	0	0

	2016	2017	2018	2019	2020	2021
Avis de sécurité (art. 22*quinquies* L.C&HS)						
Organe de recours non compétent	0	20[349]	12	0	0	0
Recours irrecevable	15	10	3	7	8	3
Recours sans objet	0	1	3	1	6	4
Confirmation de l'avis négatif	42	49	46	40	51	47
Réformation en avis positif	46	41	27	43	52	34
Donne acte de retrait de recours	0	1	0	1	5	5
Recours contre des actes normatifs d'une autorité administrative (art. 12 L. Org.recours)	0	0	0	0	0	0
TOTAL	**173**	**195**	**144**	**166**	**176**	**149**

IX.2. REMARQUES ET SUGGESTIONS DU PRÉSIDENT DE L'ORGANE DE RECOURS

IX.2.1. UNE PROCÉDURE PARTICULIÈRE ET COMPLEXE

La juridiction administrative qu'est l'Organe de recours se caractérise par une gestion administrative des dossiers particulière et plus complexe par rapport aux autres juridictions de l'ordre judiciaire et administratif.

Une première particularité est l'exigence légale de l'article 4 de la Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité (L.Org.recours) qui paraît aujourd'hui démesurée. En effet, le justiciable doit former son recours en matière d'attestations et d'avis de sécurité dans le délai strict de huit jours, par lettre recommandée. Il est indéniable pour les praticiens qu'un tel délai est résolument trop court pour le citoyen.

Une seconde particularité est que le requérant doit, au regard de la loi, faire un exposé dans son recours des circonstances de la cause et des raisons invoquées. Le président de l'Organe de recours est conscient que le prescrit légal ne prend pas en compte la difficulté du citoyen à ester en justice.

---

[349] Il s'agissait en l'espèce de recours introduits contre des avis de sécurité (négatifs) rendus par l'Autorité nationale de sécurité concernant le personnel de sous-traitants actifs pour les institutions européennes. L'Organe de recours avait décidé que les avis formulés par l'Autorité nationale de sécurité n'avaient pas de base juridique. En conséquence, l'Organe de recours s'était déclaré sans compétence pour statuer sur le bien-fondé ou non des avis de sécurité rendus par l'Autorité nationale de sécurité.

Une troisième particularité est liée à la demande des autorités de sécurité, dans près d'un dossier sur deux (77/180), de restriction du droit du justiciable à prendre connaissance de l'intégralité de son dossier. Il est, en effet, demandé à l'Organe de recours de faire application de l'article 5 §3 L.Org.recours. Pour rappel, cet article stipule que « *A la demande d'un service de police ou de renseignement, l'organe de recours peut décider que certaines informations figurant dans la déposition d'un membre d'un service de police ou de renseignement visé au § 2, dans le rapport d'enquête ou dans le dossier d'enquête ou de vérification sont secrètes pour un des motifs visés au § 2, alinéa 4, ou parce qu'elles relèvent du secret d'une information ou d'une instruction judiciaire en cours, et qu'elles ne pourront être consultées ni par le requérant ni par son avocat. Si ces secrets concernent une information ou une instruction judiciaire en cours, l'organe de recours se concerte au préalable à ce sujet avec le magistrat compétent. Lorsque ces informations proviennent d'un service de renseignement étranger, la décision de non-consultation est prise par le service de renseignement et de sécurité. Ces décisions ne sont susceptibles d'aucun recours*.» Il en résulte que la préparation des dossiers de l'Organe de recours nécessite que ceux-ci soient scannés puis 'caviardés'. Ce travail se réalise page par page, paragraphe par paragraphe ou mots par mots par le greffe. *In concreto*, il s'agit d'une analyse juridique, approuvée par le président de la juridiction et mise en œuvre par les membres du greffe. Il s'agit pour la juridiction de garantir le droit du justiciable à être mis en possession d'un maximum d'informations face à une demande légale de restriction d'accès.

Une quatrième particularité est due au délai de transmission des dossiers administratifs par les autorités de sécurité et cela nonobstant le prescrit légal. Le greffe de l'Organe de recours a dû adresser dans 45 des 180 dossiers introduits, un ou plusieurs rappels aux autorités de sécurité pour obtenir le dossier administratif. Ces retards se sont multipliés et touchent un dossier sur quatre contre un dossier sur dix il y a encore cinq ans. Par conséquent, l'Organe de recours ne peut pas rendre ses décisions dans les délais impartis. Au-delà, il en résulte avant tout un préjudice pour le justiciable pour qui l'obtention de l'habilitation ou de l'avis de sécurité est le plus souvent la condition *sine qua non* à l'exercice d'une fonction.

Enfin, une cinquième particularité consiste en la multiplication des recours déposés par des demandeurs étrangers ou ayant séjourné à l'étranger et l'inadéquation des outils légaux à disposition des autorités de sécurité pour répondre à cette réalité sociale. Il en résulte parfois la nécessité pour les autorités de sécurité de conclure des traités permettant l'échange d'informations et de renseignements avec des autorités de sécurité étrangères. En l'absence de tels accords, les autorités de sécurité, sans motivation circonstanciée, ne suivent pas la jurisprudence de l'Organe de recours en ce qui concerne la problématique des enquêtes ou des vérifications sur des personnes qui n'ont pas la nationalité belge. Le président de l'Organe de recours considère que les autorités de sécurité belges

devraient chercher à obtenir des informations auprès des services homologues étrangers.[350]

Pour le président de l'Organe de recours, la loi et ses arrêtés royaux ne sont plus en phase avec les exigences modernes d'accès à la justice. En effet, les articles 2 et 3 de l'AR Org. recours, stipulent respectivement que *'l'envoi à l'organe de recours de toutes pièces de procédure se fait sous pli recommandé à la poste'* et que *'le recours est signé et daté par le requérant ou par son avocat'*. De nombreux justiciables ne respectent pas ces règles, le plus souvent en raison d'une maîtrise imparfaite (mais compréhensible au vu de leur complexité) des règles de procédure.

C'est le sens de la proposition de loi rédigée, par le président de l'Organe de recours avec l'aide, comme expert, de l'ancien président de la Cour de cassation, Ivan Verougstraete. Il y a lieu, en effet, de mieux prendre en compte la qualité, voire la fragilité, de nombreux requérants et de prévoir des dispositions légales qui n'entraînent pas la nullité de plein droit ou l'irrecevabilité de la requête.

On relèvera que le texte de réforme a été adressé à la Chambre des représentants le 24 novembre 2020. Compte tenu des différentes propositions de loi en préparation modifiant entre autres la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&HS), l'Organe de recours estime qu'il convient d'établir un lien avec ce texte de réforme. Après tout, la règlementation concernant les habilitations, attestations et avis de sécurité doit être reliée de manière harmonieuse aux règlements concernant le recours éventuel contre ces décisions administratives.

Le 14 février 2022, la présidente de la Chambre a, en réponse, adressé un courrier au président de la juridiction administrative en insistant notamment sur une nouvelle concertation avec le Comité permanent P et la Chambre contentieuse de l'Autorité de Protection des données.

L'accessibilité à la juridiction administrative reste la priorité de l'Organe de recours. Le texte tel que rédigé avait pour but de consacrer l'Organe de recours comme juge naturel des questions de sécurité, d'harmoniser les délais de recours, de faciliter la procédure et de rendre sa digitalisation possible.

IX.2.2. DÉCISION DU CONSEIL D'ÉTAT

Dans un cas particulier, le requérant s'est pourvu 'en cassation' devant le Conseil d'État contre une décision de l'Organe de recours. C'était la première fois depuis

[350] Par la loi du 23 février 2018 (*M.B.* 1er juin 2018), le législateur a explicitement donné à la police et aux services de renseignement le pouvoir de solliciter des informations pertinentes auprès des services partenaires étrangers dans le cadre d'une vérification de sécurité (voir article 22*sexies*, 3° L. C&HS et *Doc. parl.* Chambre, 2017-2018, 54 2767/001, 13). Par cette disposition, le législateur a décidé que, outre le fait qu'une vérification de sécurité ne se limite pas toujours à une simple vérification de certaines bases de données, des informations étrangères peuvent être pertinentes pour une vérification de sécurité.

la création de l'Organe de recours en 1998. Le Conseil d'État a pourtant déclaré le recours recevable[351], bien que non fondé.[352]

IX.2.3. RESPONSABILITÉ DE L'ORGANE DE RECOURS

Nonobstant l'absence de personnalité juridique dans le chef de l'Organe de recours, à la suite d'une décision de la juridiction administrative et d'un arrêt d'incompétence du Conseil d'État, un justiciable a lancé une action en responsabilité. Citation fut introduite devant le Tribunal francophone de Première instance de Bruxelles. Relevons qu'il avait non seulement cité l'État belge, mais également l'Organe de recours. Cette affaire est pendante devant la Cour d'appel de Bruxelles à la suite du jugement rendu le 7 septembre 2018 par la juridiction d'instance mentionnée qui avait condamné l'Organe de recours au paiement d'un dommage.

IX.2.4. DEUX QUESTIONS AU REGARD DE L'ARTICLE 6 DE LA CONVENTION EUROPÉENNE DES DROITS DE L'HOMME (CEDH)

Le président de l'Organe de recours estime approprié de sensibiliser la Chambre des représentants sur les questions soulevées par la jurisprudence européenne et que la Loi organique sur l'Organe de recours n'a pas, jusqu'à ce jour, envisagées.

En effet, l'article 6 de la CEDH consacre le droit à un procès équitable tant en matière judiciaire qu'administrative. Il vise en son alinéa premier notamment la question de la publicité des audiences et du prononcé des décisions à intervenir :
"Toute personne a droit à ce que sa cause soit entendue équitablement, publiquement et dans un délai raisonnable, par un tribunal indépendant et impartial, établi par la loi, qui décidera, soit des contestations sur ses droits et obligations de caractère civil, soit du bien-fondé de toute accusation en matière pénale dirigée contre elle. Le jugement doit être rendu publiquement, mais l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique, lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent, ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice."

---

351 *In extenso* : W. VAN LAETHEM, 'Problemen met veiligheidsadvies van beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen', *Juristenkrant* 2021, 439, 8-9.

352 Conseil d'État, arrêt n° 251.927, 26 octobre 2021 (www.raadvst-consÉtat.be).

La situation au regard du droit actuel et de la jurisprudence européenne nécessite une réflexion dans l'intérêt du justiciable. Il s'agit, d'une part, de la question de la publication des décisions et, d'autre part, de la question des audiences publiques.

IX.2.4.1. LA PUBLICATION

Déjà fin juin 2014, la Commission de Modernisation de l'Ordre judiciaire (CMOJ) avait abordé cette question.[353] Pour rappel, la Belgique a trois cours suprêmes : la Cour de cassation, le Conseil d'État et la Cour constitutionnelle. Chacune d'entre elles est soumise à un régime différent de publication de ses décisions et chacune en assure de façon autonome la publicité. De manière plus générale, l'accessibilité de la jurisprudence est assurée en Belgique par des banques de données publiques ou privées et par des revues.

Pour le Conseil d'État, la matière est régie par un arrêté royal et un arrêté ministériel.[354] La règle est la publication de tous les arrêts, sous la seule réserve de la matière très spécifique de la législation concernant l'accès au territoire, le séjour, l'établissement et l'éloignement des étrangers. Il n'y a donc pas, contrairement à celle de la Cour de cassation, de filtre qualitatif empêchant l'accès à une partie de la jurisprudence. Le Conseil d'État a en effet adopté une double approche dans la publication de ses décisions : d'une part, il met en ligne très rapidement l'ensemble de sa jurisprudence, d'autre part, dans une banque de données séparée, il procède à une sélection raisonnée et structurée des arrêts qu'il estime intéressants. Cette banque de données est publique et gratuite. Le rapport au Roi précédent l'arrêté royal est très éclairant sur l'importance d'assurer l'accessibilité à la jurisprudence de cette juridiction. La question de l'anonymisation est également traitée dans l'arrêté royal lui-même.

Plus fondamentalement, le rapport de la CMOJ constatait le « *déficit démocratique* » qu'engendre cette indisponibilité de la jurisprudence des cours et tribunaux : comment garantir l'accès pour tous à la justice si cette jurisprudence est inaccessible ? Comment enseigner et pratiquer le droit si nul ne sait comment la justice se dit et se fait ?

En ce qui concerne l'Organe de recours, la Loi organique du 11 décembre 1998 ne prévoit aucune disposition à cet égard. Les différentes autorités de sécurité ont exprimé leur inquiétude face à une telle publication.

---

353 Commission de Modernisation de l'Ordre judiciaire, *Rapport consacré à la question de la publication des décisions judiciaires. La plume, le Pélikan et le nuage*, 30 juin 2014.

354 Arrêté royal du 7 juillet 1997 relatif à la publication des arrêts du Conseil d'État et des ordonnances de non-admission du Conseil d'État et Arrêté ministériel du 3 février 1998 déterminant le réseau d'informations accessible au public et le support magnétique en vue de la consultation et de l'enregistrement des arrêts du Conseil d'État.

Le président de l'Organe de recours est bien conscient que sa jurisprudence traite des questions spécifiques et dont certaines pourraient toucher la sécurité des intérêts de l'État. Il est indéniable que l'anonymisation doit être systématique et très prudente à cet égard. La problématique de l'anonymisation est, en Belgique, étroitement liée à celle de la protection de la vie privée dans le cadre des banques de données. Dans le cadre de sa compétence – limitée aux personnes physiques – l'ancienne Commission de protection de la vie privée a suggéré une anonymisation poussée.[355]
L'ouverture par la Chambre des représentants d'un débat sur la publication des décisions de l'Organe de recours n'apparaît-elle pas aujourd'hui comme nécessaire dans le cadre du renforcement démocratique des institutions ?

IX.2.4.2. LES AUDIENCES PUBLIQUES

L'article 6 CEDH consacre le droit à un procès équitable et vise en son alinéa premier notamment la question de la publicité des audiences et du prononcé des décisions à intervenir. Le législateur belge de 1998 n'a pas abordé la question de la publicité des audiences dans la Loi organique sur l'Organe de recours.

Il ressort de l'analyse de la Cour européenne les principes généraux suivants en matière d'audience[356] :
« Le justiciable a, en principe, le droit à une audience publique car cela le protège contre une justice secrète échappant au contrôle du public. Par la transparence qu'elle donne à l'administration de la justice, l'audience publique aide à réaliser le but de l'article 6 § 1 : le procès équitable. Si la tenue d'une audience publique constitue un principe fondamental consacré par l'article 6 § 1, cette obligation n'est pas pour autant absolue (De Tommaso c. Italie [GC], 2017, § 163). Pour déterminer si un procès répond à l'exigence de publicité, il faut envisager la procédure dans son ensemble (Axen c. Allemagne, 1983, § 28).
Dans une procédure se déroulant devant un seul tribunal, le droit de chacun à ce que sa cause soit « entendue publiquement », au sens de l'article 6 § 1, implique le

---

355 Avis n°42/97 du 23 décembre 1997 et recommandation n°03/2012 du 8 février 2012. En 1997, la Commission de la protection de la vie privée écrivait : « *La protection est d'autant plus nécessaire que les outils de navigation et les capacités des systèmes d'information en termes d'interconnexion de données sont de plus en plus puissants et que le contrôle des utilisations opérées à partir de ces interrogations à distance est quasiment inexistant. Ainsi, on peut imaginer la facilité avec laquelle un internaute averti recueillera l'ensemble de la jurisprudence relative à des licenciements pour motifs graves pour en extraire les noms et adresses des employés mis en cause, ou identifiera les médecins dont la responsabilité aurait été mise en cause devant les tribunaux. Le comportement d'un juge face à tel ou tel type de conflits pourra être évalué statistiquement et le nom d'un avocat pourra être associé à un pourcentage d'issues favorables de procès.* » (Avis CPVP n°42/97 du 23 décembre 1997).

356 CONSEIL DE L'EUROPE, COUR EUROPÉENNE DES DROITS DE L'HOMME, *Guide sur l'article 6 de la Convention européenne des droits de l'homme*, 31 décembre 2021 https://www.echr.coe.int/documents/guide_art_6_fra.pdf

droit à une «audience » (Göç c. Turquie [GC], 2002, § 47 ; Fredin c. Suède (no 2), 1994, §§ 21-22 ; Allan Jacobsson c. Suède (no 2), 1998, § 46 ; Selmani et autres c. l'ex-République yougoslave de Macédoine, 2017, §§ 37-39).

La publicité des débats doit également être lue sous l'angle de la question de la présence du public et de la presse : La publicité des débats judiciaires protège les justiciables contre une justice secrète échappant au contrôle du public et constitue ainsi l'un des moyens qui contribue à la préservation de la confiance dans les tribunaux. Elle aide à atteindre le but tenant à l'équité du procès (Martinie c. France [GC], 2006, § 39 ; Diennet c. France, 1995, § 33 ; Gautrin et autres c. France, 1998, § 42 ; Hurter c. Suisse, 2005, § 26 ; Lorenzetti c. Italie, 2012, § 30). L'article 6 § 1 ne fait cependant pas obstacle à ce que les juridictions décident, au vu des particularités de l'affaire, de déroger à ce principe (Martinie c. France [GC], 2006, §§ 40-44). Le huis clos, qu'il soit total ou partiel, doit alors être strictement commandé par les circonstances de l'affaire (Lorenzetti c. Italie, 2012, § 30). Le texte de l'article 6 § 1 prévoit plusieurs exceptions. Selon le libellé de cet article, « l'accès de la salle d'audience peut être interdit à la presse et au public pendant la totalité ou une partie du procès » :

– dans l'intérêt de la moralité, de l'ordre public ou de la sécurité nationale dans une société démocratique » (B. et P. c. Royaume-Uni, 2001, § 39 ; Zagorodnikov c. Russie, 2007, § 26) ;

– lorsque les intérêts des mineurs ou la protection de la vie privée des parties au procès l'exigent » : les intérêts des mineurs ou la protection de la vie privée des parties au procès sont en jeu, par exemple, dans les procédures relatives à la garde d'enfants mineurs à la suite du divorce ou de la séparation des parents, ou lors des litiges entre membres d'une même famille (ibidem, § 38). En revanche, dans les affaires qui concernent le placement d'un enfant dans une institution publique, les raisons de soustraire l'affaire à l'examen du public doivent faire l'objet d'un examen attentif (Moser c. Autriche, 2006, § 97). Dans le cas d'une procédure disciplinaire dirigée contre un médecin, si la nécessité de préserver le secret professionnel ou la vie privée des patients peut motiver le huis clos, celui-ci doit être strictement commandé par les circonstances (Diennet c. France, 1995, § 34). Pour un exemple de procédure dirigée contre un avocat, voir Hurter c. Suisse, 2005, §§ 30-32 ;

– « ou dans la mesure jugée strictement nécessaire par le tribunal, lorsque dans des circonstances spéciales la publicité serait de nature à porter atteinte aux intérêts de la justice » : il est possible de déroger au principe de la publicité des débats pour protéger la sécurité et l'intimité des témoins ou pour favoriser le libre échange d'informations et d'opinions dans la poursuite de la justice (B. et P. c. Royaume-Uni, 2001, § 38 ; Osinger c. Autriche, 2005, § 45).

La Cour a ajouté que la jurisprudence concernant la tenue d'une audience en tant que telle – et visant surtout le droit à s'exprimer devant le tribunal prévu à l'article 6 § 1 – pouvait s'appliquer par analogie s'agissant de la tenue de débats ouverts au public. Ainsi, lorsqu'une audience s'est tenue en vertu du droit national, cette audience doit en principe être publique. La tenue d'une audience publique n'est pas pour autant

absolue, les circonstances qui permettent de s'en dispenser dépendant essentiellement de la nature des questions dont les tribunaux internes se trouvent saisis (De Tommaso c. Italie [GC], 2017, §§ 163-167). Des « circonstances exceptionnelles – et notamment le caractère hautement technique des questions à trancher – peuvent justifier l'absence de publicité, pourvu que la spécificité de la matière n'exige pas le contrôle du public » (Lorenzetti c. Italie, 2012, § 32).
La simple présence de documents classifiés dans un dossier judiciaire n'implique pas automatiquement l'exclusion du public des débats. Ainsi, avant d'exclure le public d'une affaire particulière, le tribunal devrait considérer de manière spécifique si une telle exclusion est nécessaire à la protection d'un intérêt public et la limiter à ce qui est strictement nécessaire pour atteindre l'objectif poursuivi (Nikolova et Vandova c. Bulgarie, 2013, §§ 74-77 au sujet d'un huis clos en raison de documents classés secret d'État ; voir aussi sur les principes, Vasil Vasilev c. Bulgarie, 2021,§§ 105-106). »*

La question de la publicité des audiences mérite une attention particulière et un débat approfondi soumis à la Chambre des représentants. Le président de l'Organe de recours est prêt à participer activement à ce processus.

IX.2.5. EFFECTIVITÉ DES DÉCISIONS DE L'ORGANE DE RECOURS

La question de l'effectivité des décisions de l'Organe de recours se pose à l'égard de l'Autorité nationale de sécurité (ANS). Outre le refus de transmettre des dossiers administratifs dans le cadre de certains recours, le président de l'Organe de recours rappelle le prescrit de l'article 12 § 6 de la Loi organique qui stipule : « *Les décisions de l'organe de recours sont exécutoires de plein droit dès leur notification* ».

C'est ainsi que, dans une affaire, l'Organe de recours avait octroyé à l'intéressé une habilitation de sécurité (niveau SECRET UE) qui lui était refusée par l'ANS. Le 19 juillet 2021, le Tribunal de première instance francophone de Bruxelles (RG 2021/51/C) a, par ordonnance contradictoire, en référé, donné injonction à l'État belge, par l'intermédiaire de l'ANS, de délivrer au requérant son habilitation de sécurité dans le mois de la signification de l'ordonnance sous peine d'une astreinte fixée à 500 euros par jour de retard, avec un maximum de 10.000 euros.

Relevons que dans ce même dossier, les médiateurs fédéraux saisis par l'intéressé en raison de la non-exécution de la décision de l'Organe de recours, étaient intervenus, toujours sans succès. Ils ont classé la plainte comme fondée avec la motivation suivante : *« […] Dans un état de droit, la non-exécution d'une décision prise dans le cadre d'un recours administratif porte une atteinte sérieuse à la sécurité juridique ».*

IX.2.6. PERSPECTIVE

La ministre de la Défense, suivant les recommandations du Comité permanent R, entend déposer des projets de loi visant à systématiser le principe d'une vérification de sécurité tant pour les civils que pour les miliaires de la Défense. Cet avis de sécurité ne serait plus uniquement requis lors de la candidature mais durant toute la vie professionnelle des différents membres de la Défense. On peut supposer que cet avis de sécurité sera renouvelé tous les cinq ans. Les éventuels recours seront en principe de la compétence de l'Organe de recours.

À la suite de l'enquête de contrôle de septembre 2021 du Comité permanent R sur la manière dont la Sûreté de l'État a assuré le suivi de la commissaire du gouvernement Ishane Haouach, celui-ci avait recommandé que l'exercice de certaines « fonctions publiques » requiert la vérification préalable de l'intégrité, de la loyauté et de la discrétion, comme l'exige la législation en vigueur dans certains pays européens. La mise en œuvre de cette recommandation devrait entraîner une extension des avis de sécurité qui eux aussi feront l'objet d'un contrôle juridictionnel de l'Organe de recours.

La question de la franchise postale devrait être rencontrée tout comme la possibilité d'introduire un recours par voie digitale et de permettre les actes de notification, suivant la préférence du justiciable, par voie postale ou digitale pour la procédure pendante devant l'Organe de recours.

CHAPITRE X.
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

X.1. COMPOSITION DU COMITÉ PERMANENT R

La composition du Comité est restée identique en 2021 : Serge Lipszyc (F), premier substitut de l'auditeur du travail près de l'auditorat du travail de Liège, a continué à remplir sa mission de président. Pieter-Alexander De Brock (N), et Thibaut Vandamme (F), substitut du procureur du Roi de l'arrondissement du Luxembourg, ont exercé leur mandat de membre.[357] [358]

En attendant la nomination d'un greffier, Wauter Van Laethem (N) a été désigné comme greffier faisant fonction.[359]

Plusieurs changements sont également intervenus au sein du services d'Enquêtes, dont la direction est assurée par Fabian Poncelet (F) depuis le 1er janvier 2021. Un nouveau commissaire-auditeur francophone a rejoint les rangs du service en juin 2021. Il est détaché de la Police fédérale. Un commissaire-auditeur a remis sa démission et sera remplacé dans le courant de l'année 2022.

Enfin, le cadre administratif du Comité permanent R a lui aussi subi quelques changements. Le juriste, recruté en décembre 2020, et en fonction à la Section documentation et analyse juridique, a repris ses fonctions dans son service d'origine en août 2021. Deux attachés francophones ont rejoint les rangs de cette

---

357 Thibaut Vandamme a prêté serment le 11 janvier 2021. En application de l'article 157, paragraphe 6, du règlement de la Chambre, lors de la séance plénière du 20 mai 2021, Thierry Werts a été désigné comme premier suppléant de Thibaut Vandamme (CRABV55PLEN105, 20 mai 2021, 46).

358 Fin 2021, Wauter Van Laethem a remis sa démission en tant que deuxième suppléant du conseiller néerlandophone (*C.R.I.* Chambre 2021-2022, 10 novembre 2021 CRIV55PLEN139, 68). Il a été remplacé en mars 2022 par Filip Vanneste, substitut du procureur général près la Cour d'appel d'Anvers (*C.R.I.* Chambre 2021-2022, 24 mars 2022, CRIV55PLEN171, 67).

359 Un appel à candidature pour le poste de greffier du Comité permanent R est paru à la mi-mai 2020 au Moniteur belge. Le 21 juin 2021, un projet de loi a été déposé pour élargir les conditions de nomination des greffiers respectifs des Comités permanents R et P (*Doc.Parl.* Chambre 2020-21, 55K2064/001). La question a d'abord été examinée en Conférence des présidents (24 février et 3 mars 2021) (*Doc.Parl.* Chambre 2020-21, 55K1924/001). La 'loi du 14 août 2021 modifiant la loi organique du 18 juillet 1991 [...], et visant à élargir les conditions de nomination des greffiers du Comité R et du Comité P' a été publiée au Moniteur belge le 8 décembre 2021. Une nouvelle vacance est parue au Moniteur belge le 19 juillet 2021. Le 26 avril 2022, Frédéric Givron (F) a prêté serment en présence de la Présidente de la Chambre en tant que nouveau Greffier du Comité permanent R.

section en octobre 2021. En avril 2021, une secrétaire statutaire néerlandophone a été recrutée. Fin 2021, le cadre administratif comptait 18 collaborateurs.

À la mi-juin 2021, le président du Comité permanent R s'est à nouveau adressé à la Présidente de la Chambre des représentants concernant le manque de personnel et l'augmentation considérable de tâches assignées au Comité.[360] Malgré le dynamisme dont fait preuve la Chambre dans le cadre des objectifs de synergie, auxquels le Comité apporte son soutien, le Comité a jugé nécessaire de solliciter un renfort urgent. Il n'est en effet pas en mesure de mener à bien toutes les missions légales ni de répondre de manière adéquate aux différentes demandes formulées par la Chambre.

X.2. UN AUDIT RELATIF AU BIEN-ÊTRE AU COMITÉ

À la suite des signes de malaise au sein du Comité permanent R, il a été décidé de charger IDEWE, un service externe de prévention et de protection au travail, d'effectuer une analyse des risques psychosociaux. L'audit a analysé des thèmes correspondant aux cinq domaines des risques psychosociaux au travail (contenu du travail, organisation du travail, environnement de travail, conditions de travail et relations interpersonnelles au travail). En a résulté un rapport complet[361] détaillant les résultats de l'analyse et formulant un avis à l'employeur.[362]

Prenant appui sur cet audit, un processus de changement a été initié. Le Comité permanent R sera guidé par le SPF Stratégie et Appui. Le projet comprend une enquête auprès des *stakeholders*, une analyse SWOT et une analyse PESTEL[363] approfondies. Le projet devrait être achevé à la fin du mois de juin 2022.

Suite aux résultats de l'audit, une nouvelle personne de confiance néerlandophone a été nommée à la mi-décembre 2021. La nomination d'une personne de confiance francophone a suivi à la fin du mois de janvier 2022.[364]

---

360 Lettre du Président du Comité permanent R à la Présidente de la Chambre des représentants datée du 16 juin 2021.

361 IDEWE, Analyse des risques psychosociaux, 23 novembre 2021, 30 p.

362 Le modèle 'd'efficacité collective' (SDRPI) a été utilisé pour traiter les problèmes identifiés. Ce modèle se concentre sur le **S**ystème (contexte dans lequel le travail est effectué), les **O**bjectifs (fixation d'objectifs clairs et partagés), les **R**ôles (ce que l'on peut attendre de chacun), les **P**rocédures (développement de pratiques appropriées) et les **R**elations interpersonnelles.

363 L'analyse PESTEL est un modèle d'analyse de stratégie d'entreprise utilisé pour identifier l'influence des facteurs externes sur une organisation. L'acronyme PESTEL renvoie aux facteurs politiques, économiques, sociologiques, technologiques, environnementaux et légaux.

364 La législation (2014) sur les risques psychosociaux au travail impose aux personnes de confiance de suivre une formation de base de 30 heures. L'employé est tenu de suivre la formation dans les deux ans suivant sa nomination en tant que personne de confiance.

X.3. RÉUNIONS AVEC LA COMMISSION DE SUIVI

La composition de la Commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de Contrôle des services de renseignement et de sécurité (la Commission de suivi) a connu quelques changements en 2021. En étaient membres avec voix délibérative Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen)[365], Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Denis Ducarme (MR), Servais Verherstraeten (CD&V), Nabil Boukli (PVDA-PTB), Patrick Dewael[366] (Open Vld) et Bert Moyaers (Vooruit). La Présidente de la Chambre, Eliane Tillieux (PS), assume la présidence de la Commission. Georges Dallemagne (Les Engagés) participe en tant que membre sans voix délibérative.

Dans le courant de l'année 2021, et malgré la crise sanitaire, plusieurs réunions (neuf au total) ont eu lieu avec la Commission. Lors de ces réunions, tenues à huis clos, plusieurs enquêtes de contrôle que le Comité permanent R avait clôturées ont été discutées.[367] Fin avril et début juillet 2021, des réunions ont eu lieu avec le Comité permanent P pour discuter respectivement de l'enquête de contrôle conjointe relative à l'Organe de coordination pour l'analyse de la menace (OCAM) et ses services d'appui, et de l'enquête de contrôle conjointe relative au rôle de l'OCAM dans le suivi de Jürgen Conings. Du temps a également été consacré au rapport rédigé dans le cadre de la compétence de contrôle partagée avec l'Organe de contrôle de l'information policière (C.O.C.) concernant les banques de données (art. 44/6 LFP). Lors de la réunion du 22 septembre 2021, le *Rapport d'activités 2020* du Comité permanent R a été discuté.[368] La Commission a notamment souligné *'l'importance d'un rapport annuel, non seulement pour rendre compte des activités du Comité R au parlement, mais également pour informer les personnes extérieures en toute transparence (professeurs, journalistes, personnel des services de renseignement, ...)'*. Une série de thématiques ont particulièrement retenu l'attention des Députés telles que le suivi des plaintes, le Memorandum of Understanding (MoU) entre le SGRS et les services de renseignement rwandais, le COVID-19 et le rôle des services de renseignement, ou encore les interceptions étrangères. En guise de

365 Remplacée depuis lors par Julie Chanson (Ecolo-Groen).

366 Remplacé depuis lors par Tim Vandeput (Open Vld).

367 Une réunion s'est tenue avec comme point à l'agenda notamment le rapport intermédiaire (état des lieux) de l'enquête de contrôle relative à Jürgen Conings.

368 La Commission se réfère à cet effet à l'article 66*bis*, § 3,1° L.Contrôle, tel que modifié par la loi du 6 janvier 2014 modifiant diverses lois de réformes institutionnelles, *M.B.* 31 janvier 2014.

conclusion, la Commission a pris *'acte du Rapport d'Activités 2020 du Comité R et souscrit à ses recommandations*.[369]

Enfin, la Commission s'est également penchée sur les problèmes internes à la tête du Comité permanent R.[370] Trois réunions de la Commission ont été organisées, à huis clos, à l'automne 2021.

X.4. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

Sans compter les quelques contacts (informels), aucune réunion commune ne s'est tenue en 2021 avec le Comité permanent P.[371]

Trois enquêtes communes ont été effectuées en 2021 : l'enquête de suivi sur la mise en œuvre des recommandations émises par les Comités permanents R et P dans le cadre de l'enquête sur les services d'appui de l'OCAM (cf. I.1) et l'enquête de contrôle sur les quatre services d'appui 'supplémentaires' de l'OCAM (cf. I.2). La troisième enquête commune portait sur 'le rôle de l'OCAM dans le suivi du militaire Jürgen Conings' (cf. I.10). À cette fin, les services d'appui des deux Comités ont coopéré activement.

Les deux Comités ont chargé leurs services d'Enquêtes respectifs de préparer des procédures de travail pour le traitement des plaintes et des enquêtes de contrôle conjointes. Le Comité permanent P a également accepté la demande du Comité permanent R, et plus particulièrement de son service d'Enquêtes, d'obtenir une formation dans le cadre de la consultation de la Banque de données nationale générale (BNG).[372] Enfin, conformément à l'art. 52 L.Contrôle, les rapports d'activités et les rapports d'enquêtes de contrôle ont été échangés.

---

369 *Doc. parl.* Chambre 2020-21, 55K2209/01, 20 octobre 2021 (Rapport d'activités 2020 du Comité permanent de Contrôle des services de renseignement et de sécurité, Rapport fait au nom de la commission spéciale chargée de l'accompagnement parlementaire du Comité permanent de Contrôle des services de police et du Comité permanent de contrôle des services de renseignement et de sécurité).

370 La Commission s'est notamment réunie suite à la parution d'un article publié à la suite de l'affaire Jürgen Conings (Q. JARDON, 'Serge Lipszyc. Gendarme des services secrets, *Wilfried*, Automne 2021, n° 17, 1-7) et une demande introduite auprès de la Présidente de la Chambre par les deux conseillers.

371 Art. 52 L.Contrôle prévoit qu'au minimum deux réunions communes doivent s'organiser chaque année.

372 En octobre 2017, le Comité permanent R a signé un protocole d'accord avec la Police fédérale concernant l'application de l'arrêté royal du 30 octobre 2015 relatif à l'accès direct du Comité permanent de contrôle des services de renseignement et de sécurité et de son Service d'enquêtes aux données et informations de la Banque de données Nationale Générale visée à l'article 44/7 de la loi sur la fonction de police (*M.B.* 20 novembre 2015).

X.5. UNE ATTENTION MÉDIATIQUE IMPORTANTE

Le Comité permanent R a fait l'objet d'une attention médiatique importante en 2021, ce qui dénote des années précédentes. Quatre événements (repris en ordre chronologique) en sont principalement à l'origine :

Tout d'abord, la publication du rapport de l'enquête de contrôle relative au suivi opéré par les services de renseignements de la menace posée par l'extrême droite.[373] Les principales conclusions ont été partagées par plusieurs médias belges.

L'affaire Jürgen Conings et le rôle occupé par le Comité ont ensuite été largement médiatisés. Pour rappel, le Comité a été chargé par la ministre de la Défense de réaliser une enquête de contrôle afin de vérifier notamment la fiabilité des informations relatives aux personnes suspectées de radicalisation au sein de la Défense, de formuler des recommandations en vue de garantir le bon fonctionnement du SGRS ainsi que de la Défense dans son ensemble.[374] Les conclusions de ce rapport (très attendu) ont été largement relayées par les médias.

Le Comité permanent R a également été saisi dans l'affaire Haouach, ancienne commissaire de gouvernement auprès de l'Institut pour l'égalité entre les femmes et les hommes.[375] Cette affaire a fait l'objet d'une importante attention médiatique suite aux allégations dans la presse faisant état de l'existence d'une note de la VSSE évoquant des 'contacts étroits' entre les Frères musulmans et la commissaire de gouvernement, à l'insu ou non de cette dernière.

Enfin, est parue en octobre 2021 l'interview accordée par le président du Comité à la revue *Wilfried (supra)*. Dans cette interview, le président exprimait certaines inquiétudes personnelles suite à plusieurs événements et dossiers marquants tels que l'affaire Jürgen Conings. Cette interview, les réactions à celle-ci, ainsi que les tensions au sein de la direction du Comité qui s'en sont suivies, ont retenu l'attention des médias.

Le Comité est conscient que la communication sur ses missions constitue un enjeu complexe mais ô combien essentiel. Il ambitionne d'y prêter une attention plus grande à l'avenir, en améliorant notamment la mise à disposition des informations. La révision future de son site internet s'inscrit pleinement dans cette démarche.

X.6. LE 'DATA PROTECTION OFFICER' AU COMITÉ

Un *Data Protection Officer* (DPO) est nommé depuis plusieurs années au sein du Comité, pour tous les traitements de données à caractère personnel qui ne relèvent

---

373 COMITÉ PERMANENT R, *Rapport d'activités 2020*, 38 et s. ('I.7. Le suivi de l'extrême droite par les services de renseignements belges').

374 À ce propos, 'I.9. La détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings.'

375 À ce propos, voir 'I.11. Le suivi d'un commissaire de gouvernement par la VSSE'.

pas de la «sécurité nationale». Dans le cadre de l'exercice de synergie réalisé par la Chambre des représentants, le DPO remplit également cette fonction pour d'autres institutions à dotation situées dans le bâtiment du Forum. Le *Data Protection Officer* a fourni des conseils sur la surveillance par caméra pour laquelle un registre a été établi et la déclaration formalisée suite à la 'nouvelle loi caméras'[376]. En outre, le DPO a également fourni des conseils et des informations sur la gestion interne des données à caractère personnel des membres du personnel, notamment dans le contexte de la pandémie de COVID-19.

X.7. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Le budget 2021 du Comité permanent R a été fixé à 5,215 millions d'euros, ce qui représente une augmentation de 13 % par rapport à 2020.[377]

La principale raison de cette augmentation provient en grande partie de la présentation d'un projet opérationnel de digitalisation des processus de travail. Ce projet était présenté en partenariat avec un opérateur industriel coutumier des administrations publiques et habitué à leurs procédures administratives. Bien qu'adhérant aux principes présentés par le Comité, la Commission de la Comptabilité a cependant décidé de geler le processus de gestion documentaire dans l'attente de conclusions des concertations en cours entreprises entre les services de la Questure et le Comité afin que le projet puisse être intégré dans les synergies éventuelles.

Les sources de financement attribuées par la Chambre des représentants[378] sont les suivantes : 74,44 % au titre du budget de dotation et 25,56 % de boni de 2019.

L'exécution du budget 2021 a produit un boni comptable de 1,87 millions d'euros (chiffres non-audités) euros, représentant la différence entre le budget approuvé et les dépenses constatées.

Le budget est composé de différentes sources de financement dont le seul apport en termes de trésorerie nette est constitué par la dotation inscrite au budget général de l'État. Jusqu'en 2017, cette dotation ne suffisait pas à couvrir les dépenses réelles du Comité, ce qui générait une perte structurelle. La tendance à appliquer autant que possible l'article 57 alinéa 1er L.Contrôle (qui stipule que les crédits de fonctionnement sont inscrits au budget des dotations) permet à ce jour au Comité de financer ses activités.

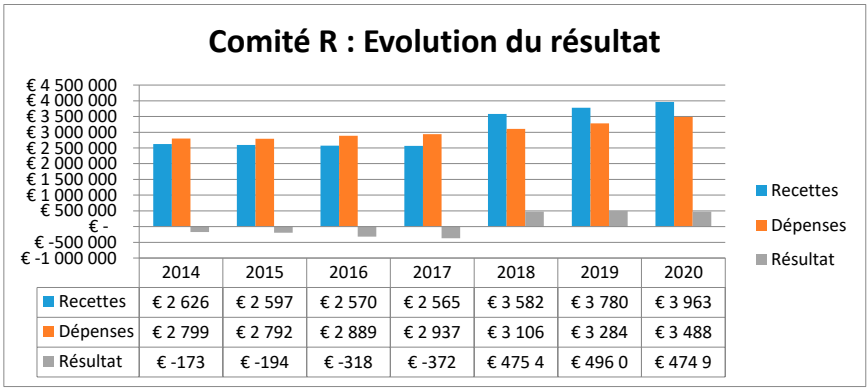
---

376 Loi du 30 juillet 2018 modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, en vue d'améliorer la cohérence du texte et sa conformité avec le Règlement général sur la protection des données (RGPD), *M.B.* 31 août 2018.

377 *C.R.I.* Chambre 2020-21, 17 décembre 2020, PLEN 081, 63.

378 *Doc. parl.* Chambre 2020-21, 55-1676/001, 30-34.

Le dégagement d'un boni comptable considérable provient essentiellement de l'écart temporel existant entre l'approbation des budgets et l'entrée effective en service du personnel à cause de la longueur des procédures de recrutement et de l'obtention des habilitations de sécurité requises. Cette tendance a été particulièrement marquée pendant l'exercice 2021, où le Comité a été confronté à plusieurs phénomènes concomitants tels que le départ à la retraite de plusieurs membres du personnel et les retards enregistrés dans le remplacement de ces personnes. On peut affirmer que 2021 a connu un *turnover* important dans les effectifs de chaque catégorie de personnel tant au niveau managérial qu'au niveau opérationnel : ainsi, le poste de greffier est resté vacant durant toute l'année jusqu'à désignation récente d'un successeur par la Chambre des représentants (voir *supra*). D'autres postes ont également été affectés par des choix de carrière différents de la part de leurs titulaires. Cela, cumulé au gel du budget affecté au projet de digitalisation (*voir supra*) décidé par la Chambre, a généré un boni important qui sera probablement réaffecté au budget de fonctionnement 2023 lors de l'examen des propositions budgétaires par la Chambre des représentants.



	2014	2015	2016	2017	2018	2019	2020
Recettes	€ 2 626	€ 2 597	€ 2 570	€ 2 565	€ 3 582	€ 3 780	€ 3 963
Dépenses	€ 2 799	€ 2 792	€ 2 889	€ 2 937	€ 3 106	€ 3 284	€ 3 488
Résultat	€ -173	€ -194	€ -318	€ -372	€ 475 4	€ 496 0	€ 474 9

À partir de l'exercice 2023, le Comité sera pleinement intégré dans le projet de mise en place de Synergies initié par la Chambre (voir *infra*)[379] qui auront des impacts indéniables sur le fonctionnement des organes à dotation en général et du Comité permanent R en particulier. Ces changements auront un effet sur le cadre du personnel et sur les crédits de fonctionnement qui seront mutualisés dans la mesure du possible. La date-pivot d'entrée en application de ces modifications a été fixée au 1er janvier 2023.

379 *Doc. parl.* Chambre 2020-21, 55-1924/001.

X.8. MISE EN ŒUVRE DES RECOMMANDATIONS DE L'AUDIT DE LA COUR DES COMPTES

À la demande de la Commission de la Comptabilité de la Chambre des représentants, la Cour des comptes a, dès 2017, initié une enquête sur les institutions à dotation, conjointement à Ernst & Young.[380] Le rapport d'audit, transmis fin mars 2021, reprenait des recommandations concernant les 'missions' des neuf institutions à dotation concernées par l'audit, dont le Comité permanent R. [381]

Entre janvier et début février 2021, les services de la Questure et le secrétariat de la Commission ont auditionné les institutions concernées, parmi lesquelles le Comité permanent R.

En avril 2021, un accord a été trouvé au sein de la Commission de la Comptabilité sur les synergies à initier entre les institutions concernées. Il s'agit notamment de mettre en place un centre de services partagés (Incentris) et un portail citoyen. Il a également été décidé d'harmoniser les statuts du personnel et les barèmes des institutions concernées ainsi que de rationaliser le parc automobile des institutions. Une réorganisation de certains locaux, notamment ceux du Comité permanent R, afin d'y accueillir la Commission BIM, est aussi envisagée. Pour concrétiser ces orientations, des groupes de travail thématiques ont été mis en place auxquels participent des membres de la Chambre ainsi que de certaines institutions, la logique étant qu'il ait une représentation par 'famille' d'institutions (une famille étant constituée d'institutions aux missions apparentées).[382] [383]

En septembre 2021, une réunion a été organisée par la Chambre à destination des membres du personnel des institutions concernées afin d'informer ces derniers des orientations décidées pour maximiser les synergies et l'état d'avancement des projets visant à les concrétiser.

Afin d'étudier la possibilité d'allouer une partie des locaux du Comité permanent R à la Commission BIM, plusieurs visites des locaux du Comité permanent R ont été organisées à partir d'octobre 2021 en présence de l'architecte de la Chambre. Des réunions se sont également tenues avec la Commission BIM,

---

380 La Cour des comptes s'est surtout concentrée sur les aspects budgétaires (une analyse des recettes et des dépenses) et sur la délimitation des missions des différentes institutions. De son côté, Ernst & Young était principalement chargé de procéder à une analyse approfondie des processus, des systèmes et de l'organisation de chacune de ces institutions.

381 *Institutions à dotation. Missions – Recettes– Dépenses.* Audit réalisé à la demande de Commission de la Comptabilité de la Chambre des représentants, Rapport approuvé le 28 mars 2018 par l'assemblée générale de la Cour des comptes.

382 Le Comité permanent R appartient à la famille « Sécurité et protection » à laquelle appartiennent également le Comité permanent P, l'Autorité de protection des données, le C.O.C. et la Commission BIM.

383 A la mi-octobre 2021, la Présidente de la Chambre a demandé au Comité de participer plus activement et de veiller à un flux d'informations efficace afin de permettre aux groupes de travail mis en place dans le cadre du projet 'synergie entre les institutions à dotation' de remplir adéquatement leurs tâches. La Présidente s'est dit consciente que l'absence de greffier pouvait complexifier les choses.

le Comité permanent R et ce même architecte afin d'évaluer les implications et les coûts d'un tel projet. Un dossier sera remis dans le courant de l'année 2022 à la Commission de la Comptabilité amenée à se prononcer sur un déménagement effectif de la Commission BIM.

X.9. FORMATIONS

Compte tenu de l'intérêt pour l'organisation, le Comité permanent R encourage ses membres et ses collaborateurs à suivre des formations générales (en informatique, en management, etc.) ou propres au secteur, ou encore à participer à des conférences.[384] En raison des mesures adoptées dans le cadre de la crise sanitaire, il n'a pas été possible de suivre des formations internes ou externes en 2021.

[384] Les briefings de sécurité auxquels les collaborateurs sont tenus d'assister ont, quant à eux, bien eu lieu.

CHAPITRE XI.
RECOMMANDATIONS

À la lumière des enquêtes de contrôle, des contrôles et des inspections clôturés en 2021, le Comité permanent R formule les recommandations reprises ci-après. Ces recommandations portent à la fois sur la protection des droits que la Constitution et la loi confèrent aux personnes, sur la coordination et l'efficacité des services de renseignement, de l'Organe de coordination pour l'analyse de la menace (OCAM) et des services d'appui ainsi que sur l'optimalisation des possibilités d'enquête du Comité permanent R.

XI.1. RECOMMANDATIONS RELATIVES À LA PROTECTION DES DROITS QUE LA CONSTITION ET LA LOI CONFÈRENT AUX PERSONNES

XI.1.1. RÉDACTION D'UNE PROPOSITION DE DIRECTIVE SUR LA COMMUNICATION D'INFORMATIONS PAR LA VSSE OU LE SGRS AUX EMPLOYÉS ET ADAPTATION DES DIRECTIVES EXISTANTES[385]

Le Comité a recommandé que la Sûreté de l'État (VSSE) et le Service Général du Renseignement et de la Sécurité (SGRS), dans les six mois suivant la conclusion de l'enquête de contrôle intitulée '*L' échange d'informations sur un collaborateur entre les services de renseignement et un employeur privé ou public*', rédigent une proposition de directive visant à mettre en œuvre la dernière partie de phrase de l'article 19, alinéa 1er L.R&S à l'attention des ministres de la Justice et de la Défense, en leur demandant de soumettre la proposition au Conseil national de sécurité pour approbation.

La VSSE doit en outre évaluer ses directives en la matière et les adapter au cadre légal. Compte tenu de l'importance de cette matière, cette adaptation doit également avoir lieu dans un délai de six mois.

Par ailleurs, le Comité recommande au législateur de préciser si l'article 19, alinéa 1er, dernière phrase L.R&S contient également une obligation, dans certains

[385] Voir Chapitre 'I.3. L'échange d'informations sur un collaborateur entre les services de renseignement et un employeur privé ou public'.

cas, de répondre à une question ou de fournir des informations d'initiative. Dans l'attente d'une initiative législative, cette question doit être réglée dans la directive du Conseil national de sécurité.

XI.1.2. DIRECTIVES EN MATIÈRE DE SUIVI DE MANDATAIRES POLITIQUES[386]

Le Comité permanent R réitère avec insistance sa recommandation précédente remontant à 2013, selon laquelle le SGRS doit établir des directives claires quant au recueil, au traitement, à la consultation, au stockage et à l'archivage des données des mandataires politiques.

Le Comité permanent R recommande également que les services de renseignement accordent, dans leurs rapports, l'attention nécessaire à la position d'une personne mentionnée dans un rapport vis-à-vis de la menace (victime, acteur, passant, etc.)

XI.2. RECOMMANDATIONS RELATIVES À LA COORDINATION ET À L'EFFICACITÉ DES SERVICES DE RENSEIGNEMENT, DE L'OCAM ET DES SERVICES D'APPUI

XI.2.1. RECOMMANDATIONS RELATIVES À L'OCAM ET SES (NOUVEAUX) SERVICES D'APPUI[387]

Une (in)formation pour les membres du personnel de la Direction Générale des Établissements Pénitentiaires détachés auprès de l'OCAM

Il a été constaté que les membres détachés de Direction générale des Établissements Pénitentiaires (DG EPI) ne se déplacent que peu, voire pas du tout, au sein de leur service d'origine et disent ne pas être mis au courant des changements qui pourraient s'y opérer. Une (in)formation régulière leur permettant de connaître les changements éventuels (législatifs ou d'ordre interne par exemple) au sein de leur service d'origine serait une plus-value.

386 Voir Chapitre 'I.8. Enquête de contrôle sur le suivi des mandataires politiques'

387 Voir Chapitres 'I.1 Les services d'appui de l'OCAM (suivi)' et 'I.2. L'OCAM et les services d'appui supplémentaires'

BINII pour la DG EPI et le Service des Cultes et de la Laïcité

Il serait opportun que le SPF Justice dispose du système BINII (*Belgian Intelligence Network Information Infrastructure)* dans les plus brefs délais afin de permettre aux deux services d'échanger des informations classifiées.

Accès de la Trésorerie aux BDC

Il serait opportun que la Trésorerie dispose au plus vite de ses accès aux Banques de données communes (BDC).

Une boîte mail fonctionnelle pour le Service des Cultes et de la Laïcité

Il serait opportun que le Service des Cultes et de la Laïcité dispose d'une boîte mail fonctionnelle, laquelle permettrait de garantir un suivi de tous les échanges et documents par l'ensemble des membres de la cellule « terrorisme et radicalisme ».

Un accès aux BDC pour le Service des Cultes et de la Laïcité conforme au cadre légal

Il a été constaté que le Service des Cultes et de la Laïcité disposait d'un accès plus large à la Banque de données commune 'Propagandistes de haine' (BDC PH) que ce que prescrit l'AR PH. L'Organe de contrôle de l'information policière (C.O.C.) et le Comité permanent R ont invité les responsables du traitement à mettre un terme aux accès irréguliers et ont recommandé à la Police fédérale d'apporter les solutions techniques nécessaires pour mettre l'accès de ce service en conformité avec la législation en vigueur (soit accès indirect à la BDC PH uniquement). Le C.O.C. et le Comité permanent R ont recommandé par ailleurs aux responsables de traitement d'évaluer, sur les plans juridique et opérationnel, si la règlementation de l'accès du Service des Cultes et de la Laïcité devait (ou non) être révisée.

XI.2.2. APPLICATION CONFORME DE LA POSSIBILITÉ D'INTRODUIRE DES DEMANDES DE SCREENINGS DE SÉCURITÉ[388]

Le Comité invite les acteurs des secteurs publics et privés à examiner si certaines menaces potentielles ne peuvent pas être évitées en recourant, pour certaines fonctions, autorisations ou permis, au système de screening de sécurité prévu

[388] Voir Chapitre 'I.3. L'échange d'informations sur un collaborateur entre les services de renseignement et un employeur privé ou public'.

dans la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&H). Le Comité insiste toutefois sur un recours judicieux, donc non débridé, à ce système.

XI.2.3. SIGNALEMENT OBLIGATOIRE AUPRÈS DE L'EMPLOYEUR EN CAS DE REPRISE DANS UNE BANQUE DE DONNÉES COMMUNE[389]

Le Comité suggère d'examiner s'il serait utile de prévoir une notification obligatoire à l'employeur pour chaque collaborateur (ou candidat à un emploi) figurant dans la Banque de données commune Terrorist Fighters ou Prédicateurs de haine.

XI.2.4. UN DÉBAT ÉTENDU SUR LES TÂCHES ET PRIORITÉS DES SERVICES DE RENSEIGNEMENT[390]

Le Comité permanent R recommande qu'un débat sociétal (parlementaire) plus large soit mené sur les missions attribuées aux deux services de renseignement dans la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité ainsi que sur les priorités associées. Ceci nécessitera une discussion étayée scientifiquement, ou 'stratégiquement', car il n'y a actuellement pas de méthode scientifique à cet effet sur l'octroi des capacités et moyens suffisants pour permettre à chacun des services de détecter, suivre et maîtriser comme il se doit toutes les menaces contre la sécurité (inter)nationale. Les services de renseignement et de sécurité doivent retenir l'attention du Parlement, et ce pas uniquement au moment où des problèmes individuels surviennent (politique du chalumeau).

XI.2.5. PLUS DE SCREENINGS DE SÉCURITÉ DES MILITAIRES ET DES CIVILS À LA DÉFENSE[391]

Le Comité permanent R a constaté que, sauf à considérer que la carrière de l'intéressé impose une modification du niveau de sécurité, un militaire du département de la Défense ne subit qu'un seul screening de sécurité durant l'entièreté de sa carrière militaire. Pourtant, il apparaît que l'intégrité de certains

---

389 *Ibid.*

390 Voir Chapitres 'I.5. Le suivi des organisations sectaires nuisibles et des organisations criminelles par la Sûreté de l'État' et 'I.9. Enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings'. Un niveau de priorité très élevé a été attribué à cette recommandation.

391 Voir Chapitre 'I.7. Le screening de sécurité des militaires et des civils à la Défense'.

militaires peut effectivement poser problème sur la base de leurs activités entreprises ultérieurement notamment. Cela signifie que ces militaires ne seront connus comme tels que lorsqu'ils représenteront une menace qui aura été détectée par le SGRS.

Le Comité a relevé que les civils du département de la Défense, à de rares exceptions près, ne font l'objet d'aucune vérification de sécurité. Cette différence de traitement ne peut se justifier que si l'usage inapproprié de la fonction qu'ils occupent n'est pas susceptible de menacer les intérêts fondamentaux de l'État. Le Comité recommande par conséquent que l'autorité administrative compétente analyse si la possibilité créée par la Loi du 23 février 2018 de demander des vérifications de sécurité doit être activée. Cette loi permet après une analyse de risque, une analyse de la menace et une analyse d'impact de déteminer les fonctions pour lesquelles il est indiqué d'exiger un avis de sécurité.

La loi permet également qu'une telle évaluation soit effectuée tous les cinq ans et qu'un avis positif soit transformé en avis négatif dans l'intervalle. En ce sens, cette loi offre une possibilité intéressante qui ne s'applique pas actuellement au personnel militaire ; celui-ci ne peut être contrôlé qu'une seule fois (c'est-à-dire au moment de son recrutement). Il faut toutefois garder à l'esprit que l'actuel «avis négatif» pour les militaires implique une «décision négative» *de facto*, alors qu'en vertu de la loi de 2018, les conséquences d'un «avis négatif» reviennent à l'autorité qui a demandé l'avis.

Le Comité a constaté que les étudiants de l'École Royale Militaire (ERM) et d'autres écoles qui dépendent du département de la Défense, à l'inverse des militaires, et à quelques exceptions près, ne sont pas soumis à une vérification de sécurité lors de leur recrutement. Cette différence de traitement n'est pas justifiée et elle présente un risque pour le département de la Défense qui recrute du personnel sans avoir pu idéalement identifier les individus pouvant représenter une source de menace ou ne disposant pas des qualités morales nécessaires à l'exercice de leurs fonctions.

Le Comité a relevé que les étudiants étrangers de l'ERM ne sont pas soumis à une vérification de sécurité lors de leur admission. Cela devrait être précédé d'une analyse de risque systématique et préalable réalisée par le SGRS pour chaque candidat.

Ces recommandations devraient être appliquées à toutes les écoles qui dépendent du département de la Défense.

XI.2.6. LA MISE EN PLACE D'UN ENSEMBLE COHÉRENT 'RENSEIGNEMENT'[392]

Le Comité permanent R recommande la création d'un « ensemble cohérent renseignement » à la Défense reprenant l'entièreté des fonctions militaires de renseignement et permettant de former et de valoriser de manière continue le personnel qui s'y retrouve. Ceci doit permettre de disposer de personnel militaire de qualité et formé au SGRS. Cet ensemble doit disposer d'un maximum d'autonomie en matière de gestion et valorisation de son personnel. Cette recommandation est fondamentale et soulignée depuis de nombreuses années par le Comité.

XI.2.7. STABILITÉ DANS LA GESTION DU PERSONNEL AU SEIN DU SGRS

Le Comité permanent R recommande également d'instaurer une stabilité dans la mise en place de personnel militaire et d'éviter un 'turnover' beaucoup trop fréquent, tel que celui que l'on retrouve ailleurs à la Défense. Une stabilité de cinq ans doit être visée pour les fonctions clés.

XI.2.8. LA VALIDATION DU PLAN DIRECTEUR DU RENSEIGNEMENT (ET DE SÉCURITÉ)

Le Comité permanent R recommande que le Plan Directeur du Renseignement (et de Sécurité) soit validé sans délai. Et le Comité de recommander que ce Plan soit approuvé et évalué chaque année et qu'il soit soumis à l'approbation du ministre de la Défense. Ce plan stratégique définit, en fonction des obligations légales et des missions du SGRS, les moyens nécessaires à mettre en place et, en tenant compte de ceux-ci, les priorités accordées.

XI.2.9. UNE MEILLEURE COMMUNICATION INTERNE AU SGRS

Le Comité permanent R recommande que le SGRS communique mieux avec son personnel pour le familiariser davantage avec la structure et les flux d'informations qui s'y rapportent avant d'envisager des modifications. Il ne sert à rien de remettre

[392] Les recommandations reprises aux points XI.2.6 à XI.2.16. sont issues de l'enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings (Chapitre I.9.). Un niveau de priorité très élevé a été attribué à ces recommandations.

l'ensemble des réalisations en question, mais bien de veiller à l'ancrage de la nouvelle structure où cela s'avère nécessaire. Le Comité était néanmoins conscient que la période du Covid n'a pas facilité la communication en interne, pourtant primordiale pour le lancement d'une nouvelle structure.

XI.2.10. UNE MEILLEURE COMMUNICATION ENTRE LE SGRS ET LES AUTRES AUTORITÉS EN CAS D'INFRACTIONS JUDICIAIRES OU PÉNALES

Le Comité permanent R recommande d'évaluer les canaux et les procédures de communication, tant avec les autorités disciplinaires au sein de la Défense qu'avec les services de police et les autorités judiciaires. Le SGRS doit toujours être informé à temps des mesures administratives (les mises en observation, etc.), décisions (mises sous mandat d'arrêt, inculpations, etc.) et condamnations pénales relatives à un membre du personnel de la Défense. Ce genre de communication doit systématiquement avoir lieu afin que les mesures à prendre puissent être envisagées, plus précisément concernant les habilitations de sécurité.

XI.2.11. UNE MEILLEURE COMMUNICATION INTERNE DU SGRS VERS LE COMMANDEMENT ET LE MINISTRE DE LA DÉFENSE

Le Comité permanent R recommande que le SGRS établisse des directives internes précises quant au flux de communication d'informations vers le commandement et le ministre de la Défense. Ce flux d'informations doit être standardisé, précis et contenir les informations nécessaires à la prise de décision au plus haut niveau. Ceci est une condition *sine qua non* de contrôle adéquat du fonctionnement de l'organisation et fait partie de l'organisation et de la mise au point d'un système de contrôle interne.

XI.2.12. SUIVI ACTIF DE L'EXTRÉMISME AU SEIN DE LA DÉFENSE PAR LE SGRS

Le Comité permanent R recommande que le SGRS prenne les mesures qui s'imposent pour assurer une participation active aux Local Task Forces (LTF).

Le Comité recommande également que des directives soient établies et qu'une stratégie soit élaborée d'urgence sur le rôle du SGRS dans le cadre du Plan Radicalisme en ce qui concerne le suivi des militaires (de réserve) actifs. Il convient plus particulièrement de définir ce que doit être l'apport précis du SGRS, d'une

part dans le fonctionnement du groupe de travail national et des groupes de travail thématiques, et d'autre part, dans les LTF.

Le Comité permanent R recommande, en outre, que le SGRS déploie des ressources suffisantes pour la détection de l'extrémisme au sein de la Défense. Cela doit être le résultat d'une analyse préalable des ressources nécessaires pour chaque mission/menace.

Par ailleurs, le Comité recommande que le SGRS établisse des directives en rapport avec la consultation et l'alimentation de la Banque de données commune 'Terrorist fighters' (BDC TF) par ses collaborateurs.

XI.2.13. ÉVALUATION DU PLAN STRATÉGIQUE NATIONAL DU RENSEIGNEMENT (PSNR)

Le Comité permanent R invite les ministres de la Justice et de la Défense à procéder à l'évaluation du premier PSNR aux fins de voir renforcer les synergies entre les deux services au vu de ladite évaluation.

XI.2.14. DE MEILLEURES RÈGLES ET CONNAISSANCES SUR L'INTRODUCTION DES ENTITÉS DANS LES BANQUES DE DONNÉES COMMUNES (BDC)

Le Comité permanent R invite la ministre de la Défense à prendre les initiatives nécessaires avec les ministres compétents pour que les textes législatifs et/ou réglementaires établissent dorénavant les règles pour l'éventuelle inscription d'une entité dans la BDC TF ou l'attribution d'un certain niveau à un militaire par l'OCAM.

Le Comité permanent R invite la ministre de la Défense à solliciter les ministres compétents à la mise en œuvre par l'OCAM de recyclages réguliers de ses collaborateurs en la matière.

Le Comité permanent R recommande de revoir le Règlement IF5 qui doit être conforme à la structure et au matériel actuels de la Défense. L'IF5 revisité doit notamment décrire clairement les tâches de l'officier de sécurité et ses prérogatives. Il doit également formaliser les mesures et le contrôle des dépôts de munitions, notamment le rôle et les missions du SGRS.

XI.2.15. L'ÉCHANGE D'INFORMATIONS ENTRE SERVICES DE RENSEIGNEMENT CONCERNANT LE PERSONNEL DE LA DÉFENSE

Le Comité permanent R recommande que la VSSE informe systématiquement le SGRS lorsqu'elle possède des informations concernant le personnel (civil ou militaire) de la Défense. D'autre part, il apparaît nécessaire de voir les deux services conclure un accord de collaboration en matière de suivi du personnel de la Défense.

XI.2.16. RESPECT DES ACCORDS HUMINT[393]

Le Comité permanent R insiste sur le respect des accords conclus entre les services de renseignement en ce qui concerne le HUMINT, tel que repris dans le Plan Stratégique National du Renseignement.

XI.2.17. RESPECT DU TRANSFERT D'INFORMATIONS À L'OCAM

Le Comité permanent R recommande, comme le prévoit la L.OCAM, que les services de renseignement fournissent à l'OCAM, systématiquement et dans le respect des délais légaux, toute information pertinente pour l'analyse et l'évaluation de la menace.

XI.2.18. UNE POLITIQUE DE RECRUTEMENT FLEXIBLE ET PROACTIVE POUR LES SERVICES DE RENSEIGNEMENT

Le Comité permanent R recommande que les services de renseignement aient la possibilité de mener une politique de recrutement flexible et proactive. Ceci nécessite une meilleure collaboration avec le SELOR, mais également un renforcement du personnel nécessaire pour gérer le flux entrant de personnel civil prévu dans les années à venir.

---

393 Les recommandations reprises aux points XI.2.17 à XI.2.31. sont issues de l'enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings (Chapitre I.9.). Un niveau de priorité élevé a été attribué à ces recommandations.

XI.2.19. UN ENVIRONNEMENT DIGITAL DE QUALITÉ

Pour conserver le personnel, il faut par ailleurs que le SGRS dispose d'un environnement digital à la hauteur de ses obligations et missions. Le dernier rapport du Comité en la matière a montré l'insuffisance de l'infrastructure globale IT pour un service de cette importance.

XI.2.20. UNE MÉTHOLOGIE UNIFORME EN MATIÈRE D'ÉVALUATION DE LA MENACE DANS LE DOMAINE DU RENSEIGNEMENT

Le Comité permanent R recommande, afin d'améliorer la communication entre les différents partenaires du secteur du renseignement (VSSE et OCAM en particulier) que le SGRS s'aligne autant que possible sur la (ou les) méthodologie(s) déjà éprouvée(s) par ses partenaires, de manière telle qu'une même menace reçoive la même attention au sein de la communauté du renseignement.

Cette méthodologie doit comprendre une mise à jour des fiches individuelles à réaliser quant aux mesures de collecte de données à prévoir et quant aux actions à entreprendre auprès de l'objet de la menace.

L'ensemble de la 'watchlist' doit faire l'objet d'une réévaluation périodique au terme de laquelle les niveaux de menaces sont (ré)évalués et les menaces identifiées (dans les fiches individuelles) maintenues, revues à la hausse ou à la baisse, voire complètement écartées du système d'information lorsque l'analyse menée révèle que l'attention du SGRS n'est plus (ou pas) requise.

Le Comité permanent R recommande également que le principe de la 'watchlist' soit systématiquement 'implémenté' pour toutes les menaces de la compétence du SGRS, à savoir également celles qui ne nécessitent qu'un niveau minimal de suivi (suivi passif) mais en nécessite néanmoins un. Dès lors que la 'watchlist' comporte des niveaux de menace et les mesures de suivi à y réserver, il n'apparaît pas justifié de maintenir deux documentations distinctes : elle doit pouvoir donner une vision globale de la menace.

XI.2.21. L'IMPORTANCE DE DIVERS RÈGLEMENTS

Le Comité permanent R invite la ministre de la Défense à rappeler au ministre de la Justice la COL 8/2014, actualisée en janvier 2018, et à insister sur le respect systématique de cette circulaire.

Le Comité permanent R recommande d'harmoniser, de (ré)écrire et de centraliser les règles (SOP).

Le Comité permanent R recommande que le SGRS, et par extension la Défense, s'inscrivent dans le Plan R et collaborent dans un état d'esprit constructif.

XI.2.22. AUTORITÉ DISCIPLINAIRE SUR LE PERSONNEL CIVIL DE LA DÉFENSE

Le Comité permanent R recommande une nouvelle fois de remédier à la situation actuelle, le Chef du SGRS ne disposant pas de l'autorité disciplinaire sur le personnel civil du SGRS. Il faut absolument établir une unité de Commandement et non deux chaînes parallèles (une civile, une militaire), comme c'est le cas actuellement.

XI.2.23. UTILISATION DES MÉTHODES DE RECUEIL DE DONNÉES

Le Comité permanent R recommande d'utiliser au maximum les possibilités (Méthodes de recueil de données (MRD), HUMINT, etc.) prévues par les lois pour recueillir des informations, en collaboration avec la VSSE aux fins d'optimalisation.

XI.2.24. RECRUTEMENT DE JURISTES

Le Comité permanent R recommande de recruter davantage de juristes pour assurer une fonction juridico-opérationnelle en appui aux collaborateurs chargés de la collecte et des analystes.

XI.2.25. INVESTIR DANS LE MANAGEMENT

Le Comité permanent R recommande que le SGRS investisse dans une stratégie de 'knowledge management'.

Le Comité permanent R recommande de réformer le *Steering Committee* pour en faire un comité de direction à part entière et efficace, qui doit recevoir les moyens nécessaires pour se concentrer sur sa tâche de coordination et de synchronisation de toutes les activités de renseignement. Il devrait se voir supprimer la gestion des projets à moyen et long terme ainsi que son intervention dans la logistique de base. D'autres entités sont prévues au SGRS pour effectuer ces tâches, mais elles ne sont pas correctement effectuées par manque de personnel.

XI.2.26. CLARIFICATION DES MISSIONS DE COUNTERINTELLIGENCE AU SEIN DU SGRS

Le Comité permanent R recommande que le SGRS s'efforce encore de préciser les missions en matière de 'Counterintelligence' et de les faire connaître à tous les départements des Forces armées.

XI.2.27. FONCTIONNEMENT DES OFFICIERS DE SÉCURITÉ AU SEIN DU SGRS

Le Comité permanent R recommande que le SGRS conscientise davantage les officiers de sécurité (S2) sur l'ensemble des problèmes de sécurité qui peuvent se poser, les responsabilise et les exhorte à assurer une collaboration plus proactive entre les unités et le SGRS. Le SGRS doit quant à lui établir une relation de confiance avec les différents officiers de sécurité.

XI.2.28. IDENTIFICATION D'INDICATEURS DE RADICALISATION PAR LE SGRS

Le Comité permanent R recommande qu'en matière de détection de la radicalisation, le SGRS, épaulé par la Défense, donne des instructions précises afin d'identifier des indicateurs clairs de radicalisation.

XI.2.29. VISIBILITÉ DES ENTITÉS RESPECTIVES À SUIVRE PAR LA VSSE ET LE SGRS

Le Comité permanent R recommande de chercher une solution de type informatique (hit/no hit) pour permettre aux deux services de renseignement de prendre connaissance de leurs entités respectives à suivre, tout en respectant les finalités et le secret des sources propres à chacun des services.

XI.2.30. LES MOYENS POUR LA LUTTE CONTRE L'EXTRÉMISME

Le Comité permanent R recommande que le SGRS soit doté de moyens suffisants pour être en mesure de détecter l'extrémisme au sein de la Défense. Ceci doit

résulter d'une analyse préalable des moyens requis pour les différentes missions/ menaces.

XI.2.31. ACTUALISATION DE DIRECTIVES EXISTANTES[394]

Les directives du Comité ministériel du renseignement et de la sécurité portant sur toutes sortes de règles de sécurité (portée des enquêtes de sécurité, règles de classification, conservation des pièces classifiées, infosec, missions des officiers de sécurité) devraient être actualisées. Ces directives en question datent toutes de 2001.

Le Comité permanent R invite la ministre de la Défense à envisager, avec ses collègues compétents, d'établir une directive commune pour définir les critères légaux (Loi du 11 décembre 1998).

XI.2.32. CUMUL AU SEIN DE LA DÉFENSE

Le Comité permanent R recommande que la Défense puisse s'interroger sur la possibilité offerte aux militaires d'exercer une profession complémentaire dans le domaine de la 'sécurité privée' et sur la conformité de celle-ci avec la dignité de la fonction militaire.

XI.2.33. LE FONCTIONNEMENT DES BANQUE DE DONNÉES COMMUNES AU SEIN DU SGRS

Le Comité permanent R recommande que le SGRS informe son personnel de l'existence de la BDC TF et les sensibilise à son intérêt et à son utilisation. Il convient également d'établir des directives en rapport avec la consultation et l'alimentation de la BDC TF par le SGRS. De plus, un scénario doit être établi pour l'éventuelle inscription d'un militaire dans la BDC TF ou l'attribution d'un certain niveau de menace à un militaire par l'OCAM.

Le Comité permanent R recommande que les services de renseignement désignent des responsables pour consulter systématiquement et quotidiennement la BDC TF et, si nécessaire, partagent les informations avec la ligne hiérarchique jusqu'au plus haut niveau. En outre, le SGRS doit de toute urgence intégrer dans son fonctionnement la finalité (consultation, alimentation, etc.) des banques de

[394] Les recommandations reprises aux points XI.2.32 à XI.2.36. sont issues de l'enquête sur la détection et le suivi de la radicalisation d'un militaire de la Défense : l'affaire Jürgen Conings (Chapitre I.9.). Un niveau de priorité 'urgence moyenne' a été attribué à ces recommandations.

données communes. Par ailleurs, le SGRS doit systématiquement mettre à jour la liste des utilisateurs de la BDC TF.

XI.2.34. NOTIFICATION ET SUIVI DES INCIDENTS DE SÉCURITÉ AU SEIN DU SGRS

Le Comité permanent R recommande que le SGRS établisse un rapport détaillé de tout incident de sécurité. Ce rapport doit reprendre un examen et une analyse de toutes les dimensions (pas seulement techniques, mais aussi comportementales), et a fortiori si un des intéressés détient une habilitation de sécurité. Ce rapport doit être transmis aux autorités de sécurité compétentes, éventuellement avec une proposition de décision.

XI.2.35. COLLABORATION ENTRE LES BUREAUX DE SÉCURITÉ DU SGRS ET DE LA VSSE

Le Comité permanent R recommande que le bureau de sécurité de la VSSE et la Direction S du SGRS collaborent de manière plus étroite et plus formelle, en concluant un protocole d'accord.

XI.2.36. UTILISATION COHÉRENTE DES NIVEAUX DE LA MENACE ET COMMUNICATION DES ÉVALUATIONS PAR L'OCAM[395]

Lors de l'attribution d'un niveau de menace (1, 2, 3 ou 4), une catégorie pour le suivi (A, B ou C) est également accordée lors de l'enregistrement dans la BDC. Les deux paramètres sont indépendants. Les Comités permanents R et P recommandent une amélioration de la cohérence et de l'harmonisation entre le niveau de menace d'une part et la catégorie de suivi d'autre part.

En ce qui concerne le mode de communication et les destinataires des analyses de la menace de l'OCAM, il y a une différence selon qu'il s'agit d'une évaluation de la menace ponctuelle visant des personnes, des groupements ou des événements ou d'une évaluation de la menace individuelle par une personne. Les Comités permanents R et P recommandent, au niveau de la communication de l'évaluation de la menace par une personne, en plus de l'enregistrement dans la BDC, d'également communiquer cette analyse de la menace aux services intéressés

395 Voir Chapitre 'I.10. Le rôle de l'OCAM dans le suivi du militaire Jürgen Conings'. Pour rappel, cette enquête a été réalisée conjointement avec le Comité permanent P.

qui reçoivent les évaluations de la menace contre des personnes conformément à la L. OCAM.

En dépit du pragmatisme dont l'OCAM fait preuve lors de l'application de la Circulaire du ministre de l'Intérieur et du ministre de la Justice concernant l'échange d'informations à propos de Terrorist Fighters et de Propagandistes de haine et de leur suivi, les Comités permanents R et P ont relevé l'importance d'adapter la Circulaire aux nouvelles catégories ajoutées par l'arrêté de modification du 20/12/2019 à la BDC, à savoir les Extrémistes Potentiellement Violents (E.P.V.) et les Personnes Condamnées pour Terrorisme (P.C.T.).

En ligne avec la recommandation précédente, il pourrait être utile, dans le cadre d'une adaptation de la Circulaire des ministres de l'Intérieur et de la Justice concernant l'échange d'informations à propos de Terrorist Fighters et de Propagandistes de haine et de leur suivi, d'évaluer les possibilités d'étendre les mesures existantes de réduction de la menace et de les préciser pour les catégories existantes et nouvelles.

XI.2.37. COMMUNICATION ÉCRITE EN CAS D'APPLICATION DE L'ARTICLE 19 L.R&S[396]

L'article 19 L.R&S ne précise pas de quelle manière les renseignements doivent être communiqués aux ministres concernés et autres. Le Comité permanent R estime que la communication doit se faire par écrit, et ce pour des raisons de sécurité juridique, excepté en cas d'extrême urgence. L'objectif est d'éviter des discussions par la suite et de permettre un contrôle parlementaire (voire juridique). Le Comité recommande de mettre en œuvre sans délai le principe d'une communication écrite systématique.

XI.2.38. LE TRAITEMENT D'INFORMATIONS CLASSIFIÉES PAR DES TIERS[397]

Les destinataires d'information classifiées doivent être prudents avec de telles notes et être conscients des dommages qu'ils pourraient causer aux personnes qui font l'objet de ces notes ainsi qu'au bon fonctionnement des services de renseignement et de sécurité.

Le Comité permanent R invite la VSSE et l'Autorité nationale de sécurité (ANS) à prendre les initiatives nécessaires, dans un délai de six mois, afin de sensibiliser les destinataires et de rappeler les tâches qui incombent aux officiers de sécurité.

---

396 Voir Chapitre 'I.11. Le suivi d'un commissaire de gouvernement par la VSSE'.

397 *Ibid.*

XI.2.39. DES SCREENINGS DE SÉCURITÉ POUR DES FONCTIONS DE CONFIANCE[398]

Le Comité permanent R estime que l'exercice de certaines « fonctions publiques » requiert la vérification préalable de l'intégrité, de la loyauté et de la discrétion, comme l'exige la législation en vigueur dans certains pays européens.

Cette vérification devrait, selon le Comité, notamment être réalisée pour les candidats à la fonction de commissaire du gouvernement mais aussi à d'autres fonctions publiques comme celle d'aumônier, ou d'autres fonctions clés au niveau fédéral, régional et communautaire.

Par conséquent, le Comité permanent R invite le gouvernement à prendre les initiatives législatives pour la fin avril 2022 avec les ministres fédéraux compétents. Le ministre de la Défense est invité à préciser si des fonctions clés au sein de la Défense doivent être intégrée à ces initiatives. Dans le cas contraire, le ministre est invité à prendre les initiatives législatives parallèles nécessaires pour établir le cadre légal des vérifications pour les fonctions l'exigeant au sein de la Défense. Enfin, à l'initiative du ministre de la Justice, la question d'une vérification préalable de fonctions clés aux autres niveaux de pouvoir devrait également être mise à l'agenda d'une réunion du Comité de concertation.

XI.2.40. INDICATION DES DESTINATAIRES SUR LES NOTES SORTANTES[399]

Afin de limiter les fuites, le Comité permanent R recommande que la VSSE mentionne, dans les notes qu'elle rédige, l'ensemble des destinataires de celles-ci et 'individualise' lesdites notes lors de leur envoi.

Le Comité permanent R recommande qu'en règle générale les notes de la VSSE validées en Comité de direction soient transmises sans délai aux destinataires repris dans ces notes.

---

398 Voir Chapitres 'I.11. Le suivi d'un commissaire de gouvernement par la VSSE' & 'I.12. Le suivi des Frères musulmans et l'évaluation de la menace éventuelle que ceux-ci constituent en Belgique'.

399 Voir Chapitre 'I.11. Le suivi d'un commissaire de gouvernement par la VSSE.'

XI.2.41. COMMUNIQUER LES BESOINS DU CONSEIL NATIONAL DE SÉCURITÉ AUX SERVICES DE RENSEIGNEMENT[400]

Le Comité permanent R invite le Conseil national de sécurité (CNS) à préciser aux services de renseignement le type et la nature des notes qu'il souhaite recevoir ainsi que les délais d'envoi.

XI.2.42. COLLABORATION DANS LE CADRE DE LA PROBLÉMATIQUE DES FRÈRES MUSULMANS[401]

Le Comité permanent R est d'avis qu'il appartient aux ministres de la Justice et de la Défense de renforcer avec leurs collègues de l'Intérieur la coopération entre les services de renseignement et leurs partenaires (la Police fédérale, l'OCAM, etc.) et de déterminer, avec les services le cadre de coopération adéquat. Un plan d'action sur la problématique des Frères musulmans devra être mis en œuvre en 2022. Il aura :

- à définir de manière commune :
  - Le phénomène et ses éléments constitutifs ;
  - Le niveau de la menace constituée par celui-ci ;
  - Une stratégie de suivi du phénomène (avec une éventuelle répartition des tâches dans le respect du cadre légal)[402] tenant compte des moyens dont disposent les services ;
  - Une stratégie de sensibilisation des autorités et administrations (avec une répartition des compétences dans le respect du cadre légal).
- à établir une liste actualisée des associations liées aux Frères musulmans, des membres et sympathisants du mouvement ;
- à s'assurer que la capacité des effectifs est garantie pour en assurer le suivi adéquat.

---

400 *Ibid.*

401 Les recommandations reprises aux points XI.2.43 à XI.2.46. sont issues de l'enquête de contrôle 'Une attention renouvelée pour les Frères musulmans' (Chapitre I.12.).

402 Cet exercice a déjà été réalisé pour ce qui concerne le SGRS et la VSSE, et acté dans les plans stratégiques (voir *supra*).

XI.2.43. ANALYSE DES MOYENS DU SGRS DANS LE CADRE DE LA PROBLÉMATIQUE DES FRÈRES MUSULMANS

Le Comité permanent R recommande au SGRS de procéder en 2022 à une analyse pour déterminer si les moyens qu'il déploie pour le suivi des Frères musulmans sont suffisants au regard de la probabilité estimée du risque de tentative d'influence des Frères musulmans à l'égard de la Défense, et tenant compte de la priorité accordée au suivi du phénomène par le service. Dans le cas contraire, il appartient au SGRS d'inviter la ministre de la Défense à établir un plan de recrutement adéquat.

XI.2.44. SENSIBILISATION GÉNÉRALE DANS LE CADRE DE LA PROBLÉMATIQUE DES FRÈRES MUSULMANS

La Comité permanent R salue l'ambition de la VSSE de réaliser une brochure sur les Frères musulmans pour une diffusion large dans un but de sensibilisation et recommande à la VSSE de diffuser celle-ci au plus tard à la fin de l'année 2022.

XI.2.45. SENSIBILISATION DES OFFICIERS DE SÉCURITÉ DE LA DÉFENSE DANS LE CADRE DE LA PROBLÉMATIQUE DES FRÈRES MUSULMANS

Le Comité permanent R invite le SGRS à organiser des briefings internes pour les officiers de sécurité désignés afin de les sensibiliser à la problématique, et augmenter leur capacité de détection d'une menace concrète pour la Défense.

XI.2.46. L'ICT DANS LE PROCESSUS DU RENSEIGNEMENT AU SEIN DE LA DIRECTION CYBER DU SGRS[403]

Le Comité permanent R recommande de prendre en compte les points suivants en vue de garantir une efficacité optimale du service, et ce afin que celui-ci puisse remplir ses objectifs stratégiques :
- Effectuer les engagements nécessaires correspondants au plan de personnel, tel qu'il a été présenté au Comité permanent R ;
- Prendre des mesures complémentaires (*no-break*, UPS complémentaire, monitoring) afin de pallier les problèmes d'infrastructure électrique du quartier ;

[403] Voir Chapitre 'I.13. Les technologies de l'information et de la communication dans le processus de renseignement au sein de la Direction Cyber du SGRS et au sein de la VSSE'.

– Augmenter les ressources hardwares lorsque cela serait nécessaire afin de garantir une meilleure qualité de service rendu aux utilisateurs ;
– Porter une grande attention aux contrats avec des firmes externes, par exemple en envisageant des logiciels '*on premises*' (sur infrastructure propre).

XI.3. RECOMMANDATION RELATIVE À L'EFFICACITÉ DU CONTRÔLE

XI.3.1. SIGNALEMENT PAR LE SGRS DU SUIVI DES MANDATAIRES POLITIQUES[404]

Le Comité permanent R recommande au SGRS de lui remettre tous les trois mois un aperçu de tous les documents dans lesquels des mandataires politiques sont mentionnés, le cas échéant, avec une absence de « hit » si aucune mention de ce genre n'a été faite.

[404] Voir Chapitre 'I.8. Enquête de contrôle sur le suivi des mandataires politiques'.

ANNEXES

ANNEXE A
APERÇU DES PRINCIPALES RÉGLEMENTATIONS RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2021 AU 31 DÉCEMBRE 2021)

Loi du 27 juin 2021 contenant le troisième ajustement du budget général des dépenses pour l'année budgétaire 2021, *M.B.* 9 juillet 2021

Loi du 14 août 2021 modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et visant à élargir les conditions de nomination des greffiers du Comité R et du Comité P, *M.B.* 8 décembre 2021

Loi du 23 décembre 2021 contenant le budget général des dépenses pour l'année budgétaire 2022, *M.B.* 29 décembre 2021

A.R. 30 septembre 2021 fixant la liste des bénéficiaires des actions menées par le Service public fédéral Stratégique et Appui dans le cadre de sa mission de développement d'initiatives culturelles, promotionnelles, divertissantes, formatrices et sportives, *M.B.* 4 novembre 2021

Directive commune des ministres de la Justice et de l'Intérieur relative à la détermination des modalités de communication des données à caractère personnel et informations traitées dans le cadre de leurs missions de police administrative et judiciaire, telles que visées aux articles 14 et 15 de la loi sur la fonction de police, par les services de police et à l'accès direct et l'interrogation directe de la BNG, *M.B.* 2 février 2021

Appel aux candidats pour la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité, *M.B.* 12 février 2021

Par arrêté ministériel du 3 février 2021, le mandat de directeur d'encadrement de la Sûreté de l'État de Monsieur Hugues Brulin, est renouvelé pour une durée de 5 ans, à partir du 1er septembre 2020, *M.B.* 16 février 2021

Avis prescrit par l'article 3*quater* de l'arrêté du Régent du 23 août 1948 déterminant la procédure devant la section du contentieux administratif du Conseil d'État l'association sans but lucratif Syndicat de la Police Belge, "Sypol.be", a demandé l'annulation de l'arrêté royal du 24 septembre 2020 'modifiant l'arrêté royal du 13 décembre 2006 portant le statut des agents des services extérieurs de la Sûreté de l'État', *M.B.* 16 février 2021

Directeur de l'Organe de coordination pour l'analyse de la menace, fin de la désignation, *M.B.* 24 février 2021

Directeur de l'Organe de coordination pour l'analyse de la menace, désignation ad interim, *M.B.* 24 février 2021

Comité permanent de contrôle des services de renseignements et de sécurité, poste vacant pour un attaché francophone (m/f/x) de niveau universitaire, *M.B.* 5 mars 2021

Recrutement, par détachement, et constitution d'une réserve de recrutement de commissaires-auditeurs francophones (m/f/x), dotés de connaissances particulières en gestion des enquêtes judiciaires et en gestion de l'information (Intelligence-led Policing), pour le Service d'Enquêtes du Comité permanent R, *M.B.* 18 mars 2021

Appel aux candidats pour la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité, *M.B.* 2 avril 2021

Nomination du greffier du Comité permanent de contrôle des services de renseignement (Comité R), *M.B.* 19 juillet 2021

Cour Constitutionnelle : extrait de l'arrêt n° 64/2021 du 22 avril 2021, n° du rôle : 7416, en cause : la question préjudicielle relative à l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, posée par le Comité permanent de contrôle des services de renseignement et de sécurité, *M.B.* 20 septembre 2021

Recrutement, par détachement, et constitution d'une réserve de recrutement de commissaires-auditeurs francophones (m/f/x), dotés de connaissances particulières en ICT/Data, pour le Service d'Enquêtes du Comité permanent R, *M.B.* 1er octobre 2021

Cour Constitutionnelle : extrait de l'arrêt n° 107/2021 du 15 juillet 2021, n° du rôle : 7261, en cause : le recours en annulation de la loi du 23 mars 2019 'concernant l'organisation des services pénitentiaires et le statut du personnel pénitentiaire', introduit par Michel Jacobs, *M.B.* 6 octobre 2021

Appel à candidats pour le mandat de second membre suppléant néerlandophone du Comité permanent de contrôle des services de renseignement (Comité R), *M.B.* 25 novembre 2021

Recrutement, par détachement, et constitution d'une réserve de recrutement de commissaires-auditeurs francophones (m/f/x), dotés de connaissances particulières en ICT/Data, pour le Service d'Enquêtes du Comité permanent R, *M.B.* 23 décembre 2021

Sélection comparatives, épreuves préalables des sélections comparatives et résultats des sélections comparatives de :

- HR Business Partners pour le service de renseignement militaire (m/f/x) (niveau A1), néerlandophones, pour le Ministère de la Défense, n° de sélection : ANG21132, *M.B.* 17 mai 2021
- HR Business Partners pour le service de renseignement militaire (m/f/x) (niveau A1), francophones, pour le Ministère de la Défense, n° de sélection : ANG21132, *M.B.* 17 mai 2021
- Data Officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21100, *M.B.* 1er juin 2021
- Data Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21130, *M.B.* 1er juin 2021
- Technical Officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État. - n° de sélection : AFG21102, *M.B.* 1er juin 2021
- Technical Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État. - n° de sélection : ANG21134, *M.B.* 1er juin 2021
- Administrateurs système Windows/Linux (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21119, *M.B.* 13 juillet 2021
- Gestionnaires de réseaux (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21153, *M.B.* 13 juillet 2021
- Collaborateurs Imagery Intelligence pour le Service général du Renseignement et de Sécurité (SGRS) (m/f/x) (niveau B), néerlandophones, pour le Ministère de la Défense, n° de sélection : ANG21216, *M.B.* 16 juillet 2021
- Documentalistes renseignement et sécurité (m/f/x) (niveau B) néerlandophones, pour le Ministère de la Défense, n° de sélection : ANG21218, *M.B.* 26 juillet 2021

- Spécialistes Query & Reporting (m/f/x) (niveau A1), francophones, pour le Ministère de la Défense, n° de sélection : AFG21134, *M.B.* 6 août 2021
- Attachés analyste habilitation de sécurité (m/f/x) (niveau A), francophones, pour le Ministère de la Défense, n° de sélection : AFG21135, *M.B.* 6 août 2021
- Chercheur en cyber défense A2 (m/f/x) (niveau A2), francophones, pour le Ministère de la Défense, n° de sélection : AFG21156, *M.B.* 16 août 2021
- Inspecteurs francophones pour les services extérieurs (m/f/x) (niveau B) de la Sûreté de l'État, n° de sélection : AFG21149, *M.B.* 29 septembre 2021
- Inspecteurs néerlandophones pour les services extérieurs (m/f/x) (niveau B) de la Sûreté de l'État, n° de sélection : AFG21212, *M.B.* 29 septembre 2021
- Finance Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21303, *M.B.* 30 septembre 2021
- Technical Officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21102, *M.B.* 26 octobre 2021
- Administrateurs système Windows/Linux (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21119, *M.B.* 26 octobre 2021
- Technical Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21134, *M.B.* 26 octobre 2021
- Gestionnaires de réseaux(m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21153, *M.B.* 26 octobre 2021
- Attachés analystes habilitation de sécurité (m/f/x) (niveau A1) francophones pour le Ministère de la Défense, n° de sélection : AFG21135, *M.B.* 17 novembre 2021
- Néerlandophones d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État, n^{os} de sélection : BNG21341 et BNG21342, *M.B.* 8 décembre 2021
- francophones d'accession au niveau B (épreuve particulière) pour la Sûreté de l'État, n^{os} de sélection : BFG21188 et BFG21189, *M.B.* 8 décembre 2021
- Data Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21130, *M.B.* 16 décembre 2021
- Data Officers (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21100, *M.B.* 16 décembre 2021
- Finance Officers (m/f/x) (niveau B), néerlandophones, pour la Sûreté de l'État, n° de sélection : ANG21303, *M.B.* 27 décembre 2021
- Inspecteurs pour les services extérieurs (m/f/x) (niveau B), francophones, pour la Sûreté de l'État, n° de sélection : AFG21149, *M.B.* 30 décembre 2021
- Inspecteurs néerlandophones pour les services extérieurs (m/f/x) (niveau B) de la Sûreté de l'État, n° de sélection : ANG21212, *M.B.* 30 décembre 2021

ANNEXE B
APERÇU DES PRINCIPALES PROPOSITIONS DE LOIS, DES PROJETS DE LOIS, DES RÉSOLUTIONS, MOTIONS D'ORDRE ET DES DÉBATS PARLEMENTAIRES RELATIFS AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2021 AU 31 DÉCEMBRE 2021)

Sénat

Rapport d'information concernant la nécessaire collaboration entre l'autorité fédérale et les Communautés en matière de lutte contre les infox (fake news) de S. D'Hose, E. Ampe, R. Daems, W.-F. Schiltz, C. Van Cauter, F. Ahallouch, L. Gahouchi, G.-L. Bouchez, Ph. Dodrimont, V. Durenne, S. Laruelle, A. Miesen, G. Van Goidsenhoven, J.-P. Wahl, K. Brouwers, B. Anciaux, K. De Loor, A. Lambrecht, K. Segers, A. Antoine, A.-C. Goffinet, F. Ben Chikha, S. Bex, R. Demeuse, S. Hoessen, F. Masai, J. Pitseys, H. Ryckmans, Ch. Steenwegen et F. Tahar, Doc. 7-110, *Ann. Parl.*, Sénat, 2021-2022, 17 novembre 2021, n° 6-24, p. 5

Cour constitutionnelle, arrêt n° 158/2021, rendu le 18 novembre 2021, en cause le recours en annulation de la loi du 1er septembre 2016 portant modification de l'article 127 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 16/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, introduit par P. Van Assche et autres (n° du rôle 6672), *Ann. Parl.*, Sénat, 2021-2022, 17 décembre 2021, n° 6-25, p. 43

Chambre des représentants

Commissions, comités d'avis et délégations aux assemblées internationales, Doc. parl., Chambre, 2020-2021, n° 55-8/8

Motions déposées le 17 mars 2021 en réunion publique de commission (Articles 133 à 141 du Règlement de la Chambre) en conclusion de l'interpellation de N. Boukili au Premier ministre sur 'Smals et les marchés publics relatifs à la digitalisation du service public', Doc. parl., Chambre, 2020-2021, n° 55-105/1

Proposition de résolution visant à prévoir dans le plan de retrait de l'Operation Vigilant Guardian (OVG) des moyens équivalents pour les sites présentant un niveau 3 de la menace, Doc. parl., Chambre, 2020-2021, n° 55-1413/2

Proposition de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en vue de l'instauration d'une obligation de notification active pour certaines méthodes spécifiques de collecte de données, Doc. parl., Chambre, 2020-2021, nº 55-1763/1

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du premier suppléant d'un membre francophone – candidatures introduites, *C.R.I.*, Chambre, 2020-2021, 28 janvier 2021, PLEN 85, p. 38

Proposition de résolution relative à la cyberdéfense et à l'attribution des cyberattaques étatiques, Doc. parl., Chambre, 2020-2021, nº 55-1788/1

Cour des comptes, Cour constitutionnelle, Conseil supérieur de la Justice, Comité permanent de contrôle des services de police, Comité permanent de contrôle des services de renseignements et de sécurité, Médiateurs fédéraux, Autorité de protection des données, Commissions de nomination pour le notariat, Commission BIM, Organe de contrôle de l'information policière, Commission fédérale de déontologie, Conseil central de surveillance pénitentiaire, Institut des droits humains - audit de suivi de la

Cour des comptes - mise en œuvre des recommandations, Doc. parl., Chambre, 2020-2021, nº 55-1924/1

Motion d'ordre déposée par P. De Roover, P. Buysrogge et J. Donné : 'La Chambre des représentants, - considérant que des informations provenant d'un échange de vues au sujet d'une future enquête de contrôle ont été divulguées aux médias par des membres de la commission d'accompagnement parlementaire du Comité P & R; - considérant que la commission d'accompagnement entre dans le champ d'application de l'art. 67 du Règlement de la Chambre et que l'obligation de secret s'applique à l'égard de toutes les informations obtenues dans le cadre des réunions; demande à la présidente de la Chambre de mener une enquête sur les auteurs des infractions, pour ensuite prendre les sanctions appropriées en application de l'art. 67 du Règlement de la Chambre', *C.R.I.*, Chambre, 2020-2021, 27 mai 2021, PLEN 106, p. 26

Communication relative au respect de l'article 67 du Règlement, *C.R.I.*, Chambre, 2020-2021, 27 mai 2021, PLEN 106, p. 27

Projet de loi contenant le premier ajustement du budget des Voies et Moyens de l'année budgétaire 2021 (1920/1-8), projet de loi contenant le troisième ajustement du budget général des dépenses pour l'année budgétaire 2021 (1921/1-27), ajustement des budgets des recettes et des dépenses pour l'année budgétaire 2021. Exposé général (1919/1), *C.R.I.*, Chambre, 2020-2021, 24 juin 2021, PLEN 113, p. 1

Proposition de loi modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et visant à élargir les conditions de nomination des greffiers du Comité R et du Comité P (2064/1-3), *C.R.I.*, Chambre, 2020-2021, 8 juillet 2021, PLEN 117, p. 51

Motion déposée par P. De Roover : 'réquisition de la présence du Premier ministre – art. 100 de la Constitution et art. 50 du règlement eu égard aux déclarations du Premier ministre ce lundi en commission de la santé relatives à l'enquête de la Sûreté de l'État sur l'ancienne commissaire du gouvernement pour l'Institut pour l'égalité des femmes et des hommes et à la transmission au cabinet du ministre de la Justice des résultats de celle-ci, *C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, PLEN 119, p. 2

Comité permanent de contrôle des services de renseignements et de sécurité, remplacement du greffier, appel aux candidats, *C.R.I.*, Chambre, 2020-2021, 15 juillet 2021, PLEN 122, p. 44

Proposition de rejet par la commission de l'Intérieur, de la Sécurité, de la Migration et des Matières administratives de la proposition de résolution visant à prévoir dans le plan de retrait de l'Operation Vigilant Guardian (OVG) des moyens équivalents pour les sites présentant un niveau 3 de la menace (1413/1-2), *C.R.I.*, Chambre, 2020-2021, 15 juillet 2021, PLEN 122, p. 62

Proposition de résolution relative à la cyberdéfense et à l'attribution des cyberattaques étatiques, Doc. parl., Chambre, 2020-2021, nº 55-1788/1

Projet de loi modifiant la loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace et visant à élargir les conditions de nomination des greffiers du Comité R et du Comité P, Doc. parl., Chambre, 2020-2021, nos 55-2064/1 à 55-2064/4

Projet de loi portant assentiment à l'accord entre le Royaume de Belgique et le Royaume d'Espagne sur l'échange et la protection mutuelle des informations classifiées, fait à Bruxelles le 15 octobre 2015, Doc. parl., Chambre, 2020-2021, nos 55-2074/1 à 55-2074/3

Projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la République de Finlande concernant la protection réciproque des informations classifiées, fait à Helsinki le 20 juillet 2016, Doc. parl., Chambre, 2020-2021, nº 55-2075/1

Projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la République de Chypre sur la protection mutuelle des informations classifiées, fait à Bruxelles le 20 juillet 2015, Doc. parl., Chambre, 2020-2021, nº 55-2085/1

Projet de loi portant assentiment à l'accord entre le Royaume de Belgique et la Hongrie sur l'échange et la protection mutuelle des informations classifiées, fait à Budapest le 21 septembre 2015, Doc. parl., Chambre, 2020-2021, nº 55-2121/1

Actualisation de la vision stratégique, échange de vues avec la ministre de la Défense, Doc. parl., Chambre, 2020-2021, nº 55-2150/1

Proposition de résolution relative à la protection de notre sécurité nationale et de notre indépendance stratégique contre les cyberattaques étrangères grâce à l'établissement d'une liste de fournisseurs à haut risque, Doc. parl., Chambre, 2020-2021, nº 55-2167/1

Cyberattaques menées contre les systèmes IT de l'état et des services publics, Doc. parl., Chambre, 2020-2021, nº 55-2169/1

Comité permanent de contrôle des services de renseignements et de sécurité – nomination du greffier – candidatures introduites, *C.R.I.*, Chambre, 2020-2021, 23 septembre 2021, PLEN 125, p. 27

Comité permanent de contrôle des services de police – nomination du greffier – candidatures introduites, *C.R.I.*, Chambre, 2020-2021, 23 septembre 2021, PLEN 125, p. 29

Affaire Jürgen Conings, Doc. parl., Chambre, 2020-2021, nº 55-2206/1

Rapport d'activités 2020 du Comité permanent de contrôle des services de renseignement et de sécurité, Doc. parl., Chambre, 2021-2022, nº 55-2209/1

Proposition de résolution relative à l'indépendance et au fonctionnement de l'Autorité de protection des données, Doc. parl., Chambre, 2021-2022, nº 55-2246/1

Projet de loi portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques, Doc. parl., Chambre, 2021-2022, nºs 55-2256/1, 55-2256/7 et 55-2256/8

Projet de loi modifiant la loi du 13 juin 2005 relative aux communications électroniques, Doc. parl., Chambre, 2021-2022, nºs 55-2257/1 à 55-2257/4

Les révélations dans la presse concernant le rôle des banques dans le blanchiment de l'argent (FINCEN FILES), Doc. parl., Chambre, 2021-2022, nº 55-2261/1

Projet de loi contenant le budget des Voies et Moyens pour l'année budgétaire 2022, Doc. parl., Chambre, 2021-2022, nº 55-2291/1

Projet de loi contenant le budget général des dépenses pour l'année budgétaire 2022, Doc. parl., Chambre, 2021-2022, nºs 55-2292/1 et 55-2292/6

Justification du budget général des dépenses pour l'année budgétaire 2022, Doc. parl., Chambre, 2021-2022, nºs 55-2293/6 et 55-2293/7

Note de politique générale, Doc. parl., Chambre, 2021-2022, nºs 55-2294/2, 55-2294/8, 55-2294/14, 55-2294/16, 55-2294/17, 55-2294/18 et 55-2294/22

Projet de loi modifiant diverses dispositions relatives au passage au sein de la même catégorie de personnel ou à l'admission dans une autre qualité ou catégorie de personnel du militaire de carrière ou du militaire avec une carrière à durée limitée, Doc. parl., Chambre, 2021-2022, nº 55-2302/1

Comité R – démission du second suppléant du membre néerlandophone, *C.R.I.*, Chambre, 2021-2022, 10 novembre 2021, PLEN 139, p. 68

Cour des comptes, Cour constitutionnelle, Conseil supérieur de la Justice, Comité permanent de contrôle des services de police, Comité permanent de contrôle des services de renseignement et de sécurité, Médiateurs fédéraux, Autorité de protection des données, Commissions de nomination pour le notariat, Commission BIM, Organe de contrôle de l'information policière, Commission fédérale de déontologie, Conseil central de surveillance pénitentiaire, Institut fédéral des droits humains, travaux des groupes de travail dans le cadre du projet de synergie, comptes de l'année budgétaire

2020, ajustements budgétaires de l'année budgétaire 2021, propositions budgétaires pour l'année budgétaire 2022, Doc. parl., Chambre, 2021-2022, nos 55-2368/1 à 55-2368/3, *C.R.I.*, Chambre, 2021-2022, 22 décembre 2021, PLEN 152, p. 27 et *C.R.I.*, Chambre, 2021-2022, 22 décembre 2021, PLEN 154, p. 17

Proposition de loi modifiant la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, en vue de soumettre les fournisseurs de services essentiels du service public qui dépendent des réseaux et des systèmes d'information à certaines exigences en matière de sécurité et de notification, Doc. parl., Chambre, 2021-2022, nos 55-2401/1

ANNEXE C
APERÇU DES INTERPELLATIONS, DES DEMANDES D'EXPLICATIONS ET DES QUESTIONS ORALES ET ÉCRITES RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2021 AU 31 DÉCEMBRE 2021)

Sénat

Question écrite de G. D'haeseleer au ministre de la Justice sur les 'personnes condamnées pour terrorisme - nombre - motifs - nationalité' (Sénat, 2020-2021, 3 mars 2021, Q. no 7-1107)

Question écrite de T. Ongena au ministre de la Justice sur la 'Turquie - salafisme - ingérence d'états étrangers - chiffres et tendances' (Sénat, 2020-2021, 5 mars 2021, Q. no 7-1140)

Question écrite de T. Ongena à la ministre de l'Intérieur sur la 'Turquie - salafisme - ingérence d'États étrangers - chiffres et tendances' (Sénat, 2020-2021, 5 mars 2021, Q. no 7-1141)

Question écrite de R. Daems au ministre de la Justice sur les 'médias sociaux - confidentialité en ligne - cryptage - Sûreté de l'État - chiffres et tendances - mesures possibles' (Sénat, 2020-2021, 31 mars 2021, Q. no 7-1154)

Question écrite d'A. Frédéric au ministre de la Justice sur les 'sectes - nouvelles pratiques - lutte - évolution de la législation - moyens institutionnels, financiers et humains - renforcement - crise de la Covid-19 - impact - évaluation' (Sénat, 2020-2021, 28 avril 2021, Q. no 7-1219)

Question écrite de R. Daems au ministre de la Justice sur 'l'écologie - climat - réduction des émissions - objectifs – respect des promesses – 'espionnage vert' - contrôle par les pays tiers et des pays tiers - Sûreté de l'État - participation' (Sénat, 2020-2021, 3 mai 2021, Q. no 7-1227)

Question écrite de T. Ongena au ministre de la Justice sur la 'Turquie - mouvement Gülen - crimes de haine en Belgique - protection policière - incidents - chiffres et tendances - communauté turque - protection - mesures' (Sénat, 2020-2021, 3 mai 2021, Q. no 7-1229)

Question écrite de T. Ongena à la ministre de l'Intérieur sur 'l'extrême droite - sociétés de gardiennage et de sécurité - infiltration - chiffres et tendances' (Sénat, 2020-2021, 21 mai 2021, Q. no 7-1248)

Question écrite de T. Ongena au ministre de la Justice sur 'l'extrême droite - risque d'attentats - concertation - violence - Coronavirus - forums de discussion en ligne (Covid-19)' (Sénat, 2020-2021, 21 mai 2021, Q. no 7-1249)

Question écrite de T. Ongena à la ministre de l'Intérieur sur les 'cyberattaques - cybersécurité - chiffres et tendances - auteurs - acteurs étatiques - vie privée - protection - mesures' (Sénat, 2020-2021, 22 juillet 2021, Q. nº 7-1311)

Question écrite d'A. Miesen à la ministre de la Défense sur les 'Militärdienste - Reform der Nachrichtendienste - Extremismusbekämpfung Services de la Défense - réforme des services de renseignement - lutte contre l'extrémisme' (Sénat, 2020-2021, 24 août 2021, Q. nº 7-1322)

Question écrite d'E. Ampe au ministre de la Justice sur les 'smartphones - acteurs étatiques - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1385)

Question écrite d'E. Ampe à la ministre de l'Intérieur sur les 'smartphones - acteurs étatiques - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1386)

Question écrite d'E. Ampe au ministre de la Justice sur les 'smartphones - logiciels de harcèlement - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1387)

Question écrite d'E. Ampe à la ministre de l'Intérieur sur les 'smartphones - logiciels de harcèlement - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1388)

Question écrite de R. Daems au ministre de la Justice sur la 'cryptographie - ordinateurs quantiques - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1391)

Question écrite de R. Daems à la ministre de l'Intérieur sur la 'cryptographie - ordinateurs quantiques - vie privée - espionnage - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1392)

Question écrite de T. Ongena à la ministre de la Défense sur les 'drones - police - espionnage - acteurs étrangers - vie privée - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1395)

Question écrite de T. Ongena à la ministre de l'Intérieur sur les 'drones - police - espionnage - acteurs étrangers - vie privée - chiffres et tendances' (Sénat, 2021-2022, 27 octobre 2021, Q. nº 7-1396)

Chambre des représentants

Question de S. Moutquin au secrétaire d'État à l'Asile et la Migration sur 'la forte croissance du nombre de screenings de sécurité effectuée à la demande de l'OE et du CGRA' (*C.R.I.*, Chambre, 2020-2021, 6 janvier 2021, COM 322, p. 16, Q. nº 11488C)

Interpellation et questions jointes de D. Van Langenhove, K. Metsu et Ph. Pivin au ministre de la Justice sur 'l'avis négatif de la Justice concernant la reprise des activités à la Grande Mosquée de Bruxelles' (*C.R.I.*, Chambre, 2020-2021, 6 janvier 2021, COM 324, p. 1, Q. nºs 58I, 11916C et 12037C)

Question de Th. Francken au ministre de la Justice sur 'l'arrêté de subvention pour l'Exécutif des Musulmans' (*C.R.I.*, Chambre, 2020-2021, 6 janvier 2021, COM 324, p. 36, Q. nº 11948C)

Question de D. Safai au secrétaire d'État à l'Asile et la Migration sur 'le suivi et le contrôle des illégaux radicalisés et des réfugiés reconnus radicalisés en Belgique' (*Q.R.*, Chambre, 2020-2021, 12 janvier 2021, nº 34, p. 151, Q. nº 59)

Question d'E. Burton à la ministre de l'Intérieur sur 'l'arrestation d'un radicalisé devant le commissariat de Bruxelles' (*Q.R.*, Chambre, 2020-2021, 12 janvier 2021, nº 34, p. 394, Q. nº 110)

Question de T. Vandenput à la ministre de l'Intérieur sur 'la mise à jour de la base de données de l'OCAM' (*Q.R.*, Chambre, 2020-2021, 12 janvier 2021, nº 34, p. 408, Q. nº 119)

Question et interpellation jointes de S. De Wit et M. Dillen au ministre de la Justice 'le gardien grièvement blessé à la prison de Gand' (*C.R.I.*, Chambre, 2020-2021, 13 janvier 2021, COM 334, p. 14, Q. nos 12064C et 75I)

Question de K. Metsu à la ministre de l'Intérieur sur 'la lutte contre l'extrémisme violent' (*C.R.I.*, Chambre, 2020-2021, 13 janvier 2021, COM 336, p. 49, Q. nº 11874C)

Question d'E. Samyn à la ministre des Affaires étrangères sur 'le rapport des Nations Unies sur le risque de nouvelles campagnes de terreur de l'EI en Europe' (*Q.R.*, Chambre, 2020-2021, 18 janvier 2021, nº 35, p. 91, Q. nº 117)

Question de J. Pillen à la ministre de la Défense sur le 'port de l'uniforme par des militaires' (*Q.R.*, Chambre, 2020-2021, 18 janvier 2021, nº 35, p. 297, Q. nº 83)

Question de K. Jadin à la ministre de l'Intérieur sur 'les interpellations pour menace de personnalités publiques' (*Q.R.*, Chambre, 2020-2021, 18 janvier 2021, nº 35, p. 405, Q. nº 171)

Débat d'actualité et questions jointes de B. Segers, H. Rigot, S. Moutquin, T. Vandenput et G. Daems au secrétaire d'État à l'Asile et la Migration sur 'l'affaire Kucam' (*C.R.I.*, Chambre, 2020-2021, 19 janvier 2021, COM 337, p. 1, Q. nos 12673C, 12674C, 12721C, 12723C, 12735C et 12756C)

Question de Th. Francken au secrétaire d'État à l'Asile et la Migration sur 'le renvoi des extrémistes' (*C.R.I.*, Chambre, 2020-2021, 19 janvier 2021, COM 337, p. 18, Q. nº 12073C)

Question de K. Jadin au ministre de la Justice sur 'l'extrême droite en Belgique' (*C.R.I.*, Chambre, 2020-2021, 21 janvier 2021, PLEN 084, p. 42, Q. nº 1286P)

Question de J. Pillen à la ministre de la Défense sur 'les intrusions sur les domaines militaires' (*Q.R.*, Chambre, 2020-2021, 27 janvier 2021, nº 36, p. 349, Q. nº 80)

Question d'A. Ponthier à la ministre de la Défense sur 'la fraude téléphonique depuis la Syrie' (*Q.R.*, Chambre, 2020-2021, 27 janvier 2021, nº 36, p. 352, Q. nº 92)

Question de J. Pillen à la ministre de la Défense sur les 'appels téléphoniques suspects' (*Q.R.*, Chambre, 2020-2021, 27 janvier 2021, nº 36, p. 356, Q. nº 98)

Questions jointes de B. Moyaers, P. Pivin, S. Matheï et K. Van Vaerenbergh au ministre de la Justice sur 'les appels aux émeutes en Belgique diffusés par les médias sociaux' (*C.R.I.*, Chambre, 2020-2021, 28 janvier 2021, PLEN 85, p. 2, Q. nos 1303P, 1311P,1312P et 1315P)

Question de M. Freilich à la ministre de la Fonction publique sur 'la campagne d'intimidation de Huawei contre le gouvernement belge' (*C.R.I.*, Chambre, 2020-2021, 24 février 2021, COM 387, p. 6, Q. nº 12479C)

Question de Th. Francken, D. Ducarme et G. Dallemagne au ministre de la Justice sur 'le CCIF en Belgique' (*C.R.I.*, Chambre, 2020-2021, 24 février 2021, COM 389, p. 17, Q. nos 14172C, 14331C et 14455C)

Question de L. Dierick au ministre de la Justice sur 'les délais de paiement au SPF Justice' (*Q.R.*, Chambre, 2020-2021, 4 mars 2021, nº 41, p. 167, Q. nº 289)

Question de J.-M. Delizée au ministre de la Justice sur 'la déclassification des archives dites africaines' (*Q.R.*, Chambre, 2020-2021, 4 mars 2021, nº 41, p. 178, Q. nº 369)

Débat d'actualité et questions jointes d'H. Rigot, B. Segers, P. De Roover, S. Moutquin, G. Daems et E. Platteau au secrétaire d'État à l'Asile et la Migration sur 'les nouveaux soupçons de trafic de visas humanitaires' (*C.R.I.*, Chambre, 2020-2021, 9 mars 2021, COM 397, p. 1, Q. nos 14898C, 14920C, 15041C, 15045C, 15067C et 15086C)

Débat d'actualité et questions jointes de Th. Francken, J. Pillen, A. Ponthier, H. Bayet, G. Defossé et K. Verduyckt à la ministre de la Défense sur 'l'amélioration des conditions des

militaires' (*C.R.I.*, Chambre, 2020-2021, 10 mars 2021, COM 402, p. 1, Q. nos 12466C, 13889C, 14028C, 14251C, 14265C, 15097C, 15109C et 15144C)

Question d'E. Van Hoof à la ministre des Affaires étrangères sur 'les déclarations du diplomate iranien traduit en justice' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 115, Q. no 60)

Question de W. Vermeersch au ministre des Finances sur la 'douane - la préoccupation croissante suscitée par les scanneurs chinois' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 205, Q. no 230)

Question de M. Freilich au ministre des Finances sur 'Nuctech - scanners chinois' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 208, Q. no 231)

Question de K. Metsu au ministre de la Justice sur les 'perquisitions dans le cadre de l'enquête sur le financement des groupes terroristes' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 288, Q. no 368)

Question d'A. Ponthier à la ministre de la Défense sur 'la coopération entre des universités belges et les Seven Sons of National Defence en Chine' (*Q.R.*, Chambre, 2020-2021, 11 mars 2021, no 42, p. 304, Q. no 124)

Questions jointes de B. Segers, F. Demon et K. Gabriëls au ministre de la Justice sur 'l'opération Sky' (*C.R.I.*, Chambre, 2020-2021, 11 mars 2021, PLEN 91, p. 24, Q. nos 1428P, 1431P et 1430P)

Questions jointes de K. Aouasti, N. Gilson, N. Boukili, G. Dallemagne et G. Vanden Burre au ministre de la Digitalisation sur 'le respect de la vie privée et le projet 'Putting data at the center" (*C.R.I.*, Chambre, 2020-2021, 11 mars 2021, PLEN 91, p. 35, Q. nos 1427P, 1435P, 1438P, 1445P et 1449P)

Question de S. Van Hecke au ministre de la Justice sur 'le suivi des organisations sectaires dans le cadre de la crise du coronavirus' (*Q.R.*, Chambre, 2020-2021, 17 mars 2021, no 43, p. 218, Q. no 381)

Question de S. Goethals à la ministre de l'Intérieur sur les 'organes relevant de vos compétences' (*Q.R.*, Chambre, 2020-2021, 17 mars 2021, no 43, p. 269, Q. no 313)

Question de Ph. Pivin à la ministre de l'Intérieur sur les 'mesures de protection des enseignants - menace radicalisme et terrorisme' (*Q.R.*, Chambre, 2020-2021, 17 mars 2021, no 43, p. 279, Q. no 318)

lnterpellation de N. Boukili au Premier ministre sur 'Smals et les marchés publies relatifs à la digitalisation du service public' (*C.R.I.*, Chambre, 2020-2021, 17 mars 2021, COM 411, p. 31, Q. no 105I)

Question de K. Gabriëls au ministre de la Justice sur 'la numérisation de la Sûreté de l'État' (*C.R.I.*, Chambre, 2020-2021, 17 mars 2021, COM 415, p. 36, Q. no 15422C)

Question de S. Cogolati au ministre de la Justice sur 'les menaces et intimidations du gouvernement turc vis-à-vis d'opposants en Belgique' (*C.R.I.*, Chambre, 2020-2021, 17 mars 2021, COM 415, p. 42, Q. no 15442C)

Questions jointes de B. Pas et K. Metsu au Premier ministre sur 'la menace terroriste croissante en Europe' (*C.R.I.*, Chambre, 2020-2021, 18 mars 2021, PLEN 93, p. 33, Q. nos 1462P et 1471P)

Questions jointes de Ph. Pivin, M. Dillen, N. Boukili, K. Van Vaerenbergh, K. Geens et G. Dallemagne au ministre de la Justice sur 'l'accompagnement et l'indemnisation des victimes d'actes terroristes' (*C.R.I.*, Chambre, 2020-2021, 19 mars 2021, COM 418, p. 1, Q. nos 15257C, 110I, 111I, 15426C, 15448C, 15490C, 15507C, 15511C, 15519C et 15520C)

Suivi des recommandations de la commission d'enquête parlementaire "Attentats terroristes", échange de vues et questions jointes de S. Rohonyi au ministre de la Justice sur 'un fonds d'indemnisation des victimes d'attentats terroristes' (*C.R.I.*, Chambre, 2020-2021, 23 mars 2021, COM 422, p. 1, Q. nos 15751C, 15752C, 15754C, 15755C et 15760C)

Question de Th. Francken au secrétaire d'État à l'Asile et la Migration sur 'le rapatriement d'extrémistes musulmans et de combattants partis en Syrie vers leur pays d'origine' (*C.R.I.*, Chambre, 2020-2021, 26 mars 2021, COM 425, p. 10, Q. n° 15509C)

Questions jointes d'Y. Van Camp, F. Demon, E. Platteau et H. Rigot au secrétaire d'État à l'Asile et la Migration sur 'les équipes outreach actives auprès des migrants en transit' (*C.R.I.*, Chambre, 2020-2021, 26 mars 2021, COM 425, p. 18, Q. n°s 15575C, 15585C, 15851C et 15857C)

Question de B. Segers au secrétaire d'État à l'Asile et la Migration sur 'la plateforme électronique pour les procédures de demande de séjour combinées' (*C.R.I.*, Chambre, 2020-2021, 26 mars 2021, COM 425, p. 43, Q. n° 15814C)

Question de V. Scourneau à la ministre des Affaires étrangères sur 'la sécurité de nos diplomates en République démocratique du Congo' (*Q.R.*, Chambre, 2020-2021, 31 mars 2021, n° 45, p. 99, Q. n° 218)

Question d'A. Ponthier à la ministre des Affaires étrangères sur le 'Congo oriental - assassinat de l'ambassadeur d'Italie' (*Q.R.*, Chambre, 2020-2021, 31 mars 2021, n° 45, p. 113, Q. n° 242)

Question de K. Metsu au ministre de la Justice sur 'le retour des combattants partis en Syrie et le suivi par l'OCAM de femmes et d'enfants liés à Daech' (*C.R.I.*, Chambre, 2020-2021, 31 mars 2021, COM 436, p. 35, Q. n° 15824C)

Question de K. Jadin à la ministre des Affaires étrangères sur 'la terreur de Daech à la prison d'Al-Hol' (*Q.R.*, Chambre, 2020-2021, 7 avril 2021, n° 46, p. 124, Q. n° 228)

Question d'E. Burton à la ministre des Affaires étrangères sur 'les risques pour les diplomates belges en RDC' (*Q.R.*, Chambre, 2020-2021, 7 avril 2021, n° 46, p. 130, Q. n° 248)

Question de M. Freilich au ministre de la Justice sur 'l'entreprise Circles' (*Q.R.*, Chambre, 2020-2021, 7 avril 2021, n° 46, p. 221, Q. n° 378)

Question de M. Vindevoghel au ministre de la Mobilité sur 'la menace terroriste sur le rail' (*Q.R.*, Chambre, 2020-2021, 15 avril 2021, n° 47, p. 122, Q. n° 112)

Question de K. Metsu à la ministre de l'Intérieur sur 'le plan Canal à Bruxelles et la mise en place des CSIL' (*Q.R.*, Chambre, 2020-2021, 15 avril 2021, n° 47, p. 294, Q. n° 400)

Question de B. Segers au secrétaire d'État à l'Asile et la Migration sur 'l'obtention de visas humanitaires par le biais d'intermédiaires' (*Q.R.*, Chambre, 2020-2021, 15 avril 2021, n° 47, p. 352, Q. n° 155)

Question de P. Buysrogge à la ministre de la Défense sur 'les nouveaux minidrones' (*C.R.I.*, Chambre, 2020-2021, 20 avril 2021, COM 438, p. 10, Q. n° 14240C)

Question d'A. Ponthier à la ministre de la Défense sur les suspensions du contrat conclu pour l'Open Source Intelligence System' (*C.R.I.*, Chambre, 2020-2021, 20 avril 2021, COM 438, p. 16, Q. n° 14534C)

Questions jointes de G. Defossé et P. Buysrogge à la ministre de la Défense sur 'les cyberopérations offensives' (*C.R.I.*, Chambre, 2020-2021, 20 avril 2021, COM 438, p. 19, Q. n°s 14627C et 16305C)

Questions jointes de G. Defossé, Ch. Lacroix et K. Verduyckt à la ministre de la Défense sur 'l'extrême droite au sein de l'armée' (*C.R.I.*, Chambre, 2020-2021, 20 avril 2021, COM 438, p. 45, Q. n°s 15600C, 5621C et 16526C)

Question de K. Metsu au ministre de la Justice sur 'l'OCAM' (*C.R.I.*, Chambre, 2020-2021, 21 avril 2021, COM 442, p. 32, Q. n° 16385C)

Question de M. Freilich au ministre de la Justice sur 'le cyberespionnage chinois' (*C.R.I.*, Chambre, 2020-2021, 21 avril 2021, COM 445, p. 33, Q. n° 16518C)

Question de K. Metsu au ministre de la Justice sur 'le cofondateur du CCIB membre du conseil d'administration de Myria et Unia' (*C.R.I.*, Chambre, 2020-2021, 21 avril 2021, COM 445, p. 42, Q. n° 16626C)

Questions jointes d'E. Samyn, K. Aouasti, K. Metsu et Th. Francken à la ministre des Affaires étrangères sur 'les combattantes belges de l'EI en Syrie' (*C.R.I.*, Chambre, 2020-2021, 27 avril 2021, COM 449, p. 33, Q. n^{os} 14807C, 15558C, 15825C et 16400C)

Questions jointes de S. Cogolati, E. Samyn et Ch. Lacroix à la ministre des Affaires étrangères sur 'les menaces et intimidations du gouvernement turc vis-à-vis d'opposants en Belgique' (*C.R.I.*, Chambre, 2020-2021, 27 avril 2021, COM 449, p. 82, Q. n^{os} 15441C, 113I et 16346C)

Débat d'actualité et questions jointes de G. Defossé, J. Pillen, Th. Francken, K. Jadin, Ch. Lacroix et A. Ponthier à la ministre de la Défense sur 'la fin de Resolute Support Afghanistan' (*C.R.I.*, Chambre, 2020-2021, 28 avril 2021, COM 452, p. 1, Q. n^{os} 16438C, 16504C, 16580C, 16622C, 16820C et 16842C)

Question de C. Thibaut à la ministre de l'Intérieur sur 'le contrôle sur les données contenues dans la BNG' (*C.R.I.*, Chambre, 2020-2021, 28 avril 2021, COM 453, p. 16, Q. n^{o} 16719C)

Question d'E. Platteau à la ministre de la Fonction publique sur 'l'arrêt de la Cour constitutionnelle sur le stockage des données de télécommunication' (*C.R.I.*, Chambre, 2020-2021, 28 avril 2021, COM 456, p. 13, Q. n^{o} 16918C)

Question de S. Thémont à la ministre de l'Intérieur sur 'le logiciel de détectage de menaces terroristes ou de radicalisation' (*Q.R.*, Chambre, 2020-2021, 3 mai 2021, n^{o} 50, p. 306, Q. n^{o} 456)

Question de K. Jadin à la ministre de l'Intérieur sur 'le risque d'atteintes aux centres de vaccination' (*Q.R.*, Chambre, 2020-2021, 3 mai 2021, n^{o} 50, p. 313, Q. n^{o} 461)

Interpellation d'E. Gilissen à la ministre de la Fonction publique sur 'l'annulation de la loi sur la conservation des données par la Cour constitutionnelle' (*C.R.I.*, Chambre, 2020-2021, 3 mai 2021, COM 457, p. 1, Q. n^{o} 122I)

Interpellation et questions jointes de K. Bury, S. De Wit, K. Geens et N. Boukili au ministre de la Justice sur 'la législation en matière de conservation des données' (*C.R.I.*, Chambre, 2020-2021, 5 mai 2021, COM 463, p. 1, Q. n^{os} 120I, 16763C, 16799C et 17247C)

Interpellation et questions jointes de K. Jadin et S. Van Hecke au ministre de la Justice sur 'la lutte contre les sectes nuisibles' (*C.R.I.*, Chambre, 2020-2021, 5 mai 2021, COM 463, p. 19, Q. n^{os} 17266C et 17275C)

Question d'E. Platteau à la ministre de l'Intérieur sur 'l'ampleur de la menace que représente l'extrême droite' (*C.R.I.*, Chambre, 2020-2021, 5 mai 2021, COM 464, p. 53, Q. n^{o} 17111C)

Question d'O. Depoortere à la ministre de l'Intérieur sur 'la menace émanant de l'extrême gauche' (*C.R.I.*, Chambre, 2020-2021, 5 mai 2021, COM 464, p. 56, Q. n^{o} 17199C)

Question de K. Metsu à la ministre des Affaires étrangères sur la 'montée en puissance du groupe autoproclamé État islamique au Moyen-Orient' (*Q.R.*, Chambre, 2020-2021, 10 mai 2021, n^{o} 51, p. 140, Q. n^{o} 68)

Question de G. Dallemagne à la ministre de l'Intérieur sur 'la lutte contre le radicalisme durant la période de COVID-19' (*Q.R.*, Chambre, 2020-2021, 10 mai 2021, n^{o} 51, p. 323, Q. n^{o} 470)

Question de V. Scourneau à la ministre des Affaires étrangères sur la 'sécurité informatique' (*Q.R.*, Chambre, 2020-2021, 18 mai 2021, n^{o} 52, p. 117, Q. n^{o} 281)

Question de M. Freilich au ministre de la Justice sur les 'smartphones - Xiaomi, Oppo et OnePlus' (*Q.R.*, Chambre, 2020-2021, 27 mai 2021, n^{o} 53, p. 317, Q. n^{o} 466)

Question de V. Scourneau à la ministre de la Défense sur 'l'achat de drones miniatures par la Défense' (*Q.R.*, Chambre, 2020-2021, 27 mai 2021, n^{o} 53, p. 331, Q. n^{o} 230)

Question de Ch. Lacroix à la ministre de la Défense sur 'le retrait de l'habilitation de sécurité de notre attaché de défense à Paris' (*Q.R.*, Chambre, 2020-2021, 27 mai 2021, n^{o} 53, p. 343, Q. n^{o} 258)

Question de K. Jadin à la ministre de la Défense sur 'les archives de la Défense' (*Q.R.*, Chambre, 2020-2021, 27 mai 2021, n^{o} 53, p. 344, Q. n^{o} 259)

Questions jointes d'E. Gilissen, Y. Ingels, Ph. Pivin, K. Verhelst, F. Demon et M. Freilich à la ministre de l'Intérieur sur 'le piratage du SPF Intérieur' (*C.R.I.*, Chambre, 2020-2021, 27 mai 2021, PLEN 106, p. 13, Q. nos 1679P, 1684P, 1685P, 1686P, 1689P et 1695P)

Questions jointes d'A. Ponthier, S. De Vuyst et P. Buysrogge à la ministre de la Défense sur 'l'affaire Jürgen Conings et la responsabilité de la ministre ainsi que de la Défense' (*C.R.I.*, Chambre, 2020-2021, 27 mai 2021, PLEN 106, p. 101, Q. nos 131I à 133I)

Question de C. Taquin à la ministre de l'Intérieur sur 'l'évaluation du dispositif CSIL-R' (*Q.R.*, Chambre, 2020-2021, 2 juin 2021, no 54, p. 229, Q. no 555)

Débat d'actualité et questions jointes de G. Defossé, P. Buysrogge, Th. Francken, S. De Vuyst, N. Boukili, D. Ducarme, K. Verduyckt, Ch. Lacroix, W. De Vriendt et A. Ponthier à la ministre de la Défense sur 'le suivi du cas du soldat fugitif (*C.R.I.*, Chambre, 2020-2021, 2 juin 2021, COM 495, p. 14, Q. nos 18241C, 18242C, 18309C, 18311C, 18318C, 18320C, 18321C, 18328C, 18388C, 18429C, 18466C et 18482C)

Questions jointes de J. Chanson, E. Platteau, K. Jadin, Ph. Pivin, D. Ducarme et K. Aouasti au Premier ministre sur 'l'extrême droite au sein de la police' (*C.R.I.*, Chambre, 2020-2021, 2 juin 2021, COM 500, p. 7, Q. nos 17992C, 18183C, 18401C, 18420C, 18421C, 18459C et 18460C)

Questions jointes de S. De Vuyst et N. Boukili au Premier ministre sur 'la traque du militaire lourdement armé' (*C.R.I.*, Chambre, 2020-2021, 2 juin 2021, COM 501, p. 14, Q. nos 18075C et 18161C)

Question de N. Boukili au ministre de la Justice sur 'l'espionnage d'un certain nombre de pays européens par les États-Unis' (*C.R.I.*, Chambre, 2020-2021, 2 juin 2021, COM 501, p. 55, Q. no 18457C)

Question de P. De Roover au Premier ministre sur 'les fuites dans la presse au sujet de rapports secrets de la Sûreté de l'État' (*C.R.I.*, Chambre, 2020-2021, 9 juin 2021, COM 511, p. 12, Q. no 15727C)

Question de W. Vermeersch au ministre de la Justice sur 'la reconnaissance des mosquées' (*Q.R.*, Chambre, 2020-2021, 12 juin 2021, no 55, p. 247, Q. no 510)

Question de C. Thibaut au ministre de la Justice sur la 'notification obligatoire pour chaque collaborateur figurant dans une BDC Terrorist Fighters' (*Q.R.*, Chambre, 2020-2021, 12 juin 2021, no 55, p. 274, Q. no 576)

Question de W. Vermeersch à la ministre de l'Intérieur sur 'la reconnaissance des mosquées' (*Q.R.*, Chambre, 2020-2021, 12 juin 2021, no 55, p. 334, Q. no 561)

Question de C. Thibaut à la ministre de l'Intérieur sur 'la manière dont les services de renseignement communiquent avec des instances ou avec des personnes privées ou publiques' (*Q.R.*, Chambre, 2020-2021, 12 juin 2021, no 55, p. 351, Q. no 570)

Questions jointes de N. Boukili, R. Hedebouw et D. Ducarme à la ministre de l'Intérieur sur 'l'affaire Conings' (*C.R.I.*, Chambre, 2020-2021, 16 juin 2021, COM 518, p. 21, Q. nos 18652C, 18653C et 18943C)

Échange de vues et questions jointes de P. Buysrogge, Th. Francken, S. De Vuyst, K. Verduyckt, G. Defossé, M. De Maegd, A. Ponthier, D. Ducarme, Ch. Lacroix et H. Bogaert à la ministre de la Défense sur 'le rapport interne de l'inspection générale de la Défense sur l'affaire Jürgen Conings' (*C.R.I.*, Chambre, 2020-2021, 16 juin 2021, COM 519, p. 1, Q. nos 18607C, 18605C, 18618C, 18656C, 18745C, 18808C, 18835C, 18907C, 18914C, 19011C et 19020C)

Question de Th. Francken au secrétaire d'État à l'Asile et la Migration sur 'l'inspection interne de Fedasil relative aux demandeurs d'asile fauteurs de troubles dans les centres d'accueil' (*C.R.I.*, Chambre, 2020-2021, 18 juin 2021, COM 520, p. 47, Q. no 19059C)

Question de T. Van Grieken au ministre de la Justice sur 'l'agrément des mosquées' (*Q.R.*, Chambre, 2020-2021, 22 juin 2021, no 56, p. 177, Q. no 507)

Question de T. Van Grieken au ministre de la Justice sur le 'screening de demandeurs d'asile concernant des liens avec des groupements terroristes ou des groupements radicaux potentiellement dangereux' (*Q.R.*, Chambre, 2020-2021, 22 juin 2021, nº 56, p. 190, Q. nº 530)

Question de C. Thibaut au ministre de la Justice sur 'la manière dont le SGRS communique avec des instances ou avec des personnes privées ou publiques' (*Q.R.*, Chambre, 2020-2021, 22 juin 2021, nº 56, p. 233, Q. nº 560)

Question de C. Thibaut à la ministre de l'Intérieur sur 'l'évacuation de la ZAD d'Arlon' (*Q.R.*, Chambre, 2020-2021, 22 juin 2021, nº 56, p. 252, Q. nº 578)

Questions jointes de M. De Maegd, M. Ben Achour et P. De Roover à la ministre des Affaires étrangères sur 'la mission belge dans le camp de Roj' (*C.R.I.*, Chambre, 2020-2021, 29 juin 2021, COM 530, p. 89, Q. nºs 18768C, 18798C et 18884C)

Questions jointes d'O. Depoortere, Y. Ingels et T. Vandenput à la ministre de l'Intérieur sur 'le manque d'effectifs à la police' (*C.R.I.*, Chambre, 2020-2021, 30 juin 2021, COM 531, p. 20, Q. nºs 19355C, 19400C et 19429C)

Question d'E. Burton à la ministre des Affaires étrangères sur la 'présence des services des renseignements chinois à Liège' (*Q.R.*, Chambre, 2020-2021, 30 juin 2021, nº 57, p. 118, Q. nº 327)

Question de C. Thibaut au ministre de la Justice sur 'l'évaluation de la menace posée par les anti-5g' (*Q.R.*, Chambre, 2020-2021, 30 juin 2021, nº 57, p. 192, Q. nº 587)

Question de Ph. Pivin au ministre de la Justice sur le 'screening des investissements étrangers – Commission de screening interdépartementale' (*Q.R.*, Chambre, 2020-2021, 30 juin 2021, nº 57, p. 196, Q. nº 597)

Question de D. Safai au secrétaire d'État à l'Asile et la Migration sur 'les visas humanitaires accordés aux femmes et aux enfants liés à l'EI' (*C.R.I.*, Chambre, 2020-2021, 2 juillet 2021, COM 535, p. 21, Q. nº 19570C)

Échange de vues, interpellation et questions jointes de K. Jadin, A. Ponthier, Th. Francken et G. Defossé à la ministre de la Défense sur 'le rapport du Comité R et les soins psychosociaux à l'armée' (*C.R.I.*, Chambre, 2020-2021, 5 juillet 2021, COM 537, p. 1, Q. nºs 18547C, 19099C, 19136C, 00149I, 19252C, 19257C et 19595C)

Question de S. Loones à la ministre du Budget sur 'le budget de la Défense' (*C.R.I.*, Chambre, 2020-2021, 6 juillet 2021, COM 539, p. 20, Q. nº 18077C)

Question d'A. Ponthier au ministre de la Justice sur 'l'influence de Soros' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 250, Q. nº 595)

Question d'Y. Van Camp au ministre de la Justice sur 'le screening des imams prédicateurs de haine' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 261, Q. nº 553)

Question de K. Verduyckt au ministre de la Justice sur 'la présence de l'extrême droite dans les rangs du personnel pénitentiaire' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 268, Q. nº 583)

Question d'A. Van Bossuyt au ministre de la Justice sur 'l'espionnage chinois par le biais du programme Thousand Talents' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 279, Q. nº 612)

Question de K. Jadin à la ministre de la Défense sur 'le suivi du personnel de la Défense' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 291, Q. nº 274)

Question de Ph. Pivin à la ministre de l'Intérieur sur la 'Cellule radicalisme de l'Office des étrangers' (*Q.R.*, Chambre, 2020-2021, 8 juillet 2021, nº 58, p. 345, Q. nº 148)

Question de G. Dallemagne au ministre de la Justice sur 'le rapport de l'OCAM sur le wahhabisme, le djihadisme et le terrorisme' (*C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, COM 556, p. 7, Q. nº 19771C)

Questions jointes de J. Pillen, S. Creyelman et K. Jadin à la ministre de la Défense sur 'la composante cyber' (*C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, COM 557, p. 23, Q. n^{os} 17854C, 18003C et 19321C)

Questions jointes de G. Defossé, V. Reynaert et Ch. Lacroix à la ministre de la Défense sur 'la révélation de secrets sur les bombes nucléaires présentes en Europe' (*C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, COM 557, p. 27, Q. n^{os} 18336C, 18384C et 18433C)

Question de Th. Francken à la ministre de la Défense sur 'les opérations psychologiques (psy-ops)' (*C.R.I.*, Chambre, 2020-2021, 14 juillet 2021, COM 557, p. 34, Q. n^{o} 18783C)

Interpellations jointes de P. De Roover et B. Pas au Premier ministre sur 'la démission de la commissaire du gouvernement, Mme Haouach' (*C.R.I.*, Chambre, 2021-2022, 15 juillet 2021, PLEN 122, p. 26, Q. n^{os} 162I et 163I)

Question de S. Van Hecke à la ministre des Affaires étrangères sur 'les difficultés de communication avec l'Autorité nationale de Sécurité' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, n^{o} 59, p. 105, Q. n^{o} 341)

Question de C. Thibaut à la ministre des Affaires étrangères sur 'l'absence de réponses de l'ANS au Comité R en matière d'habilitation de sécurité' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, n^{o} 59, p. 108, Q. n^{o} 342)

Question d'Y. Ingels au ministre de la Mobilité sur 'l'octroi des badges d'accès au tarmac' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, n^{o} 59, p. 185, Q. n^{o} 601)

Question de K. Metsu au ministre de la Justice sur 'la reconnaissance des communautés religieuses à Bruxelles' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, n^{o} 59, p. 261, Q. n^{o} 617)

Question de K. Verduyckt à la ministre de l'Intérieur sur 'la présence de l'extrême droite dans les rangs de la police' (*Q.R.*, Chambre, 2020-2021, 15 juillet 2021, n^{o} 59, p. 347, Q. n^{o} 665)

Échange de vues et questions jointes de B. Pas, E. Samyn, D. Van Langenhove et K. Metsu au Premier ministre et à la ministre des Affaires étrangères sur 'l'opération de rapatriement de femmes et d'enfants de djihadistes' (*C.R.I.*, Chambre, 2020-2021, 22 juillet 2021, COM 560, p. 1, Q. n^{os} 19979C, 19977C, 19981C et 19995C)

Échange de vues et questions jointes de Th. Francken, A. Ponthier, W. De Vriendt, G. Dallemagne, K. Verduyckt, S. De Vuyst, G. Defossé et Ch. Lacroix à la ministre de la Défense sur 'le remplacement du général-major Boucké à la tête du SGRS' (*C.R.I.*, Chambre, 2020-2021, 22 juillet 2021, COM 561, p. 1, Q. n^{os} 19973C, 19974C, 19975C, 19976C, 19983C, 19990C, 19993C et 19994C)

Question d'Y. Ingels à la ministre des Affaires étrangères sur 'l'Autorité Nationale de Sécurité – rôle et missions' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, n^{o} 60, p. 92, Q. n^{o} 347)

Question de S. Cogolati à la ministre des Affaires étrangères sur 'l'espionnage de la NSA via le Danemark' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, n^{o} 60, p. 105, Q. n^{o} 363)

Question de K. Jadin à la ministre des Affaires étrangères sur 'l'espionnage de la NSA via le Danemark' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, n^{o} 60, p. 109, Q. n^{o} 365)

Question de B. Moyaers à la ministre des Affaires étrangères sur 'l'identification politique des pirates informatiques' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, n^{o} 60, p. 120, Q. n^{o} 376)

Question de S. De Vuyst à la ministre des Affaires étrangères sur 'l'espionnage américain' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, n^{o} 60, p. 123, Q. n^{o} 380)

Question de C. Taquin au ministre de la Justice sur 'la lutte contre les dérives sectaires durant la pandémie' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, n^{o} 60, p. 184, Q. n^{o} 567)

Question d'E. Burton au ministre de la Justice sur 'la Sûreté de l'État et l'espionnage' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, n^{o} 60, p. 194, Q. n^{o} 592)

Question de J. Pillen au ministre de la Défense sur 'l'effectif du SGRS' (*Q.R.*, Chambre, 2020-2021, 24 juillet 2021, n^{o} 60, p. 303, Q. n^{o} 286)

Question d'Y. Ingels au Premier ministre sur 'pouvoir échanger en toute sécurité des informations sensibles' (*Q.R.*, Chambre, 2020-2021, 11 août 2021, nº 61, p. 135, Q. nº 111)

Question de D. Safai à la ministre de l'Intérieur sur les 'cours sur le radicalisme et point de contact radicalisation' (*Q.R.*, Chambre, 2020-2021, 11 août 2021, nº 61, p. 337, Q. nº 227)

Échange de vues et questions jointes de Th. Francken, A. Flahaut, G. Liekens, S. de Laveleye, G. Defossé, Ch. Lacroix, V. Reynaert, D. Van Langenhove, W. De Vriendt, Fr. De Smet, H. Rigot, K. Jadin, J. Chanson, T. Vandenput, S. Moutquin, E. Platteau, N. Boukili et B. Segers au Premier ministre sur 'la situation en Afghanistan' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 575, p. 31, Q. nºs 20147C, 20148C, 20156C, 20147C, 20118C, 20094C, 20103C, 20104C, 20140C, 20162C, 20122C, 20154C, 20155C, 20083C, 20093C, 20115C, 20158C, 20137C, 20146C, 20157C, 20057C, 20067C, 20095C, 20110C, 20119C, 20120C, 20127C, 20145C, 20130C, 20132C, 20133C, 20134C, 20135C, 20136C, 20138C, 20139C, 20141C, 20142C, 20161C, 20163C, 20164C et 20165C)

Question de J. Donné au ministre des Finances sur les 'consultations du PCC2' (*Q.R.*, Chambre, 2020-2021, 6 septembre 2021, nº 62, p. 216, Q. nº 146)

Question de W. Vermeersch au ministre des Finances sur la 'reconnaissance des mosquées' (*Q.R.*, Chambre, 2020-2021, 6 septembre 2021, nº 62, p. 228, Q. nº 398)

Question de B. Segers au ministre de la Justice sur le 'screening des candidats à un visa humanitaire' (*Q.R.*, Chambre, 2020-2021, 6 septembre 2021, nº 62, p. 319, Q. nº 606)

Question de M. Freilich au ministre de la Justice sur le 'logiciel de NSO group' (*Q.R.*, Chambre, 2020-2021, 6 septembre 2021, nº 62, p. 337, Q. nº 658)

Question d'Y. Ingels au Premier ministre sur les 'projets de départements de sécurité à la Régie des Bâtiments' (*Q.R.*, Chambre, 2020-2021, 20 septembre 2021, nº 63, p. 338, Q. nº 150)

Questions jointes de Th. Francken, S. Moutquin et D. Van Langenhove au secrétaire d'État à l'Asile et la Migration sur 'le programme de visas humanitaires pour les Afghans' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 575, p. 31, Q. nºs 20703C, 20883C, 20886C, 20888C, 20916C et 20931C)

Questions jointes de M. Freilich, S. Van Hecke, N. Boukili et E. Van Hoof au ministre de la Justice sur 'le logiciel d'écoute' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 577, p. 1, Q. nºs 19985C, 20000C, 20448C et 20845C)

Questions jointes de M. Freilich, E. Gilissen et K. Gabriëls au ministre de la Justice sur 'le classement sans suite dans le cadre de l'enquête sur les espions chinois' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 577, p. 41, Q. nºs 20313C, 20325C et 20903C)

Question de Karin Jiroflée au ministre de la Justice sur 'le non-respect des interdictions temporaires de résidence' (*C.R.I.*, Chambre, 2020-2021, 22 septembre 2021, COM 577, p. 45, Q. nº 20335C)

Débat d'actualité et questions jointes de P. De Roover, K. Jadin, V. Reynaert, H. Rigot et S. Cogolati à la ministre des Affaires étrangères sur 'l'Afghanistan' (*C.R.I.*, Chambre, 2020-2021, 28 septembre 2021, COM 579, p. 7, Q. nºs 20256C, 20270C, 20271C, 20408C, 21142C, 21173C et 21221C)

Questions jointes de S. Van Hecke et E. Van Hoof à la ministre des Affaires étrangères sur 'l'incidence de Pegasus sur les relations diplomatiques et les mesures à prendre dans ce cadre' (*C.R.I.*, Chambre, 2020-2021, 28 septembre 2021, COM 579, p. 19, Q. nºs 20007C et 21061C)

Question de M. Dillen au ministre de la Justice sur 'Oussama Atar et les attentats commis à Paris et Bruxelles' (*C.R.I.*, Chambre, 2020-2021, 29 septembre 2021, COM 586, p. 15, Q. nº 20496C)

Question de Ph. Pivin au ministre de l'Économie sur le 'screening des investissements étrangers – Commission de screening interdépartementale' (*Q.R.*, Chambre, 2020-2021, 2 octobre 2021, nº 64, p. 29, Q. nº 566)

Question de S. Creyelman à la ministre de la Défense sur le 'matériel d'espionnage retrouvé dans l'ambassade de Belgique à Ankara' (*Q.R.*, Chambre, 2021-2022, 2 octobre 2021, nº 64, p. 175, Q. nº 315)

Question de S. Verherstraeten à la ministre de la Défense sur les 'militaires – sympathies pour l'extrême droite' (*Q.R.*, Chambre, 2020-2021, 2 octobre 2021, nº 64, p. 178, Q. nº 320)

Question de D. Safai au secrétaire d'État à l'Asile et la Migration sur 'le rapatriement de terroristes de l'EI et de leurs enfants' (*C.R.I.*, Chambre, 2020-2021, 5 octobre 2021, COM 588, p. 31, Q. nº 20943C)

Question de D. Van Langenhove au secrétaire d'État à l'Asile et la Migration sur 'les résultats du screening de sécurité' (*C.R.I.*, Chambre, 2020-2021, 5 octobre 2021, COM 588, p. 31, Q. nº 20993C)

Question de G. Dallemagne au ministre de la Justice sur 'le noyau salafiste à Molenbeek' (*Q.R.*, Chambre, 2020-2021, 6 octobre 2021, nº 65, p. 422, Q. nº 724)

Question d'E. Van Hoof à la ministre de la Défense sur 'le logiciel espion Pegasus' (*Q.R.*, Chambre, 2020-2021, 6 octobre 2021, nº 65, p. 439, Q. nº 326)

Question de S. Cogolati au ministre de la Justice sur 'l'enquête sur l'attribution de la cyberattaque contre Belnet du 4 mai 2021' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 596, p. 4, Q. nº 21135C)

Question de K. Metsu au ministre de la Justice sur 'les malversations constatées au sein de l'ASBL Exécutif des Musulmans' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 596, p. 26, Q. nº 21579C)

Question de S. Verherstraeten à la ministre de l'Intérieur sur 'la recrudescence de la menace provenant de l'extrême droite' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 597, p. 35, Q. nº 20009C)

Questions jointes de M. Freilich et J. Chanson à la ministre de l'Intérieur sur 'la fin de l'OVG' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 597, p. 55, Q. nºs 20331C et 20404C)

Questions jointes de M. Freilich et K. Metsu à la ministre de l'Intérieur sur 'l'arrestation de plusieurs hommes radicalisés' (*C.R.I.*, Chambre, 2020-2021, 6 octobre 2021, COM 597, p. 76, Q. nºs 20744C, 21288C et 21384C)

Questions jointes d'A. Ponthier, K. Metsu et P. Dewael au Premier ministre sur 'les problèmes récurrents de fondamentalisme au sein de l'Exécutif des Musulmans de Belgique' (*C.R.I.*, Chambre, 2020-2021, 7 octobre 2021, PLEN 127, p. 5, Q. nºs 1932P, 1945P et 1948P)

Question de M. Freilich au Premier ministre sur le 'logiciel de NSO group' (*Q.R.*, Chambre, 2020-2021, 10 octobre 2021, nº 66, p. 39, Q. nº 129)

Débat d'actualité et questions jointes de K. Jadin, A. Ponthier, G. Defossé, Th. Francken et A. FLahaut à la ministre de la Défense sur 'la recherche de l'extrémisme' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 2021, COM 606, p. 1, Q. nºs 20281C, 20292C, 20864C, 20942C,21565C, 22019C et 21674C)

Questions jointes d'A. Ponthier et G. Dallemagne à la ministre de la Défense sur 'les réformes au sein du SGRS après la nomination du vice-amiral W. Robberecht à la tête du service' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 2021, COM 606, p. 10, Q. nºs 20306C et 20923C)

Questions jointes de T. Vandenput et J. Chanson à la ministre de l'Intérieur sur 'les problèmes avec le réseau ASTRID' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 2021, COM 611, p. 40, Q. nºs 21129C et 21212C)

Question de S. Loones à la ministre de l'Intérieur sur 'le signalement de M. Puigdemont dans le système d'information Schengen (SIS)' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 2021, COM 611, p. 53, Q. n° 21308C)

Questions jointes de S. Goethals et O. Depoortere à la ministre de l'Intérieur sur 'la constitution de partie civile de la ministre' (*C.R.I.*, Chambre, 2021-2022, 20 octobre 202, COM 611, p. 66, Q. n°s 21542C et 21575C)

Question d'E. Van Hoof au ministre de la Justice sur 'le logiciel espion Pegasus' (*Q.R.*, Chambre, 2021-2022, 26 octobre 2021, n° 67, p. 247, Q. n° 689)

Question d'A. Ponthier au ministre de la Justice sur le 'coût de l'opération Jürgen Conings' (*Q.R.*, Chambre, 2021-2022, 26 octobre 2021, n° 67, p. 252, Q. n° 699)

Question de S. Creyelman à la ministre de la Défense sur 'la possible divulgation de thèses complotistes par la Russie' (*C.R.I.*, Chambre, 2021-2022, 27 octobre 2021, COM 618, p. 13, Q. n° 22136C)

Questions jointes de G. Defossé et P. Buysrogge à la ministre de la Défense sur 'les propos tenus par M. Lipszyc dans une interview' (*C.R.I.*, Chambre, 2021-2022, 27 octobre 2021, COM 618, p. 21, Q. n°s 22258C et 22364C)

Question de M. Freilich au Premier ministre sur 'la mise à mal du cryptage' (*C.R.I.*, Chambre, 2021-2022, 27 octobre 2021, COM 623, p. 20, Q. n° 22038C)

Question de K. Geens à la ministre de l'Intérieur sur 'l'opération Sky' (*C.R.I.*, Chambre, 2021-2022, 28 octobre 2021, PLEN 136, p. 24, Q. n°s 1990P)

Questions jointes d'A. Ponthier et N. Boukili au ministre de la Justice sur 'les perquisitions menées chez des militaires pour soupçons d'incitation au terrorisme' (*C.R.I.*, Chambre, 2021-2022, 10 novembre 2021, COM 625, p. 15, Q. n°s 22510C et 22521C)

Question de M. Freilich au ministre de la Justice sur 'le logiciel espion développé par NSO' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 257, Q. n° 728)

Question de S. Creyelman à la ministre de la Défense sur les 'extrémisme au sein de la Défense - suivi' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 338, Q. n° 321)

Question de M. Freilich au Premier ministre sur 'l'approche du dark web' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 129, Q. n° 145)

Question de M. Freilich au Premier ministre sur 'la capacité répressive en matière de cybercriminalité' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 130, Q. n° 146)

Question de Th. Francken au ministre de la Justice sur 'le colosse de Molenbeek' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 260, Q. n° 747)

Question de S. Creyelman à la ministre de la Défense sur 'l'extrémisme au sein de la Défense – suivi' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 338, Q. n° 321)

Question de S. Van Hecke à la ministre de la Défense sur 'les actions du SGRS à la suite du projet Pegasus' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 349, Q. n° 355)

Question de S. Matheï au Premier ministre sur 'l'évaluation du RGPD' (*Q.R.*, Chambre, 2021-2022, 18 novembre 2021, n° 69, p. 402, Q. n° 221)

Question de K. Jadin à la ministre de la Défense sur 'la sécurité des appareils d'origine chinoise' (*Q.R.*, Chambre, 2021-2022, 25 novembre 2021, n° 70, p. 285, Q. n° 357)

Question d'A. Vicaire au ministre de la Digitalisation sur 'l'affaire Pegasus et la protection des responsables politiques belges' (*C.R.I.*, Chambre, 2021-2022, 30 novembre 2021, COM 630, p. 1, Q. n° 20099C)

Question de K. Metsu au ministre de la Justice sur 'le plan d'action pour la déradicalisation dans nos prisons' (*C.R.I.*, Chambre, 2021-2022, 2 décembre 2021, PLEN 144, p. 15, Q. n° 2090P)

Question d'Y. Ingels au Premier ministre sur la 'politique fédérale en matière de drogues – crime organisé' (*Q.R.*, Chambre, 2021-2022, 6 décembre 2021, n° 71, p. 67, Q. n° 153)

Question de M. Dillen au ministre de la Justice sur le 'rapport de la Cour des comptes sur l'ASA – objectifs transversaux de simplification administrative' (*Q.R.*, Chambre, 2021-2022, 6 décembre 2021, nº 71, p. 225, Q. nº 796)

Question d'E. Burton au ministre de la Justice sur 'les deepfakes' (*Q.R.*, Chambre, 2021-2022, 6 décembre 2021, nº 71, p. 248, Q. nº 823)

Question de S. Cogolati au ministre de la Justice sur 'les risques d'espionnage au China-Belgium Technology Center' (*Q.R.*, Chambre, 2021-2022, 6 décembre 2021, nº 71, p. 250, Q. nº 824)

Questions jointes B. Pas et K. Metsu au Premier ministre sur 'le suivi défaillant des djihadistes en Belgique' (*C.R.I.*, Chambre, 2021-2022, 9 décembre 2021, PLEN 145, p. 23, Q. nºs 2099P et 2124P)

Questions jointes de K. Jadin et M. Vindevoghel à la ministre de la Défense sur 'le recrutement du militaire belge' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 640, p. 3, Q. nºs 23244C et 23388C)

Question de G. Defossé à la ministre de la Défense sur 'les menaces de mort proférées par un militaire belge contre un ministre' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 640, p. 7, Q. nº 23346C)

Question de K. Jadin à la ministre de l'Intérieur sur 'l'extrémisme en Belgique' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 642, p. 6, Q. nº 23074C)

Question d'E. Platteau à la ministre de l'Intérieur sur 'la lutte contre l'extrémisme au travers de la réinsertion sociale et du désengagement' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 642, p. 13, Q. nº 23104C)

Questions jointes d'E. Platteau, F. Demon, T. Vandenput et O. Depoortere à la ministre de l'Intérieur sur 'le rapport de l'OCAM sur la crise du coronavirus ' (*C.R.I.*, Chambre, 2021-2022, 15 décembre 2021, COM 642, p. 14, Q. nºs 23178C, 23229C, 23393C et 23415C)

Questions jointes K. Metsu et Ph. Pivin au ministre de la Justice sur 'l'Exécutif des Musulmans de Belgique' (*C.R.I.*, Chambre, 2021-2022, 16 décembre 2021, PLEN 148, p. 15, Q. nºs 2131P et 2143P)

Questions jointes K. Metsu et B. Pas au ministre de la Justice sur 'la communication d'informations erronées au Parlement' (*C.R.I.*, Chambre, 2021-2022, 16 décembre 2021, PLEN 148, p. 15, Q. nºs 206I et 214I)

Question de S. Cogolati à la ministre de la Fonction publique sur 'les risques de censure et cybersurveillance sur les smartphones Huawei, Xiaomi et One Plus' (*Q.R.*, Chambre, 2021-2022, 16 décembre 2021, nº 72, p. 180, Q. nº 349)

Question de S. Creyelman à la ministre de la Défense sur 'le développement de la composante Cyber au sein de la Défense' (*Q.R.*, Chambre, 2021-2022, 16 décembre 2021, nº 72, p. 228, Q. nº 346)

Question de Th. Francken à la ministre de l'Intérieur sur 'la vérification lors de l'opération d'évacuation' (*Q.R.*, Chambre, 2021-2022, 16 décembre 2021, nº 72, p. 335, Q. nº 386)

Question de G. Dallemagne à la ministre de l'Intérieur sur 'le rapport annuel de la Sûreté de l'État' (*C.R.I.*, Chambre, 2021-2022, 20 décembre 2021, COM 645, p. 2, Q. nº 22634C)

Question de K. Bury au ministre de la Justice sur 'l'achat d'immeubles de bureaux dans le quartier Nord à Bruxelles' (*C.R.I.*, Chambre, 2021-2022, 20 décembre 2021, COM 645, p. 26, Q. nº 23267C)

Rapport d'activités 2021
Activiteitenverslag 2021

Comité Permanent R
Vast Comité I

Comité Permanent de Contrôle des
services de renseignement et de sécurité

Vast Comité van Toezicht op
de inlichtingen- en veiligheidsdiensten

ACTIVITEITENVERSLAG 2021
RAPPORT D'ACTIVITÉS 2021

Quis custodiet ipsos custodes ?

Quis custodiet ipsos custodes? is een publicatiereeks die een bijdrage wil leveren tot het bevorderen van een geïnformeerde discussie over de werking, de bevoegdheden en de controle op de inlichtingen- en veiligheidsdiensten en op het inlichtingenwerk. In deze reeks worden o.m. wetenschappelijke studies, de activiteitenverslagen van het Vast Comité I en verslagboeken van colloquia opgenomen.

Redactie

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Leuvenseweg 48 bus 4, 1000 Brussel (02 286 29 88).

Reeds verschenen in deze reeks

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Vast Comité I, *Activiteitenverslag 2006,* 2007, 147 p.
3) Vast Comité I, *Activiteitenverslag 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, 2010, 220 p.
5) Vast Comité I, *Activiteitenverslag 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Vast Comité I, *Activiteitenverslag 2009,* 2010, 127 p.
8) Vast Comité I, *Activiteitenverslag 2010,* 2011, 119 p.
9) Vast Comité I, Activiteitenverslag 2011, 2012, 134 p.
10) W. Van Laethem en J. Vanderborght (eds), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, 2013, 565 p.
11) Vast Comité I, *Activiteitenverslag 2012*, 2013, 115 p.
12) Vast Comité I, *Activiteitenverslag 2013*, 2014, 210 p.
13) Vast Comité I, *Activiteitenverslag 2014*, 2015, 135 p.
14) Vast Comité I, *Activiteitenverslag 2015*, 2016, 132 p.
15) Vast Comité I, *Activiteitenverslag 2016*, 2017, 230 p.
16) Vast Comité I, *Activiteitenverslag 2017*, 2018, 152 p.
17) Vast Comité I, *Activiteitenverslag 2018*, 2019, 166 p.
18) J. Vanderborght (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, 2019, 151 p.
19) Vast Comité I, *Activiteitenverslag 2019*, 2020, 148 p.
20) Vast Comité I, *Activiteitenverslag 2020*, 2021, 189 p.
21) Vast Comité I, *Activiteitenverslag 2021*, 2022, 241 p.

ACTIVITEITENVERSLAG 2021

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de
inlichtingen- en veiligheidsdiensten

Voorliggend *Activiteitenverslag 2021* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 25 mei 2022.

(*getekend.*)
Serge Lipszyc, voorzitter
Pieter-Alexander De Brock, raadsheer
Thibaut Vandamme, raadsheer
Frédéric Givron, griffier

Activiteitenverslag 2021
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Alle rechten voorbehouden. Behoudens uitdrukkelijk bij wet bepaalde uitzonderingen mag niets uit deze uitgave worden verveelvoudigd, opgeslagen in een geautomatiseerd gegevensbestand of openbaar gemaakt, op welke wijze ook, zonder de uitdrukkelijke voorafgaande toestemming van de uitgevers.

Ondanks alle aan de samenstelling van de tekst bestede zorg, kunnen noch de auteurs noch de uitgever aansprakelijkheid aanvaarden voor eventuele schade die zou kunnen voortvloeien uit enige fout die in deze uitgave zou kunnen voorkomen.

INHOUD

Lijst met afkortingen ..... *xi*

Woord vooraf ..... *xv*

HOOFDSTUK I. **1**
DE TOEZICHTONDERZOEKEN **1**
I.1. Het OCAD en de ondersteunende diensten (opvolging) 2
I.1.1. De opvolging van de aanbevelingen door Douane en Accijnzen 3
I.1.2. De opvolging van de aanbevelingen door de FOD Mobiliteit en Vervoer 4
I.1.3. Conclusie 4
I.2. Het OCAD en de 'bijkomende' ondersteunende diensten 5
I.2.1. De informatiestroom tussen het OCAD en de vier 'bijkomende' ondersteunende diensten 5
I.2.1.1. FOD Binnenlandse Zaken – Algemene Directie Crisiscentrum 6
I.2.1.2. FOD Justitie – Directoraat-generaal Penitentiaire Inrichtingen 7
I.2.1.3. FOD Financiën – Algemene Administratie van de Thesaurie 8
I.2.1.4. FOD Justitie – Directoraat-generaal Wetgeving en Fundamentele rechten en Vrijheden – Dienst Erediensten en Vrijzinnigheid 8
I.2.2. Vaststellingen en conclusies 9
I.3. De uitwisseling van informatie over een werknemer tussen inlichtingendiensten en een private- of publieke werkgever 10
I.3.1. Het algemene kader 11
I.3.2. De werkgever wil een veiligheidsscreening 11
I.3.2.1. De wettelijke basis voor veiligheidsscreenings 11
I.3.2.2. Artikel 19, eerste lid, eerste zinsnede W.I&V 12
I.3.3. De werkgever is het voorwerp van een (vermeende) dreiging 13
I.3.3.1. Artikel 19, eerste lid, laatste zinsnede W.I&V 13
I.3.3.2. Een nadere uitwerking van deze regeling in een richtlijn? 13
I.3.3.3. Limieten gesteld door de Inlichtingenwet 14
I.3.3.4. Wat mag of moet worden meegedeeld? 16
I.3.4. Conclusies 18

I.4. Ernstige tekortkomingen aangaande de Nationale Veiligheid 19
I.5. De opvolging van schadelijke sektarische organisaties en criminele organisaties 20
I.5.1. Contextualisering 21
I.5.1.1. De schadelijke sektarische organisaties 21
I.5.1.2. Criminele organisaties 22
I.5.2. De materiële bevoegdheid 22
I.5.3. De procedurele bevoegdheid 23
I.5.4. De beleidsprioriteiten 24
I.5.5. De toegelaten beleidsruimte 25
I.5.6. De organisatorische vertaling van de beleidsprioriteiten 26
I.5.7. Nood aan versterking en een breder maatschappelijk debat ... 27
I.6. Aandacht van de Belgische inlichtingendiensten voor een ADIV-medewerker en zijn relaties met Russische burgers 28
I.7. Veiligheidsscreenings van militairen en burgerpersoneel bij Defensie. 29
I.7.1. De screening van militairen en burgers bij Defensie 29
I.7.2. Een veiligheidsscreening voor de (buitenlandse) studenten van de Koninklijke Militaire School? 31
I.8. De opvolging van politieke mandatarissen 32
I.8.1. Introductie 32
I.8.2. Vaststellingen aangaande de uitvoering van de aanbevelingen van het Vast Comité I 33
I.8.2.1. De uitwerking van richtlijnen met betrekking tot de inwinning, de verwerking, de raadpleging, de opslag en de archivering van gegevens 33
I.8.2.2. Bijzondere aandacht voor de positie van de vermelde politieke mandatarissen 35
I.8.2.3. De uitwerking van artikel 19 W.I&V 36
I.8.3. De collecte, de analyse en de verspreiding van inlichtingen over politieke mandatarissen tussen 2019 en 2020 36
I.8.3.1. Collecte en analyse 36
I.8.3.2. De verspreiding van inlichtingen 37
I.8.4. Respect voor de grondrechten van politieke mandatarissen ... 37
I.9. Het opsporen en opvolgen van de radicalisering van een militair: de zaak-Jürgen Conings 38
I.9.1. Een beeld van de professionele loopbaan van Jürgen Conings 39
I.9.2. Het juridisch en beleidsmatig kader 40
I.9.2.1. De inlichtingenopdracht van de VSSE en de ADIV ... 40
I.9.2.2. Het uitvoeren van veiligheidsscreenings door de twee inlichtingendiensten 42

I.9.2.3. De verantwoordelijkheid van de ADIV inzake militaire veiligheid 42
I.9.3. Onderzoeksvaststellingen 43
I.9.3.1. De informatiepositie van de VSSE 43
I.9.3.2. De informatiepositie van de ADIV 44
I.9.3.3. Gebrekkige communicatie 46
I.9.3.4. De 'watchlist extreemrechts' 48
I.9.3.5. De opeenvolgende veiligheidsmachtigingen van Jürgen Conings 49
I.9.3.6. De opdracht van de veiligheidsofficier 50
I.9.3.7. Het wapendepot en de rol van de ADIV 50
I.9.4. Conclusies 51
I.10. De rol van het OCAD in de opvolging van de militair Jürgen Conings 52
I.10.1. Analyse van het wettelijk kader 52
I.10.2. Het OCAD en de gemeenschappelijke gegevensbanken 53
I.10.2.1. De inschrijvingsprocedure 55
I.10.2.2. De informatie-uitwisseling met de partners 56
I.10.3. De rol van het OCAD in de opvolging van Jurgen Conings: de opname in de gemeenschappelijke gegevensbank 57
I.10.4. Informatieuitwisseling 57
I.10.5. Conclusies 59
I.11. De opvolging van een regeringscommissaris door de VSSE 59
I.11.1. Een nota van de veiligheid van de Staat 59
I.11.2. Onderzoeksvaststellingen 60
I.11.2.1. Een vernieuwde aandacht voor de Moslimbroederschap (en Ihsane Haouach)? 60
I.11.2.2. Het zorgvuldigheidsbeginsel 61
I.11.2.3. Geen verdere onderzoeksbevindingen? 61
I.11.2.4. Het lekken van een geclassificeerde nota 62
I.11.2.5. Een 'verstoringsactie'? 62
I.11.2.6. De noodzaak van een screening voor functies met een openbaar karakter? 63
I.12. Een vernieuwde aandacht voor de Moslimbroederschap 63
I.12.1. De Moslimbroeders: contextualisering 64
I.12.1.1. Ontstaan en internationalisering van de beweging 64
I.12.1.2. De omvang van het fenomeen in België? 64
I.12.1.3. Een beweging die in het buitenland als een bedreiging wordt beschouwd? 65
I.12.2. Onderzoeksvaststellingen 66
I.12.2.1. Maakt de beweging voorwerp van opvolging uit door de inlichtingendiensten? 66
I.12.2.2. Wordt de beweging geïdentificeerd als een bedreiging voor België? 67
I.12.2.3. Samenwerking 68

I.12.2.4. Welke strategieën hanteren de inlichtingendiensten om de geïdentificeerde dreiging in te dammen? 69
I.13. Informatie- en communicatietechnologie in het inlichtingenproces bij de Directie Cyber van de ADIV en bij de VSSE 70
I.13.1. De *core business* van een inlichtingendienst 70
I.13.2. De ICT-omgeving en -organisatie bij de Directie Cyber van de ADIV 72
I.13.2.1. Context 72
I.13.2.2. Evaluatie van de risico's 74
I.13.3. De ICT-omgeving en -organisatie bij de VSSE 75
I.13.3.1. Context 75
I.13.3.2. Evalutie van de risico's 78
I.14. Toezichtonderzoeken waar in de loop van 2021onderzoeksdaden werden gesteld en onderzoeken die in 2021 werden opgestart 78
I.14.1. De toepassing van nieuwe (bijzondere) inlichtingenmethoden 78
I.14.2 de opvolging van vrijgelaten terro-veroordeelden door de VSSE 79
I.14.3. Het risico op infiltratie bij de twee inlichtingendiensten 80
I.14.4. Mogelijke dreigingen voor het Belgische wetenschappelijk en economisch potentieel (PRISM/ WEP): opvolgonderzoek 80
I.14.5. Spionage via gemanipuleerde codeerapparatruur: de operatie Rubicon 82
I.14.6. (bijkomende) inlichtingencapaciteiten voor de Belgische inlichtingendiensten in het buitenland 82
I.14.7. Controle op de speciale fondsen: opvolgonderzoek 83
I.14.8. Onderzoek naar de opvolging door de inlichtingendiensten van 'des mouvements sectaires à obédience religieuse ayant des visées politiques' 84

HOOFDSTUK II. 85
DE CONTROLE OP DE BIJZONDERE EN BEPAALDE GEWONE INLICHTINGENMETHODEN 85
II.1. Cijfers met betrekking tot de bijzondere en bepaalde gewone methoden 86
II.1.1. Algemene trends 86
II.1.1.1. Inzet van bijzondere inlichtingenmethoden door de VSSE en de ADIV 86
II.1.1.2. De inzet van gewone methoden plus, in het bijzonder artikel 16/2 W.I&V 89
II.1.1.3. Gevolgen van de vernietiging van de Dataretentiewet? 91

II.1.2. Methoden aangewend door de ADIV 92
II.1.2.1. Gewone methoden 'plus' 92
II.1.2.2. De specifieke methoden 94
II.1.2.3. De uitzonderlijke methoden 95
II.1.2.4. De opdrachten en de dreigingen die de inzet van (de gewone en) bijzondere methoden rechtvaardigen 96
II.1.3. Methoden aangewend door de VSSE 99
II.1.3.1. De gewone methoden 'plus' 99
II.1.3.2. De specifieke methoden 100
II.1.3.3. De uitzonderlijke methoden 102
II.1.3.4. De opdrachten en de dreigingen die de inzet van (de gewone en) bijzondere methoden rechtvaardigen 103
II.2. De activiteiten van het Vast Comité I als (jurisdictioneel) controleorgaan en als prejudicieel adviesverlener 105
II.2.1. Controle op bepaalde gewone methoden 105
II.2.1.1. Algemeen 105
II.2.2. Controle op bijzondere methoden 106
II.2.2.1. De cijfers 106
II.2.2.2. De rechtspraak 110
II.3. Algemene vaststellingen 117

HOOFDSTUK III. 119
HET TOEZICHT OP BUITENLANDSE INTERCEPTIES, BEELDOPNAMEN EN IT-INTRUSIES 119
III.1. De bevoegdheden van de ADIV en de controletaak van het Vast Comité I 119
III.2. Het in 2021 verrichte toezicht 121
III.2.1. Het toezicht voorafgaand aan de interceptie, intrusie of opname 121
III.2.2. Het toezicht tijdens de interceptie, intrusie of opname 121
III.2.3. Het toezicht na de uitvoering van de methode 122

HOOFDSTUK IV. 123
HET VAST COMITÉ I ALS BEVOEGDE TOEZICHTHOUDENDE AUTORITEIT IN HET KADER VAN DE VERWERKING VAN PERSOONSGEGEVENS 123
IV.1. Inleiding 123
IV.2. De behandeling van individuele verzoeken 124
IV.3. Adviesverlening 127
IV.4. De melding van een mogelijke data breach 128
IV.5. Evaluatie van de Gegevensbeschermingswet 129

HOOFDSTUK V. 131
DE CONTROLE VAN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN 131
V.1. De controleopdracht en het voorwerp van controle 131

V.2. Onderzoeksvaststellingen 132
V.2.1. Het gebrek aan toegang van de NVO 132
V.2.2. De opvolging van de vroegere aanbevelingen 133
V.2.2.1. Aanbevelingen waaraan gevolg werd gegeven.....133
V.2.2.2. Aanbevelingen waaraan geen gevolg werd gegeven .134
V.2.2.3. Aanbevelingen waaraan deels gevolg werd gegeven.134
V.2.3. Nieuwe aanbevelingen 136
V.3. De adviesopdracht 136

HOOFDSTUK VI. 139
ADVIEZEN 139
VI.1. Advies over de oprichting van een federaal inlichtingenagentschap .. 140
VI.2. Advies over het instellen van een actieve kennisgevingsplicht voor de inlichtingendiensten 140
VI.2.1. De actieve notificatie..... 141
VI.2.2. De passieve notificatie 144
VI.3. Advies over dataretentie..... 144
VI.3.1. Wijzigingen aan de Inlichtingenwet 145
VI.3.1.1. Gerichte bewaring van verkeers- en lokalisatiegegevens 145
VI.3.1.2. Toegang tot verkeers- en lokalisatiegegevens 146
VI.3.1.3. Algemene en ongedifferentieerde bewaring van verkeers- en lokalisatiegegevens.....146
VI.3.1.4. Verplichte kennisgeving aan de operatoren.....147
VI.3.2. Wijzigingen aan de telecomwet (WEC) 148
VI.4. Advies over het voorontwerp van wet tot wijziging van de Inlichtingenwet..... 148
VI.4.1. Een te complexe regelgeving..... 149
VI.4.2. Cybersecurity - opdracht van de ADIV 149
VI.4.3. Het plegen van ondersteunende misdrijven 150
VI.4.3.1. Algemeen.....150
VI.4.3.2. Lacune binnen de strafprocedure.....151
VI.4.3.3. Het plegen van misdrijven door agenten 151
VI.4.3.4. Het plegen van misdrijven door informanten.....152
VI.4.3.5. Schade opgelopen of veroorzaakt door een menselijke bron.....152
VI.4.3.6. Onvoldoende rechtsbescherming voor de menselijke bron.....152
VI.4.4. Fictieve identiteit en hoedanigheid: als ondersteuningsmaatregel bij een inlichtingenmethode of louter om veiligheidsredenen 153
VI.4.5. Infiltratie in de reële en virtuele wereld..... 153
VI.4.6. Gewone methoden plus..... 154
VI.4.7. Vorderen van financiële gegevens 155
VI.4.8. Personele en financiële middelen..... 155

VI.5. Advies over de strafbaarstellingen ter bevordering van de democratische weerbaarheid 155
VI.5.1. Voorafgaande observatie 156
VI.5.2. Samenwerking en uitwisseling van informatie met gerechtelijke actoren 157
VI.5.3. Samenwerking en uitwisseling van informatie met bestuurlijke actoren 157
VI.6. Gemeenschappelijk advies op het voorontwerp van wet tot wijziging van de OCAD-Wet 158
VI.6.1. Uitbreiding van de lijst van ondersteunende diensten 158
VI.6.2. Wijzigingen van de benoemingsvoorwaarden voor directeur en adjunct-directeur 160
VI.6.3. Uitbreiding van de opdrachten van het OCAD 160
VI.6.3.1. Het coördineren van de globale aanpak tegen dreigingen 160
VI.6.3.2. Nieuwe opdrachten voor het OCAD van de Nationale Veiligheidsoverheid? 161
VI.6.4. Mededeling en consultatie van evaluaties 162
VI.6.5. Mededeling en consultatie van inlichtingen van gerechtelijke aard onder embargo 162
VI.6.6. Mededeling en consultatie van inlichtingen bedoeld in artikel 12, 1ste lid W.OCAD 163

HOOFDSTUK VII. 165
DE OPSPORINGS- EN GERECHTELIJKE ONDERZOEKEN 165

HOOFDSTUK VIII. 167
EXPERTISE EN EXTERNE CONTACTEN 167
VIII.1. Expert op diverse fora 167
VIII.2. Samenwerkingsprotocol met de Federale Ombudsmannen 168
VIII.3. Partnership met het Federaal Instituut Mensenrechten 169
VIII.4. Een multinationaal initiatief inzake internationale informatie-uitwisseling 169
VIII.5. Contacten met buitenlandse toezichthouders 170

HOOFDSTUK IX. 171
HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN 171
IX.1. Het activiteitenverslag van het Beroepsorgaan 171
IX 1.1. Inleiding 171
IX.1.2. Gedetailleerde cijfers 172
IX.2. Opmerkingen en suggesties van de voorzitter van het Beroepsorgaan 182
IX.2.1. Een bijzondere en complexe procedure 182
IX.2.2. Beslissing van de Raad van State 185
IX.2.3. Aansprakelijkheid van het Beroepsorgaan 185
IX.2.4. Twee kwesties met betrekking tot artikel 6 van het Europees Verdrag voor de Rechten van de Mens (EVRM) ... 186
IX.2.4.1. De publicatie 186

IX.2.4.2. De openbaarheid van de zittingen 188
IX.2.5. De doeltreffendheid van de beslissingen van het Beroepsorgaan 190
IX.2.6. Vooruitzichten 191

HOOFDSTUK X. 193
DE INTERNE WERKING VAN HET VAST COMITÉ I 193
X.1. Samenstelling van het Vast Comité I 193
X.2. Een welzijnsaudit op het Comité 194
X.3. Vergaderingen met de Begeleidingscommissie 195
X.4. Gemeenschappelijke vergaderingen met het Vast Comité P 196
X.5. Een aanzienlijke aandacht vanuit de media 197
X.6. De *Data Protection Officer* op het Comité 198
X.7. Financiële middelen en beheersactiviteiten 198
X.8. Implementatie van de aanbevelingen van de audit van het Rekenhof 200
X.9. Vorming 201

HOOFDSTUK XI. 203
AANBEVELINGEN 203
XI.1. Aanbevelingen in verband met de bescherming van de rechten die de Grondwet en de wet aan personen waarborgen 203
XI.1.1. Uitwerken van een voorstel van richtlijn i.v.m. medeling van informatie door de VSSE of de ADIV aan werkgevers en aanpassing van bestaande richtlijnen 203
XI.1.2. Richtlijnen inzake de opvolging van politieke mandatarissen 204
XI.2. Aanbevelingen in verband met de coördinatie en de efficiëntie van de inlichtingendiensten, het OCAD en de ondersteunende diensten 204
XI.2.1. Aanbevelingen m.b.t. Het OCAD en zijn (nieuwe) ondersteunende diensten 204
XI.2.2. Correcte toepassing van de mogelijkheid om veiligheidsscreenings aan te vragen 206
XI.2.3. Verplichte melding naar werkgever in geval van opname in een gemeenschappelijke gegevensbank 206
XI.2.4. Een breed debat over de taken en de prioriteiten van de inlichtingendiensten 206
XI.2.5. Meer veiligheidsscreenings van militairen en burgerpersoneel bij Defensie 207
XI.2.6. De oprichting van een coherent 'intelligence' geheel 208
XI.2.7. Stabiliteit in het personeelsbeleid bij de ADIV 208
XI.2.8. Bekrachtiging inlichtingen- (en veiligheids-) stuurplan 208
XI.2.9. Betere interne communicatie binnen ADIV 209
XI.2.10. Betere communicatie tussen ADIV en andere overheden bij tucht- of strafbare feiten 209
XI.2.11. Betere interne communicatie door ADIV naar Commando en MOD 209

XI.2.12. Actievere opvolging van extremisme binnen Defensie door de ADIV 209
XI.2.13. Evaluatie van het Nationaal Strategisch Inlichtingenplan (NSIP) 210
XI.2.14. Betere regels en kennis inzake opname entiteit in de gemeenschappelijke gegevensbank 210
XI.2.15. Informatieuitwisseling tussen de inlichtingendiensten over Defensiepersoneel 211
XI.2.16. Naleving Humint-afspraken 211
XI.2.17. Naleving informatieoverdracht naar het OCAD 211
XI.2.18. Een flexibel en proactief rekruteringsbeleid voor de inlichtingendiensten 211
XI.2.19. Een kwalitetisvolle digitale omgeving 212
XI.2.20. Een uniforme methodologie inzake dreigingsevaluatie in de inlichtingensector 212
XI.2.21. Het belang van diverse reglementen 212
XI.2.22. Tuchtrechtelijk gezag over het burgerpersoneel ADIV 213
XI.2.23. Inzet inlichtingenmethoden 213
XI.2.24. Aanwerving juristen 213
XI.2.25. Investeren in management 213
XI.2.26. Verduidelijking counterintelligence binnen ADIV 214
XI.2.27. Werking veiligheidsofficieren binnen ADIV 214
XI.2.28. Vaststelling radicaliseringsindicatoren door ADIV 214
XI.2.29. Wederzijds zicht op opgevolgde entiteiten door VSSE en ADIV 214
XI.2.30. Middelen in de strijd tegen extremisme 214
XI.2.31. Actualisering bestaande reglementeringen 215
XI.2.32. Cumul binnen Defensie 215
XI.2.33. Werking van de Gemeenschappelijke gegevensbanken binnen de ADIV 215
XI.2.34. Melding en opvolging veiligheidsincidenten binnen de ADIV 216
XI.2.35. Samenwerking veiligheidsbureaus ADIV en VSSE 216
XI.2.36. Coherent gebruik van dreigingsniveaus en communicatie van evaluaties door het OCAD 216
XI.2.37. Schriftelijke communicatie bij toepassing van artikel 19 W.I&V 217
XI.2.38. Omgang met geclassificeerde informatie door derde overheden 217
XI.2.39. Veiligheidsscreenings voor vertrouwensfuncties 218
XI.2.40. Vermelding ontvangers op uitgaande nota's 218
XI.2.41. Het meedelen van de behoeften van de Nationale Veiligheidsraad aan de inlichtingendiensten 219
XI.2.42. Samenwerking in het kader van de problematiek van de Moslimbroeders 219

XI.2.43. Analyse van de middelen van ADIV m.b.t. de problematiek van de moslimbroeders 219
XI.2.44. Algemene bewustmaking m.b.t. de problematiek van de Moslimbroeders 220
XI.2.45. Bewustmaking veiligheidsofficieren Defensie m.b.t. de problematiek van de Moslimbroeders 220
XI.2.46. ICT in het inlichtingenproces bij de Directie Cyber van de ADIV 220
XI.3. Aanbevelingen in verband met de doeltreffendheid van het toezicht. 221
XI.3.1. Melding door de ADIV van de opvolging van politieke mandatarissen 221

BIJLAGEN 223

BIJLAGE A. 223
Overzicht van de belangrijkste regelgeving met betrekking tot de werking, de bevoegdheden en het toezicht op de inlichtingen- en veiligheidsdiensten en het OCAD (1 januari 2021 tot 31 december 2021) 223

BIJLAGE B. 226
Overzicht van de belangrijkste wetsvoorstellen, wetsontwerpen, resoluties, orde moties en parlementaire besprekingen met betrekking tot de werking, de bevoegdheden en het toezicht op de inlichtingen- en veiligheidsdiensten en het OCAD (1 januari 2021 tot 31 december 2021) 226

BIJLAGE C 229
Overzicht van interpellaties, vragen om uitleg en mondelinge en schriftelijke vragen met betrekking tot de werking, de bevoegdheden en het toezicht op de inlichtingen- en veiligheidsdiensten en het OCAD (1 januari 2021 tot 31 december 2021) 229

LIJST MET AFKORTINGEN

ADIV	Algemene Dienst Inlichting en Veiligheid
AG	Administrateur-generaal (VSSE)
ANG	Algemene Nationale Gegevensbank
AVG	Algemene Verordening Gegevensbescherming
BCP	*Business continuity plan*
BELPIU	*Belgian Passenger Information Unit*
BIM	Bijzondere inlichtingenmethoden
BIM-Commissie	Bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door inlichtingen- en veiligheidsdiensten
BIM-Wet	Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten
BINII	*Belgian Intelligence Network Information Infrastructure*
BS	Belgisch Staatsblad
BTA	Bevoegde Toezichthoudende Autoriteit
Cama	*Case Manager*
CCB	Centrum voor Cybersecurity Belgium
CCIRM	*Collection Coordination Information Requirement Management* (ADIV)
CCIV	Coördinatiecomité Inlichtingen en Veiligheid
CI	*Counterintelligence*
CIA-model	Confidentiality, Integrity & Availability-model
CMDB	*Component Management Database*
CMRO	Commissie voor de Modernisering van de Rechterlijke Orde
COC	Controleorgaan voor de politionele informatie
Coma	*Collection Manager*
CRAB	Compte Rendu Analytique – Beknopt Verslag
CRIV	Compte Rendu Intégral – Integraal Verslag
DG EPI	Directoraat-generaal Penitentiaire Inrichtingen
DISCC	*Defense Intelligence and Security Coordination Centre* (ADIV)
DJSOC/Terro	Directie van de bestrijding van de zware en georganiseerde criminaliteit (afdeling terrorisme) van de Federale Gerechtelijke Politie
DPA	*Data Protection Authority*
DPO	*Data Protection Officer*

DRI	Directie van de politionele informatie en de ICT-middelen (Federale politie)
DRMB	Dienst voor Religieuze en Morele Bijstand
DRP	*Disaster recovery plan*
DVZ	Dienst Vreemdelingenzaken
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
FIRM	Federale Instituut voor de bescherming en de bevordering van de rechten van de mens
FOD	Federale overheidsdienst
FTF	*Foreign terrorist fighters*
GBA	Gegevensbeschermingsautoriteit
GBA-Wet	Wet van 3 december 2017 tot oprichting van de gegevensbeschermingsautoriteit
GBW	Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (Gegevensbeschermingswet)
GGB	Gemeenschappelijke gegevensbanken
GGB HP	Gemeenschappelijke gegevensbank 'Haatpropagandisten'
GGB TF	Gemeenschappelijke gegevensbank 'Terrorist Fighters'
HTF	*Homegrown terrorist fighters*
Hand.	Handelingen
HP	Haatpropagandisten
HUMINT	*Human intelligence*
HvJEU	Hof van Justitie van de Europese Unie
ICT	Informatie- en communicatietechnologie
IOWG	*Intelligence Oversight Working Group*
JDC	*Joint Decision Centre*
JIC	*Joint Intelligence Centre*
K.B.	Koninklijk besluit
KB C&VM	Koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheids-machtigingen, veiligheidsattesten en veiligheidsadviezen
KB FTF	Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van hoofdstuk IV van de Wet op het politieambt
KB TF	Koninklijk besluit van 23 april 2018 tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' en tot uitvoering van sommige bepalingen van de afdeling 1*bis* 'Het informatiebeheer' van

	hoofdstuk IV van de Wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank 'Foreign Terrorist Fighters' naar de gemeenschappelijke gegevensbank 'Terrorist Fighters'
KB HP	Koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis 'Het informatiebeheer' van hoofdstuk IV van de WPA
KB OCAD	Koninklijk besluit van 28 november 2006 tot uitvoering van de Wet van10 juli 2006 betreffende de analyse van de dreiging
KMS	Koninklijke Militaire School
LIVC-R	Lokale integrale veiligheidscel - radicalisme
LTF	*Local task force*
M.B.	Ministerieel besluit
MOD	Minister van Defensie
MoU	*Memorandum of Understanding*
MPLUS	Gewone methoden plus
NA	*Note aux autorités*
NAVO	Noord-Atlantische Verdragsorganisatie
NSIP	Nationaal Strategisch Inlichtingenplan
NTSU-CTIF	*National Technical & Tactical Support Unit – Central Technical Interception Facility* (geïntegreerde politie)
NVO	Nationale Veiligheidsoverheid
NVR	Nationale Veiligheidsraad
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OSINT	*Open sources intelligence*
Parl. St.	Parlementaire Stukken van Kamer en Senaat
PGE	Potentieel gewelddadige extremisten
Plan R	Actieplan Radicalisme
Platform CT	Gemeenschappelijk contraterrorisme-platform
PNR-Wet	Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens
PROTEUS	Gegevensbank OCAD
RFC	*Requests for Collect*
RFI	*Request for information*
SIGINT	*Signals intelligence*
SOP	*Standard Operating Procedures*
TA	Toezichthoudende autoriteiten
TF	*Terrorist fighters*
TV	Terrorisme-veroordeelden
Vast Comité I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten
Vr. en Antw.	Schriftelijke vragen en antwoorden (Kamer of Senaat)

VSSE	Veiligheid van de Staat
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veilig-heidsattesten en veiligheidsadviezen
W.C&VM	Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheids-adviezen
WEC	Wet van 13 juni 2005 betreffende de elektronische communicatie
W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
W.OCAD	Wet van 10 juli 2006 betreffende de analyse van de dreiging
WOB	Wet van 11 april 1994 betreffende de openbaarheid van bestuur
WPA	Wet van 5 augustus 1992 op het politieambt
W.Toezicht	Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse

WOORD VOORAF

Het jaar 2021 herinnerde ons eraan hoe kwetsbaar de planeet is, hoe kwetsbaar samenlevingen zijn, hoezeer de democratie op de proef wordt gesteld en hoe precair de rechten van de burgers zijn.

Het verschijnsel van potentieel gewelddadige extremisten - religieus of ideologisch - wordt verder in de hand gewerkt door aanvallen op bepaalde instellingen. Deze aanvallen hebben de instellingen blijvend verzwakt. De aanslag op het Capitool in Washington is ongetwijfeld het meest opvallende voorbeeld van het afwijzen van democratische instellingen. Zou een dergelijk scenario geen gevolgen kunnen hebben voor onze Belgische instellingen?

Dit soort dreiging is verre van verdwenen. Het wordt integendeel versterkt door de sociale media. Zo werden er veel samenzweringstheorieën over COVID-19 verspreid. Hoewel de basis al eerder was gelegd, bleek de pandemie het perfecte voorwendsel om bevolkingsgroepen verder tegen elkaar op te zetten.

Staatsgrepen en het omverwerpen van de 'machthebbers' verplichten ons vandaag, net als in het verleden, om in te grijpen en zelfs onze landgenoten zo nodig te repatriëren. Deze betrachting om te beschermen vereist een versterking van de inzet van onze inlichtingen- en veiligheidsdiensten in het buitenland.

Het proces dat volgde op de aanslagen in Parijs, net zoals het proces in Antwerpen na de verijdelde aanslag in Villepinte, herinneren er ons ook aan dat de inlichtingendiensten hun partnerschap moeten versterken en de gezamenlijke strijd tegen het terrorisme moeten opvoeren.

In België vormden kwesties in verband met jihadistische bewegingen een vruchtbare voedingsbodem voor de toenemende polarisatie van de samenleving. Ook het onderzoeksverslag over het toezicht op extreemrechts heeft zijn relevantie bewezen. Het onderzoek van het Comité heeft, naar aanleiding van de zoektocht naar een gewapende militair die onze instellingen bedreigde, aangetoond hoe kwetsbaar sommige van onze instellingen zijn ten aanzien van dit verschijnsel, dat niet enkel onze buurlanden treft.

Wat onze inlichtingendiensten betreft, mogen wij niet vergeten dat ons land een kruispunt is voor vele Europese en internationale instellingen, alsook voor vele gemeenschappen en opposanten. Deze bijzondere situatie vereist een permanente investering in het versterken van de bescherming van de vermelde entiteiten en personen en ook in de strijd tegen buitenlandse inmenging.

De veiligheidsdiensten moeten worden aangemoedigd om proactiever op te treden en beter op elkaar in te spelen, om zo te streven naar een geconsolideerde en samenhangende Belgische inlichtingen- en veiligheidsgemeenschap. Ik steun Jaak Raes, administrateur-generaal van de Veiligheid van de Staat, in zijn streven om de 'need to know' te verzoenen met de 'need to share'.

Ik steun eveneens het project voor een geïntegreerd personeelsstatuut voor het personeel van de inlichtingen- en veiligheidsdiensten. Het is zonder twijfel een onontbeerlijke stap in de ontwikkeling van synergieën tussen de diensten. Ik roep op tot het optimaliseren van de middelen en het versterken van de beschikbare deskundigheid in de strijd tegen bedreigingen. Ik ben van mening dat het veiligheidsvraagstuk een meer duidelijke en ambitieuzere strategische visie van de Nationale Veiligheidsraad vereist op het vlak van de veiligheidsuitdagingen die ons door de constante wijziging van onze samenleving worden opgelegd.

Door de impact van COVID-19 werd de dagelijkse organisatie van het Comité grondig ontwricht. De continuïteit van de werkzaamheden kon alleen worden gewaarborgd dankzij het vastberaden en professioneel bewustzijn van ieder van ons. Onze medewerkers verdienen des te meer lof voor het feit dat zij slechts in beperkte mate gebruik hebben kunnen maken van telewerk. Wij beschikken nog steeds niet over het noodzakelijke beveiligde digitale netwerk om onze dagdagelijkse opdrachten naar behoren uit te voeren. De uitdagingen zijn talrijk, en het Comité wil er dan ook op een afdoende manier op reageren.

De noodzakelijke werkzaamheden op het gebied van synergie die door de Kamer zijn aangevat, stellen ons op heden in staat om de grondslagen ervan te zien. Logischerwijs roept dit nog steeds een aantal vragen en ongerustheid op, maar anderzijds geeft het ook aanleiding tot hoopvolle vooruitzichten. De versterking van het Comité als instelling blijft actueel, net zoals de vragen die zijn gerezen naar aanleiding van het openen van dossiers over het gebruik van *spyware*, het opvolgen van een imam en het volgen van veroordeelde terroristen… Ook al is onze instelling niet de enige, toch is het Vast Comité I een essentiële verdediging van onze rechtsstaat.

Dit jaar wuifden we Martine, Josiane, Wouter, Charles, Ludo, Frank, Jean-Philippe en Christophe uit. Ik wil graag deze medewerkers bedanken voor hun betrokkenheid.

Ik hoop dat het lezen van dit verslag bijdraagt tot een betere perceptie van ons werk en ik wens u een 'stimulerende' lezing!

25 mei 2022,
Serge Lipszyc,
Voorzitter van het Vast Comité van toezicht
Inlichtingen- en veiligheidsdiensten

HOOFDSTUK I.
DE TOEZICHTONDERZOEKEN

In 2021 finaliseerde het Vast Comité I tien toezichtonderzoeken, waarvan drie gezamenlijk met het Vast Comité van Toezicht op de politiediensten. Ook de drie informatiedossiers die werden besproken met de parlementaire Begeleidingscommissie, werden opgenomen in voorliggend hoofdstuk (I.4, I.6 en I.7).

Het zijn diverse instanties of personen die het Comité kunnen 'vatten' met een toezichtonderzoek: de Begeleidingscommissie, de voogdijministers, elke (rechts-) persoon die klacht of aangifte wenst te doen… Het Comité kan ook zelf het voortouw nemen: vijf van de tien in 2021 gefinaliseerde onderzoeken werden ambtshalve opgestart. Uitzonderlijk werden vier onderzoeken uitgevoerd op verzoek van de parlementaire Begeleidingscommissie. Slechts één toezichtonderzoek werd uitgevoerd op vraag van de minister van Defensie. Het Comité zette tevens zijn werkzaamheden voort in het kader van zeven in 2021 of eerder opgestarte onderzoeken. Een korte omschrijving van deze nog lopende en/of opgestarte onderzoeken, volgt in I.14. De naar aanleiding van de toezichtonderzoeken geformuleerde aanbevelingen werden gebundeld in Hoofdstuk XI.

In totaal ontving het Comité in 2021 75 klachten of aangiften.[1] Na een kort vooronderzoek en de verificatie van een aantal objectieve gegevens, wees het Comité 23 klachten of aangiften af omdat ze kennelijk niet gegrond waren[2] (art. 34 W.Toezicht) en in 28 gevallen bleek het Comité onbevoegd om de opgeworpen vraag te behandelen. In dat laatste geval werden de klagers doorverwezen naar de bevoegde instanties (bijv. de Brusselse procureur des Konings, het Vast Comité P of nog, de Gegevensbeschermingsautoriteit). 14 van de 24 van de klachten konden worden afgerond in 2021, tien klachten waren begin 2022 nog in behandeling. In 2021 werden 16 van de 24 klachten gehercategoriseerd als DPA-klacht.[3]

---

1 Eerst wordt de ontvankelijkheid bestudeerd en de klacht vervolgens gecategoriseerd ('gewone' klacht, DPA-klacht, BIM-klacht…). Indien zich een algemene probleemstelling voordoet, kan door het Comité worden beslist tot het openen van een toezichtonderzoek, zoniet blijft het onderzoek beperkt tot de klacht *an sich* (een klachtonderzoek).

2 Het Comité is bestemmeling van nogal wat klachten en aangiften van mensen met waanbeelden.

3 Zie hierover 'V.6. De behandeling van individuele verzoeken'.

I.1. HET OCAD EN DE ONDERSTEUNENDE DIENSTEN (OPVOLGING)

In juni 2020 rondde het Vast Comité I, samen met het Vast Comité P, een toezichtonderzoek af naar de ondersteunende diensten van het Coördinatieorgaan voor de dreigingsanalyse (OCAD).[4] Dit onderzoek had betrekking op vier ondersteunende diensten: de FOD Binnenlandse Zaken (Dienst Vreemdelingenzaken), de FOD Buitenlandse Zaken, de FOD Mobiliteit en Vervoer en de FOD Financiën (Administratie Douane en Accijnzen).[5] Het doel van het onderzoek was om de relaties tussen de vernoemde ondersteunende diensten en het OCAD te onderzoeken wat betreft de samenwerking en informatie-uitwisseling. Hierbij werd aandacht geschonken aan de rechtmatigheid, de doelmatigheid en de coördinatie van deze samenwerking en informatie-uitwisseling.

Teneinde een antwoord te kunnen bieden op de vragen vanuit de parlementaire Begeleidingscommissie naar een stand van zaken van de geïmplementeerde aanbevelingen uit dit onderzoek, werd begin juni 2020 door de Vaste Comités I en P besloten een opvolgingsonderzoek op te starten.[6]

Het initiële onderzoek had de naleving van de verwerkings- en bewaringsregels van geclassificeerde documenten alsook de goede informatiestromen tussen enerzijds de FOD Buitenlandse Zaken en de FOD Binnenlandse Zaken (Dienst Vreemdelingenzaken) en anderzijds het OCAD aangetoond.

In hun toezichtrapport formuleerden de Vaste Comités I en P een aantal specifieke aanbevelingen voor de FOD Financiën (Administratie Douane en Accijnzen) dat een plan had ontwikkeld om tegemoet te komen aan de verwachtingen gesteld aan de ondersteunende diensten. Als antwoord op de algemene conclusies en aanbevelingen van het rapport, had ook de FOD Mobiliteit en Vervoer getracht zijn samenwerking met het OCAD te verbeteren. Het opvolgonderzoek concentreerde zich dan ook op de maatregelen genomen door beide administraties.

---

4 Zie VAST COMITÉ I, *Activiteitenverslag 2020*, 2-11 ('I.1. De ondersteunende diensten van het OCAD').

5 De inlichtingen- en politiediensten vormden reeds eerder het voorwerp van een gemeenschappelijk toezichtonderzoek naar de ondersteunende diensten van het OCAD. Hierover VAST COMITÉ I, *Activiteitenverslag 2010*, 46 ('II.12.6. Mededeling van inlichtingen aan het OCAD door de ondersteunende diensten) en meer uitgebreid *Activiteitenverslag 2011*, 25-32 ('II.4. De informatiestromen tussen het OCAD en zijn ondersteunende diensten').

6 De resultaten van dit onderzoek werden in april 2021 in de Begeleidingscommissie besproken.

I.1.1. DE OPVOLGING VAN DE AANBEVELINGEN DOOR DOUANE EN ACCIJNZEN

In antwoord op de twee specifieke aanbevelingen geformuleerd in het toezichtrapport uit 2020, stelde de Algemene Administratie Douane en Accijnzen een actieplan op. Op het ogenblik van het afsluiten van het onderzoek (begin 2021) waren de meeste van de in het actieplan opgenomen maatregelen deels in uitvoering. Omwille van de gezondheidscrisis, konden een aantal acties nog niet worden gerealiseerd.

Een eerste specifieke aanbeveling bestond erin dat de dienst een interne analyse zou uitvoeren om te bepalen welke soort informatie die de administratie verzamelt, nuttig zou kunnen zijn voor het OCAD. Een eerste maatregel voorzag dan ook in het opstellen van een plan voor het verzamelen van gegevens op basis van indicatoren van extremisme of terrorisme. Er werd tevens een sensibiliseringsproject opgestart om het signaleren en delen van informatie aan te moedigen. Daartoe werden opleidingen voorzien, in het bijzonder over de indicatoren extremisme en terrorisme. De Administratie Douane en Accijnzen besliste tevens om een inventaris op te maken van de verschillende informatiebronnen waarover ze beschikt (informatie verkregen tijdens operationele activiteiten van de Administratie Operaties en de Administratie Opsporing, alsook informatie opgeslagen in andere interne gegevensbanken). In maart 2021 had de Administratie Opsporing van de Douane en Accijnzen nog altijd geen toegang tot de door het OCAD beheerde gemeenschappelijke gegevensbank.

Een tweede aanbeveling betrof het treffen van gepaste maatregelen om de minimumnormen met betrekking tot de bewaring en raadpleging van geclassificeerde documenten na te leven. Naast de aanschaf van nieuwe brandkoffers en de invoering van een volledig register voor geclassificeerde documenten, werd tevens een handboek voor de gebruikers van geclassificeerde informatie voorbereid door de veiligheidsofficier. Verder beperkte de Administratie Opsporing de toegang tot het BINII-lokaal (*Belgian Intelligence Network Information Infrastructure*, een communicatieplatform voor de uitwisseling van geclassificeerde informatie). Het actieplan voorzag tevens in de periodieke verificatie van de veiligheidsmachtigingen alsook in de organisatie van veiligheidsbriefings voor de houders van een veiligheidsmachtiging.

De Vaste Comités P en I stelden vast dat de Administratie Douane en Accijnzen een aantal acties had ondernomen en een aantal maatregelen had uitgewerkt die nodig waren om tegemoet te komen aan de aanbevelingen uit het initiële onderzoeksrapport.

I.1.2. DE OPVOLGING VAN DE AANBEVELINGEN DOOR DE FOD MOBILITEIT EN VERVOER

Niettegenstaande er in het gezamenlijk verslag van de Vaste Comités I en P geen specifieke aanbevelingen werden geformuleerd voor de FOD Mobiliteit en Vervoer, ontwikkelde ook deze steundienst een plan, vergezeld van een timing, om de doeltreffendheid van zijn activiteiten met het OCAD te verbeteren. In dat plan wordt enerzijds aandacht besteed aan sensibilisering via informatiesessies voor de interne diensten met betrekking tot de rol en de functie van het OCAD en van de Crisiscel van de FOD Mobiliteit en Vervoer. Er werden in 2020 diverse vergaderingen georganiseerd door deze crisiscel om de opdracht van de OCAD toe te lichten alsook de doelstellingen van de samenwerking, en dit met het oog op het identificeren van verbeter- en actiepunten. Zowat gelijktijdig en op het moment van het afsluiten van het toezichtonderzoek, was in de schoot van het FOD Mobiliteit en Transport een nieuwe informaticatool in ontwikkeling. Deze tool moet het beheer en de uitwisseling van informatie tussen het OCAD en de FOD vergemakkelijken.

Verder werd de nadruk gelegd op de uitbouw en de invoering van bevoorrechte kanalen voor het beheren en doorgeven van gegevens, zowel intern de FOD Mobiliteit en Vervoer als met externe diensten. In dat kader werd een handboek met procedures over het beheer van geclassificeerde documenten en het BINII-systeem intern gevalideerd.

De effecten van bovenvernoemde maatregelen kunnen pas mettertijd worden geëvalueerd. De crisiscel liet bij afloop van het onderzoek optekenen dat ze nog altijd veel te veel gegevens of evaluaties afkomstig van het OCAD krijgt, maar begrijpt dat het voor het OCAD moeilijk is om de doorgezonden informatie te filteren.

I.1.3. CONCLUSIE

Zowel de FOD Financiën, Douane en Accijnzen als de FOD Mobiliteit en Vervoer hebben actieplannen uitgewerkt om te voldoen aan de algemene besluiten en aanbevelingen uit het eindverslag van het voornoemde onderzoek. Deze verschillende maatregelen zouden het inderdaad mogelijk moeten maken om de veiligheid van de doorgezonden gegevens beter te garanderen, de informatiestroom te vergemakkelijken en binnen deze ondersteunende diensten te komen tot een betere kennis van het OCAD en zijn opdrachten.

I.2. HET OCAD EN DE 'BIJKOMENDE' ONDERSTEUNENDE DIENSTEN

Bij KB van 17 augustus 2018 werd de lijst van ondersteunende diensten van het OCAD uitgebreid met nog vier diensten, te weten het Nationaal Crisiscentrum, de Thesaurie, het Gevangeniswezen en de Dienst Erediensten en Vrijzinnigheid bij de FOD Justitie. Hoewel deze beslissing dateert van augustus 2018, maakten deze diensten nog geen deel uit van het eerste onderzoek[7] omdat het te vroeg was om de informatiestroom en de in dat kader geïmplementeerde processen te kunnen analyseren. Een nieuw met het Vast Comité P gemeenschappelijk toezichtonderzoek drong zich op.[8]

I.2.1. DE INFORMATIESTROOM TUSSEN HET OCAD EN DE VIER 'BIJKOMENDE' ONDERSTEUNENDE DIENSTEN

Het onderzoek had tot doel de relaties tussen de vier (bijkomende) ondersteunende diensten en het OCAD te bestuderen op het vlak van de doorgifte van informatie naar het OCAD en omgekeerd, alsook op het vlak van de wettelijkheid, de doeltreffendheid en de coördinatie.

Een kwantitatieve analyse van de uitwisseling gaf een eerste indruk van de informatiestromen tussen de steundiensten en het OCAD.

7 Zie VAST COMITÉ I, *Activiteitenverslag 2020*, 2-11 ('I.1. De steundiensten van het OCAD').

8 Ook hiervan werden de resultaten ter bespreking voorgelegd aan de parlementaire Begeleidings-commissie in april 2021.

	2019				
	TOTAAL	IN	OUT	RFI IN	RFI OUT
FOD Justitie - Dienst Erediensten en Vrijzinnigheid	**13**	8	5	8	0
FOD Justitie - Directoraat-generaal Penitentiaire Inrichtingen (DG EPI)	**2273**	2223	50	224	2
FOD Financiën - Algemene Administratie van de Thesaurie	**17**	14	3	7	0
FOD Binnenlandse Zaken - Algemene Directie Crisiscentrum (ADCC)	**2940**	1334	1606	7	8

Tabel 1: Cijfergegevens ontvangen van het OCAD. De gegevens "IN" zijn de inkomende gegevens bij het OCAD komende van de ondersteunende dienst en de gegevens "OUT" zijn de uitgaande gegevens van het OCAD naar de ondersteunende dienst.

De tabel[9] geeft de informatiestroom voor het jaar 2019 tussen het OCAD en de vier ondersteunende diensten weer. De diverse evaluaties vanuit het OCAD, maken geen deel uit van deze gegevens, met uitzondering deze verstuurd naar het Crisiscentrum, als eerste bestemmeling van de evaluaties.

I.2.1.1. FOD Binnenlandse Zaken – Algemene Directie Crisiscentrum

Door zijn opdrachten staat het Crisiscentrum (via zijn Directie *Incident & Crisis Management*) voortdurend in contact met het OCAD. Immers, het centrum bepaalt op basis van de dreigingsevaluaties gemaakt door het OCAD de te nemen maatregelen. In dat opzicht vinden er zeer vaak coördinatie- en veiligheidsvergaderingen plaats, en dit al voordat het Crisiscentrum als ondersteunende dienst werd opgenomen.

De informatiestroom van het OCAD naar het Crisiscentrum is de belangrijkste van de vier bijkomende steundiensten en betreft merendeel evaluaties. Het Crisiscentrum daartegen levert bijzonder weinig informatie aan, tenzij over evenementen of de komst van buitenlandse personaliteiten (bijv. door verzoeken om dreigingsevaluaties). De reden voor de aanwijzing tot steundienst is te vinden in

[9] Deze gegevens werden door het OCAD meegedeeld en werden getrokken uit de databank PROTEUS. Het gaat dus enkel om informatiestromen die door het OCAD relevant worden geacht. De cijfers houden geen rekening met verzoeken (of uitwisselingen) die niet ingevoerd zijn in PROTEUS, bijv. RFI's naar het OCAD gestuurd voor ongekende entiteiten.

de oprichting van de *Belgian Passenger Information Unit* (BelPIU) in de schoot van het Crisiscentrum.[10]

Aangezien het Crisiscentrum en het OCAD voortdurend met elkaar in contact staan en hun kantoren dicht bij elkaar liggen, zijn er geen personeelsleden van het Crisiscentrum gedetacheerd bij het OCAD. De informatiestroom met het OCAD wordt als zeer goed omschreven door de Directie ICM. De procedures die werden ingevoerd, onder meer het gebruik van functionele mailboxen, geven voldoende garanties tegen het mogelijks verlies van informatie.

De informatie-uitwisseling verloopt via drie kanalen: per e-mail (voor de niet-geclassificeerde informatie en evaluaties), via BINII voor geclassificeerde documenten en via de gemeenschappelijke gegevensbanken dewelke het Crisiscentrum rechtstreeks kan bevragen (*hit/no hit*). De veiligheidsmaatregelen aangaande geclassificeerde documenten worden gerespecteerd en toegepast door de veiligheidsofficier.

I.2.1.2. FOD Justitie – Directoraat-generaal Penitentiaire Inrichtingen

Het voornaamste contactpunt van het OCAD bij de FOD Justitie Directoraat-generaal Penitentiaire Inrichtingen is de dienst CelEx (Cel Extremisme), belast met de opvolging van als geradicaliseerd gesignaleerde gedetineerden.

Er werden twee medewerkers van de CelEx als expert gedetacheerd bij het OCAD. Ze dragen ook op die manier bij tot de opdrachten van het OCAD, bijvoorbeeld in het kader van de opvolging en evaluatie van *foreign terrorist fighters* in de schoot van de werkgroep Gevangenissen, of nog, in de *Local Task Forces* (LTF). Ze bleken daarentegen onvoldoende geïnformeerd over de veranderingen binnen het Directoraat-generaal Penitentiaire Inrichtingen (DG EPI). Terwijl de CelEx deze detachering niet meteen als een meerwaarde beschouwd maar eerder als een capaciteitsverlies, wordt de expertise over het gevangeniswezen van de twee medewerkers door het OCAD zeker naar waarde geschat.

De informatiestroom met de DG EPI verloopt in grote mate naar het OCAD. DG EPI verstrekt een grote hoeveelheid informatie uit het gevangenisnetwerk aan het OCAD en ontvangt in retour daarvoor evaluaties van gevangenen. Het is ook de dienst die de meeste verzoeken om informatie (RFI) bij het coördinatieorgaan indient.

---

[10] De Passagiersinformatie-eenheid (of *Belgian Passenger Information Unit* – BelPIU) staat in voor het verzamelen, het opslaan en het verwerken van de gegevens van passagiers die een internationaal transportmiddel vanuit, naar of via België gebruiken, en dit zowel binnen als buiten de Europese Unie. De passagiersgegevens worden voortdurend doorgegeven door de vervoerders en worden geanalyseerd aan de hand van vooraf bepaalde criteria en vergeleken met de databanken GGB en ANG. Wanneer er een '*hit*' is in de GGB (overeenstemmende identiteiten), worden de gegevens ingevoerd in de GGB en gestuurd aan onder meer het OCAD. De gegevens kunnen tevens worden gebruikt voor gerichte opzoekingen.

De toegang tot de GGB en de voeding ervan vergemakkelijken deze informatiestroom. Voorts zorgen de ingevoerde communicatie- en verzendingsroutines (per e-mail via de functionele boxen of per drager voor geclassificeerde documenten) voor een vlotte werking.

De CelEx moet echter een grote informatiestroom vanuit het gevangenisnetwerk beheren. Hoewel de dienst zegt geen personeelstekort te hebben, wordt benadrukt dat er IT-instrumenten nodig zijn om alle informatie die de dienst ontvangt, beter te kunnen analyseren en beheren.

Een officiële permanentie zou ook zeker een belangrijke toegevoegde waarde betekenen voor DG EPI en zijn diverse partners.

I.2.1.3. FOD Financiën – Algemene Administratie van de Thesaurie

De samenwerking tussen het OCAD en de Algemene Administratie van de Thesaurie van de FOD Financiën speelt zich louter af in het kader van de bevriezing van tegoeden van personen gelinkt aan terrorisme.[11] De afdeling Financiële sancties binnen de dienst *Compliance* is daartoe het contactpunt van het OCAD.

De informatiestroom tussen deze ondersteunende dienst en het OCAD is kwantitatief gering, hetgeen kan worden verklaard door de specifieke aard van hun samenwerking. Bovendien komt het zeer zelden voor dat de Algemene Administratie van de Thesaurie informatie verzamelt die als relevant wordt beschouwd voor de OCAD.

Sinds februari 2019 is één personeelslid bij OCAD gedetacheerd. De procedures voor de bevriezing van tegoeden nemen echter slechts 20% van zijn werktijd in beslag. Dit personeelslid is verbonden aan de Dienst Strategische ondersteuning - Communicatie van het OCAD en daar verantwoordelijk voor administratieve taken.

De met de Thesaurie uitgewisselde informatie is niet geclassificeerd. De uitwisselingen gebeuren hoofdzakelijk per e-mail via de functionele en professionele mailboxen. Sinds eind 2020 heeft de Thesaurie ook rechtstreeks toegang tot de GGB en is zij verplicht gegevens te verstrekken. Er werd, wat betreft de toegang tot en de codering in de GGB, door de veiligheidsofficier een interne procedure opgesteld.

I.2.1.4. FOD Justitie – Directoraat-generaal Wetgeving en Fundamentele rechten en Vrijheden – Dienst Erediensten en Vrijzinnigheid

De aanwijzing van de Dienst Erediensten en Vrijzinnigheid als ondersteunende dienst voor het OCAD moet worden gezien in het licht van zijn bevoegdheden

[11] Omzendbrief van 7 september 2015 betreffende de toepassing van de artikelen 3 en 5 van het KB van 28 december 2006 inzake specifieke beperkende maatregelen tegen bepaalde personen en entiteiten.

in het kader van de erkenning van niet-confessionele godsdiensten en levensbeschouwelijke organisaties en het beheer van het statuut van geestelijken en vertegenwoordigers van de Centrale Vrijzinnige Raad (CVR). Het OCAD werkt in het bijzonder samen met de Cel terrorisme en radicalisering. Dit nieuwe statuut maakt het mogelijk de overdracht van informatie te legaliseren, alhoewel de dienst weinig informatie verzamelt die relevant is voor het coördinatieorgaan.

Er werd erg snel een vergadering belegd tussen het OCAD en deze bijkomende ondersteunende dienst om de samenwerkingsmodaliteiten tussen beiden en tussen de functionaris voor gegevensbescherming en de veiligheidsofficier van de FOD Justitie nader te omschrijven met het oog op het opzetten van de ICT-toegangen van de GGB.

De Dienst Erediensten en Vrijzinnigheid heeft inderdaad toegang tot de GGB. Hoewel het wettelijk kader alleen voorziet in toegang tot de Gegevensbank Haatpropagandisten (GGB HP) door middel van rechtstreekse bevraging (*hit/no hit*), heeft de dienst in de praktijk een volledige toegang tot de GGB - hetgeen de dienst nuttig en noodzakelijk acht. Het Comité achtte het aangewezen om deze toegang te regulariseren.[12]

Er is geen personeelslid bij het OCAD gedetacheerd, maar een medewerker van het coördinatieorgaan werd aangewezen als contactpunt.

De (beperkte) uitwisseling van informatie vindt hoofdzakelijk per e-mail plaats. De ondersteunende dienst beschikt niet over een functionele mailbox: de e-mails worden systematisch naar de twee leden van de Cel terrorisme en radicalisering en naar het hoofd van de dienst gestuurd. Geclassificeerde documenten worden doorgegeven via het BINII-systeem, ondertussen operationeel binnen de FOD Justitie, maar in afwachting van de ontwikkeling van interne procedures voor het gebruik ervan.

I.2.2. VASTSTELLINGEN EN CONCLUSIES

Elk van de vier nieuwe ondersteunende diensten heeft een contactpunt aangewezen voor zijn uitwisselingen met het OCAD, dat de met het coördinatieorgaan uitgewisselde informatie centraliseert. Bij het OCAD zijn personeelsleden gedetacheerd voor DG EPI (twee personen) en de Thesaurie (één persoon). Terwijl DG EPI dit als een verlies van capaciteit beschouwt, waardeert het OCAD de deskundigheid waarover deze personeelsleden beschikken.

De uitwisseling van informatie is het belangrijkst met het Crisiscentrum en het DG EPI. Wat de Thesaurie en de Dienst Erediensten en Vrijzinnigheid betreft, blijft de samenwerking met OCAD zeer specifiek en beperkt tot hun bevoegdheden.

---

12 Zie 'Hoofdstuk V. De controle van de gegevensbanken' (V.2.3)'.

Het OCAD is van mening dat de uitwisseling van informatie met de vier bijkomende ondersteunende diensten zeer goed verloopt. Hoewel er in het verleden reeds uitwisselingen plaatsgevonden, legaliseert de aanwijzing als ondersteunende dienst deze samenwerking, in het bijzonder voor wat betreft de GGB. Via zijn dienst dossier- en documentatiebeheer, stelt het OCAD een permanentie ter beschikking en kan rekenen op een functionele mailbox voor alle informatie-uitwisselingen. Ook de vier ondersteunende diensten zijn van mening dat de informatie-uitwisseling met OCAD zeer goed verloopt. Met uitzondering van de Dienst Erediensten en Vrijzinnigheid, beschikken zij allen over een functionele mailbox.

De minimumveiligheidsnormen voor de bewaring van geclassificeerde documenten worden nageleefd. De procedure voor het gebruik van het BINII-systeem moet echter nog worden afgerond voor de FOD Justitie. Alleen de Thesaurie wisselt geen geclassificeerde informatie uit met het OCAD.

I.3. DE UITWISSELING VAN INFORMATIE OVER EEN WERKNEMER TUSSEN INLICHTINGENDIENSTEN EN EEN PRIVATE- OF PUBLIEKE WERKGEVER

In augustus 2019 ontving het Vast Comité I een klacht van een persoon die werkzaam was voor een publieke instelling. Deze persoon beklaagde zich over het feit dat zijn werkgever informatie had opgevraagd over hem bij een inlichtingendienst en op basis daarvan disciplinaire stappen wou ondernemen.

Na ontvangst van de klacht, en met het oog op de behandeling ervan, werd beslist een onderzoek te openen naar de meer algemene vraag in welke gevallen en onder welke voorwaarden een private of publieke instantie een vraag kan richten tot een of beide inlichtingendiensten over een (kandidaat-)werknemer alsook in welke gevallen de betrokken inlichtingendienst hierop een antwoord mag of moet formuleren en aan welke vereisten dit antwoord vervolgens moet voldoen.[13]

[13] Eind december 2019 werd een extern juridisch advies gevraagd over de eerbiediging van de privacy-rechten van werknemers in het kader van eventuele uitwisselingen tussen werkgevers en inlichtingendiensten.

I.3.1. HET ALGEMENE KADER

Of een inlichtingendienst nu op eigen initiatief of op vraag van een werkgever informatie verschaft over een (kandidaat-)werknemer, in beide gevallen betreft het een inmenging in de privacy en in het recht op de bescherming van persoonsgegevens, ook al betreft het een arbeidsrelatie. Dergelijke inmenging is slechts toegelaten indien er een duidelijke wettelijke basis is, indien de inmenging een legitiem doel nastreeft en proportioneel is (art. 8 EVRM, Conventie 108 en 108+ en art. 22 Grondwet).

Er dient in dit kader ook verwezen te worden naar artikel 2 §1, tweede lid, W.I&V dat stelt dat de inlichtingendiensten '*bij het vervullen van hun opdrachten zorgen (…) voor de naleving van, en (bij)dragen (…) tot de bescherming van de individuele rechten en vrijheden alsook tot de democratische ontwikkeling van de maatschappij*'.

Geen enkele bepaling uit de Inlichtingenwet verbiedt dat een private of publieke instantie een vraag zou richten tot een van de Belgische inlichtingendiensten. Indien een werkgever informatie opvraagt bij een inlichtingendienst, vormt dit een inmenging in het privéleven die slechts mogelijk is indien er een duidelijke wettelijke basis voorhanden is. De Inlichtingenwet laat dit toe in de mate waarin de werkgever met rede van oordeel is dat de inlichtingen die hij doorstuurt nuttig kunnen zijn voor de uitvoering van de opdrachten van de betrokken inlichtingendienst (art. 14 W.I&V m.b.t. publieke actoren; art. 16 W.I&V m.b.t. private actoren).

De Belgische wetgever heeft slechts in twee gevallen voorzien dat een werkgever (op eigen verzoek of op initiatief van de inlichtingendienst) rechtstreeks of onrechtstreeks informatie kan bekomen over een (kandidaat-)werknemer: in geval van een veiligheidsscreening of in geval van een dreiging. Ook de loutere vraag of een (kandidaat-)werknemer[14] al dan niet 'gekend' is bij één van de twee Belgische inlichtingendiensten, moet kunnen aangeknoopt worden bij een van deze twee regelingen.

I.3.2. DE WERKGEVER WIL EEN VEILIGHEIDSSCREENING

I.3.2.1. De wettelijke basis voor veiligheidsscreenings

Met veiligheidsscreenings worden situaties bedoeld waarbij een werkgever, los van een voorafgaandelijk element, alle personen wil laten *screenen* die een bepaalde toelating of vergunning behoeven. Een private of publieke werkgever kan van deze

[14] De meest klassieke voorbeelden zijn deze van een veiligheidsmachtiging om toegang te krijgen tot geclassificeerde informatie, het veiligheidsattest om toegang te krijgen tot een bepaald locatie of een bepaald evenement, of nog, het veiligheidsadvies dan kan aangevraagd worden voor tientallen verschillende toelatingen.

mogelijkheid gebruik maken onder de voorwaarden bepaald in de Classificatiewet van 11 december 1998. In principe zal de werkgever alleen het resultaat van de *screening* krijgen.[15]

In bepaalde gevallen (bijv. bij een veiligheidsmachtiging) is de werknemer onderworpen aan een vorm van een 'permanente s*creening*'. Hij moet m.a.w. gedurende de hele looptijd van zijn machtiging voldoen aan de vereisten om die machtiging te bekomen. Indien een werkgever op een gegeven ogenblik twijfelt aan die voorwaarde, kan hij hierover zijn veiligheidsofficier raadplegen. Deze kan op zijn beurt de veiligheidsoverheid en/of de onderzoekende inlichtingendienst vatten. Maar niets belet dat de werkgever rechtstreeks contact opneemt met een inlichtingendienst indien hij van oordeel is dat hij over informatie beschikt die nuttig is voor de uitoefening van hun opdrachten (artt. 14 of 16 W.I&V).

Het is dus van belang te onderlijnen dat de wettelijke regeling duidelijk bepaalt welke persoonsgegevens onder welke vorm (bijv. een onderzoeksverslag) aan welke bestemmeling (meestal een veiligheidsoverheid) kunnen worden overgezonden.

I.3.2.2. Artikel 19, eerste lid, eerste zinsnede W.I&V[16]

Het Comité wijst er op dat artikel 19 van de Inlichtingenwet geen grondslag biedt voor het systematisch doorgeven van informatie aan werkgevers die hierom verzoeken in het kader van de door hen te verlenen toelatingen of vergunningen.

---

15 Het is de veiligheidsofficier - de persoon aangeduid binnen een private of publieke instantie, die instaat voor de naleving van de classificatieregels en de contactpersoon tussen de instantie, de betrokkene en de bevoegde veiligheidsoverheid - die op de hoogte zal zijn van de concrete elementen van het dossier. Maar deze veiligheidsofficier is op zijn beurt onderworpen aan een specifiek en strafrechtelijk gesanctioneerd beroepsgeheim (artt. 23 en 24 Classificatiewet). Hij kan de elementen waarover hij beschikt niet zomaar meedelen aan de werkgever.

16 Het volledige eerste lid van art. 19 W.I&V luidt als volgt: "*De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook aan de instanties en personen die het voorwerp zijn van een [dreiging] bedoeld in de artikelen 7 en 11.*"

I.3.3. DE WERKGEVER IS HET VOORWERP VAN EEN (VERMEENDE) DREIGING

I.3.3.1. Artikel 19, eerste lid, laatste zinsnede W.I&V

Artikel 19 W.I&V luidt als volgt: '*De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee (…) aan de instanties en personen die het voorwerp zijn van een dreiging bedoeld in de artikelen 7 en 11*.'[17]

Dit artikel vormt een duidelijke wettelijke basis voor een inlichtingendienst om (persoons)gegevens mee te delen aan publieke of private[18] personen en instanties, en dus desgevallend ook aan een werkgever wiens werknemer een dreiging vormt die wettelijk gezien moet worden opgevolgd door de VSSE of de ADIV.

De bepaling vormt, in samenlezing met artikel 14 of 16 W.I&V, ook de wettelijke grondslag voor een verontruste publieke of private werkgever die een inlichtingendienst bevraagt over zijn werknemer omdat die naar het oordeel van de werkgever een (mogelijke) dreiging vormt in de zin van de Inlichtingenwet.[19] Deze bepalingen vormen ook de wettelijke basis om naar aanleiding van deze vraag desgevallend concrete elementen mee te delen over de werknemer die die (vermeende) dreiging aannemelijk kunnen maken.[20]

I.3.3.2. Een nadere uitwerking van deze regeling in een richtlijn?

Nu de laatste zinsnede van artikel 19, eerste lid W.I&V voldoende duidelijk is als de wettelijke basis voor informatieoverdracht naar publieke en private instanties, is er wél een verplichting om de modaliteiten van deze mogelijkheid nader uit te werken.

---

17 Het Comité voerde al eerder twee toezichtonderzoeken uit waarbij de toepassing van de laatste zinsnede van artikel 19, eerste lid, W.I&V centraal stond: VAST COMITÉ I, *Activiteitenverslag 2015*, 41 e.v. ('II.9. Klacht over het verstrekken van persoonlijke informatie door een inlichtingenagent aan een derde'); VAST COMITÉ I, *Activiteitenverslag 2012*, 14 e.v. ('II.2. De opvolging van buitenlandse inlichtingendiensten ten aanzien van hun diaspora in België').

18 De wet verwijst alleen naar 'instanties en personen'. Er is geen reden om aan te nemen dat deze regeling, anders dan de eerste zinssnede van artikel 19, eerste lid, W.I&V, beperkt zou zijn tot publieke (rechts)personen.

19 Het gegeven dat het wettelijk kader een werkgever van een openbare dienst toelaat om informatie te verstrekken of vragen te stellen over een van zijn personeelsleden, betekent echter niet dat de inlichtingendiensten de gestelde vraag kunnen of moeten beantwoorden. Het feit dat de inlichtingendienst een vraag niet kan (of wil) beantwoorden, betekent niet dat het onwettig of onrechtmatig is om de vraag te stellen.

20 Deze mededeling/vraag kan voor een inlichtingendienst uiteraard de aanleiding vormen om een inlichtingenonderzoek op te starten. Het al dan niet opstarten van een dergelijk onderzoek alsook de diepgang ervan, staat juridisch gezien los van de vraag of en wat een inlichtingendienst aan een werkgever mag meedelen. Uiteraard is het niet legitiem een (per definitie privacyschendend) onderzoek te starten indien er geen enkele aanwijzing is van een potentiële of concrete dreiging tegen fundamentele staatsbelangen.

Ingevolge artikel 20 §3 W.I&V dient de Nationale Veiligheidsraad (NVR) in een richtlijn de voorwaarden te bepalen waaronder inlichtingen kunnen worden meegedeeld aan private of publieke instanties of personen. Voor zover het Comité kon nagaan, werd nog niet voldaan aan deze verplichting wat betreft de situatie van personen en instanties die het voorwerp zijn van een dreiging.[21] Het Comité onderlijnde met klem zijn aanbeveling opdat de NVR een dergelijke allesomvattende richtlijn zou uitvaardigen dewelke een houvast biedt aan de inlichtingendiensten in deze delicate materie, waarbij het al dan niet doorgeven van informatie ernstige gevolgen kan hebben voor het algemene én private belangen.

Het belang van een dergelijke richtlijn is in de ogen van het Comité eens zo belangrijk nu kon worden vastgesteld dat op het niveau van de inlichtingendiensten zelf, hieromtrent geen nadere regeling werd uitgewerkt. Wat betreft de VSSE kan niettemin verwezen worden naar twee richtlijnen. Vooreerst is er de als vertrouwelijk geclassificeerde instructie van 10 oktober 2016 die handelt over de wijze waarop dient gereageerd te worden in geval van een vraag vanuit een publieke overheid om verificatie van een bepaalde persoon. Het Comité kon evenwel vaststellen dat deze richtlijn niet verduidelijkt op basis van welke wettelijke regeling bepaalde antwoorden moeten worden verschaft. De richtlijn lijkt niet van toepassing op de situatie voorzien in de laatste zinsnede van artikel 19, eerste lid, W.I&V. Alleszins regelt zij niet de verhouding met private actoren. Het Comité plaatst overigens vraagtekens bij de wettelijkheid van sommige passages van deze richtlijn, omdat ze schijnbaar ingaan tegen de wettelijke regeling inzake veiligheidsscreenings. Daarnaast stelde de VSSE in 2018 ook een vertrouwelijk geclassificeerde richtlijn op over disruptief optreden of verstoren.[22] Alhoewel het meedelen van informatie aan een persoon of instantie die het voorwerp is van een dreiging, perfect onder die definitie te brengen is, wordt in die richtlijn nergens verwezen naar artikel 19 W.I&V, noch naar enige andere wettelijke bepaling.

I.3.3.3. Limieten gesteld door de Inlichtingenwet

In welke gevallen en binnen welke limieten mag nu toepassing worden gemaakt van de mogelijkheid voor een inlichtingendienst om een (publieke of private) derde op de hoogte te brengen van inlichtingen waarover ze beschikt?

De dreigingen die bedoeld worden in artikel 19 W.I&V zijn wat betreft de VSSE, elke activiteit van spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties, criminele organisaties die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het

21 Het Comité had in het kader van een onderzoek m.b.t. de strijd tegen terrorisme en extremisme reeds aangedrongen op zo'n richtlijn (VAST COMITÉ I, *Activiteitenverslag 2012*, 92).

22 Dit is het dermate hinderen van dreigingen opdat deze niet langer plaatsvinden of dat de schadelijkheid ervan aanzienlijk wordt teruggebracht.

wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land in het gedrang kan brengen (art. 7 W.I&V). Er moet dus niet alleen een bepaalde activiteit zijn van de werknemer (bijv. extremisme), deze moet ook een gevaar inhouden voor een of meerdere fundamentele staatsbelangen. En in de context van artikel 19 W.I&V moet die private of publieke instantie ook het voorwerp zijn van de dreiging. Een werkgever mag dus niet geïnformeerd worden over bijv. de extremistische activiteiten van zijn werknemer, indien die werkgever op geen enkele wijze zelf het voorwerp is van een dreiging.

Het weze ook duidelijk dat er geen toepassing mag gemaakt worden van artikel 19 W.I&V wanneer er op geen enkele wijze fundamentele staatsbelangen op het spel staan zoals bijv. imagoschade voor een privébedrijf (tenzij dit bijv. het verlies van het vertrouwen in bepaalde instellingen betekent), een slechte werksfeer of een financieel verlies (tenzij deze financiële belangen de individuele belangen van de onderneming overstijgen en als fundamenteel voor het land kunnen aanzien worden).

De dreigingen die voor de ADIV een aanleiding kunnen zijn om publieke of private instanties of personen te verwittigen, moeten gevonden worden in artikel 11 W.I&V. Het betreft bijvoorbeeld elke activiteit die een bedreiging betekent voor de onschendbaarheid van het nationaal grondgebied of de bevolking, de militaire defensieplannen, het wetenschappelijk en economisch potentieel met betrekking tot bepaalde bedrijvenactief in defensie-gerelateerde sectoren, de vervulling van de opdrachten van de strijdkrachten, de veiligheid van de Belgische onderdanen in het buitenland, de militaire veiligheid van het personeel dat onder de minister van Defensie ressorteert…

Aangezien de mededeling van gegevens op basis de laatste zinsnede van artikel 19, eerste lid, W.I&V een duidelijke finaliteit heeft (vrijwaren van fundamentele staatsbelangen tegen bepaalde activiteiten waarvan de betrokken instantie of persoon het voorwerp is), moet de mededeling van (persoons)gegevens ook beperkt zijn tot die informatie die bijdraagt tot het opvolgen of – indien nodig - neutraliseren van de dreiging.

De eerste verplichting van een inlichtingendienst die wordt geconfronteerd met een verzoek om informatie is dan ook na te gaan om welk probleem, welk incident, welke dreiging het zou kunnen gaan. In dit verband zou de inlichtingendienst zijn databanken kunnen raadplegen om de aan hem meegedeelde naam of namen te verifiëren.[23] Het lijkt ook voor de hand te liggen dat de inlichtingendienst contact opneemt met de werkgever om het verzoek in de juiste context te plaatsen. Daartoe zal met name moeten worden nagegaan waarom de werkgever wil weten of zijn werknemer bekend is bij de inlichtingendiensten, wat het probleem en de

[23] Dit is ook wat de richtlijn van de VSSE van 10 oktober 2016 voorschrijft bij een vraag van een publieke overheid om een persoon te verifiëren.

dreiging is, of er een veiligheids- of ander incident is geweest, of er sprake is van een noodsituatie…

Indien die gegevens geen uitsluitsel geven in de ene of de andere richting, kan verder onderzoek door de dienst aangewezen zijn. De reikwijdte van dit onderzoek kan niet *in abstracto* worden bepaald. Dit zal afhangen van de aard van de bedreiging en van de informatie die in de loop van het onderzoek naar voren komt. Bij dergelijk onderzoek zal de dienst alleszins rekening moeten houden met de proportionaliteits- en subsidiairiteitsprincipes.

De antwoorden op deze vragen en de resultaten van het bijkomende onderzoek moeten de inlichtingendienst toelaten te beoordelen of ze in deze bevoegd is en desgevallend toepassing kan maken van artikel 19 W.I&V en wat ze, gelet op de dreiging, al dan niet kan meedelen aan de werkgever.

I.3.3.4. Wat mag of moet worden meegedeeld?

In wat volgt, wordt er van uit gegaan dat er effectief sprake is van een dreiging. De vraag stelt zich vervolgens wat op welke wijze kan meegedeeld worden.[24]

I.3.3.4.1. Het proportionaliteits- en subsidiariteitsbeginsel

Gelet op de eisen van de proportionaliteit en de subsidiariteit moet de eerste vraag zijn of de werkgever *überhaupt* in kennis mag gesteld worden. Indien de dreiging zeer vaag en weinig ernstig is, of indien de dienst de evaluatie van de dreiging zelf kan opvolgen of de dreiging kan counteren op een andere wijze (bijv. door de werknemer zelf aan te spreken zodat die zich realiseert dat hij wordt opgevolgd), dan is een mededeling van persoonsgegevens aan een werkgever mogelijk disproportioneel en niet subsidiair.

Indien dit niet volstaat en de dreiging is voldoende ernstig, dan dient de mogelijkheid zich aan om de werkgever in kennis te stellen. Ook hier moet worden afgewogen hoeveel en welke informatie wordt gegeven. De regel hierbij is opnieuw dat er, gegeven de aard en de ernst van de dreiging en nood en de mogelijkheden om deze te counteren, gestreefd wordt naar een de minimale inmenging in het privéleven.

---

[24] Eerst wordt kort de hypothese aangehaald waarbij de inlichtingendienst in hoofde van de werknemer (eventueel na een eerste bevraging of na een grondiger inlichtingenonderzoek) *geen enkele* dreiging in de zin van de Inlichtingenwet vaststelt. Op dat ogenblik maakt de werkgever per definitie niet het voorwerp uit van een dreiging en kan strikt genomen geen toepassing gemaakt worden van artikel 19 W.I&V. Het Comité is echter van oordeel dat in deze gevallen aan de inlichtingendienst de mogelijkheid moet gelaten worden om de werkgever mee te delen dat er geen sprake is van een dreiging in de zin van de Inlichtingenwet (hetgeen uiteraard niet betekent dat er geen andersoortige dreiging kan zijn voor de werkgever). Het Comité oordeelde reeds in die zin in in een eerder onderzoek VAST COMITÉ I, *Activiteitenverslag 2015*, 41 e.v. ('II.9. Klacht over het verstrekken van persoonlijke informatie door een inlichtingenagent aan een derde').

Indien de dreiging echter dermate ernstig is dat deze alleen door een tussenkomst van de werkgever kan gecounterd worden, kan méér en concretere informatie worden meegedeeld die bijvoorbeeld kan dienen om een administratieve of private beslissing (bijv. disciplinaire sanctie, overplaatsing, ontslag…), te onderbouwen. Het weze duidelijk dat het uiteindelijke doel van de inlichtingendienst hier het neutraliseren of verkleinen van een dreiging moet zijn.

Aansluitend bij de vraag naar een proportionele informatieverstrekking, rijst de vraag of een inlichtingendienst in zijn mededeling zelf een oplossing mag suggereren aan de bedreigde publieke of private instantie of – sterker nog – mag deelnemen aan de besluitvorming over het handelen door de bedreigde instantie of persoon. Bedoeld wordt bijvoorbeeld de suggestie om iemand te ontslaan. Het Comité was van oordeel dat dit niet onwettelijk is in de mate waarin de gesuggereerde oplossing zelf wettelijk en proportioneel is.

Tot slot stelde zich de vraag of uit artikel 19 W.I&V een *verplichting* blijkt om te antwoorden op een vraag of om *op eigen initiatief* gegevens te verstrekken. De bepaling stelt dat de inlichtingen- en veiligheidsdiensten hun inlichtingen *'slechts meedelen'* aan instanties en personen die het voorwerp zijn van een dreiging. Alhoewel de bepaling op dit vlak niet erg duidelijk is, was het Comité van oordeel dat een inlichtingendienst verplicht is om gegevens mee te delen indien alleen hierdoor de realisatie van een ernstige dreiging tegen fundamentele staatsbelangen kan voorkomen worden. In de andere gevallen bepaalt zij autonoom wat de beste strategie vormt, gegeven de dreiging. Het Comité beveelde aan dat deze onduidelijkheid wordt opgehelderd ofwel door een wetgevend initiatief ofwel door een regeling ter zake in de verplicht op te stellen richtlijn van de Nationale Veiligheidsraad.

Hierbij aansluitend suggereerde het Comité om te onderzoeken of het nuttig zou zijn om een verplichte melding naar de werkgever in het leven te roepen ten aanzien van iedere (kandidaat-)werknemer die is opgenomen in een Gemeenschappelijke gegevensbank *terrorist fighters* of haatpredikers.

I.3.3.4.2. Andere aandachtspunten: zorgvuldigheid, classificatie en schriftelijke mededeling van informatie

In een inlichtingencontext bestaan er weinig zekerheden, en dit gegeven moet mee de beslissing bepalen om en hoe een werkgever te informeren. Om over een rechtmatige informatievertrekking te kunnen spreken, moet de mededeling voldoende onderbouwd zijn door betrouwbare inlichtingen. Ze dient daarenboven zorgvuldig verwoord te zijn.[25]

[25] Er mag bijvoorbeeld geen ongenuanceerd beeld wordt gegeven van de onderliggende inlichtingen, of een bepaald element mag niet als 'vaststaand' worden voorgesteld indien het om 'een visie over' of 'een aanvoelen van' gaat. De meegedeelde informatie moet in die zin ook 'eerlijk' zijn door een objectief beeld te bieden van de wijze waarop de inlichtingendienst de dreiging en de rol van de betrokkene daarin ziet, zonder 'manipulatief' te zijn in die zin dat ze de besluitvorming van private of publieke werkgever wil sturen.

Daarnaast beschikt niet elke private en publieke instantie over een veiligheidsmachtiging. Dit betekent dat geclassificeerde informatie zal moeten gedeclassificeerd worden. Dit geldt des te meer indien de informatie moet dienen om een beslissing van de werkgever te schragen.

Tot slot bepaalt artikel 19 W.I&V niet op welke wijze een bedreigde instantie in kennis moet worden gesteld. Het Comité is van oordeel dat dit om redenen van rechtszekerheid, behoudens hoogdringendheid, schriftelijk dient te gebeuren. Dit om discussies achteraf te vermijden en een parlementaire of zelfs jurisdictionele controle toe te laten.

I.3.4. CONCLUSIES

Voor de informatieverstrekking door de inlichtingendiensten aan een private of publieke werkgever gelden – terecht – strenge regels, omdat de mededeling grote gevolgen kan hebben voor de betrokken personen. Minimaal betekent dit een inbreuk op de privacy en in het uiterste geval kan het de basis vormen voor ingrijpende maatregelen die de betrokkenen in hun rechtspositie kunnen aantasten.

Indien de VSSE en de ADIV op eigen initiatief of op verzoek informatie verstrekken aan een publieke of private werkgever (en het loutere meedelen of een persoon 'gekend' is of niet valt daar ook onder), moet aan alle wettelijke vereisten voldaan zijn, te weten:

1. er moet een specifieke wettelijke grondslag zijn;
2. de dienst moet zorgvuldig tewerk gaan bij de interne totstandkoming van de te verstrekken gegevens en in de communicatie daarover naar de ontvanger;
3. de mededeling moet beantwoorden aan de eisen van de noodzakelijkheid; en
4. de mededeling moet proportionaliteit zijn.

Wat betreft de wettelijke basis, benadrukte het Comité dat het buiten de twee besproken situaties (m.n. de werkgever wil een veiligheidsscreening of de werkgever is voorwerp van dreiging) niet toegelaten is om informatie te verschaffen over een werknemer aan een publieke of private werkgever. Vanuit het oogpunt van de inlichtingenagent is dergelijke mededeling afhankelijk van de concrete situatie mogelijks zelfs strafbaar.

Het Comité beklemtoonde tevens dat niets een werkgever uit de overheids- of de privésector belet om informatie mee te delen aan of vragen te stellen aan een Belgische inlichtingendienst over een mogelijke bedreiging in de zin van de Wet van 30 november 1998 waarvan een van zijn personeelsleden de 'oorzaak' zou zijn.

Het Comité nodigde spelers uit de publieke en private sector wel uit om te onderzoeken of bepaalde potentiële dreigingen niet preventief kunnen ondervangen worden door voor bepaalde functies, toelatingen of vergunningen een beroep te doen op het systeem van de veiligheidsscreenings uit de Classificatiewet. Het Co-

mité benadrukte wel dat dit systeem oordeelkundig moet gebruikt worden en niet mag leiden tot een ongebreidelde toepassing.

Het Comité was van oordeel dat de VSSE en de ADIV binnen zes maanden na het afsluiten van deze studie een voorstel tot richtlijn ter uitvoering van de laatste zinsnede van artikel 19, eerste lid, moesten opstellen ten behoeve van respectievelijk de minister van Justitie en van Defensie met het verzoek het voorstel ter goedkeuring voor te leggen aan de Nationale Veiligheidsraad.

I.4. ERNSTIGE TEKORTKOMINGEN AANGAANDE DE NATIONALE VEILIGHEID

Begin juli 2020 richtte de voorzitter van het Vast Comité I een geclassificeerd schrijven aan de (toenmalige) minister van Buitenlandse Zaken en Defensie, onder meer bevoegd voor de Nationale Veiligheidsoverheid (NVO) en de Algemene Dienst Inlichting en Veiligheid (ADIV). In zijn hoedanigheid van voorzitter van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen[26] werden immers ernstige tekortkomingen aangaande de nationale veiligheid vastgesteld.

De rechtstreekse aanleiding vormde een dossier aangaande de verlenging in januari 2020 van een veiligheidsadvies; de werkneemster in kwestie had in 2015 al een positief veiligheidsadvies gekregen. Dit gaf haar toegangsrecht tot zones op de luchthaven van Brussel-Nationaal dewelke omwille van veiligheidsredenen slechts beperkt toegankelijk zijn. Uit een geclassificeerd rapport bleek evenwel dat haar partner een van de vermeende co-auteurs was van de aanslagen in Parijs en Brussel. Zij onderhield regelmatig contacten met hem tijdens gevangenisbezoek in een ruimte zonder bewaking.

Ondanks het onmiskenbare veiligheidsrisico, werd het besluit om het advies of de machtiging van betrokkene in te trekken, pas genomen op het moment dat er een verzoek tot verlenging werd ingediend.[27]

Het Vast Comité I interpelleerde de Regering en onderstreepte dat hiermee het dysfunctioneren van de administraties en openbare overheden werd aangetoond, waarbij het 'vakjesdenken' verhindert om de veiligheid van de burger te kunnen garanderen. Het Comité wees de Regering ook op de recurrentie van dit probleem,

---

26 Het Beroepsorgaan is het administratief rechtscollege dat bevoegd is om kennis te nemen van beroepen inzake veiligheidsmachtigingen, -attesten en -adviezen in het kader van de Wet van 11 december 1998. De voorzitter van het Beroepsorgaan is tevens de voorzitter van het Vast Comité I. Hierover: Hoofdstuk X. Het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen.

27 Ook het toezichtonderzoek naar de wijze waarop de inlichtingendiensten veiligheidsscreenings uitvoerden, besteedde bijzondere aandacht aan deze problematiek. Hierover VAST COMITÉ I, *Activiteitenverslag 2019*, 2-14 ('I.1. De uitvoering van veiligheidsscreenings door de inlichtingendiensten').

dat al werd onderstreept tijdens de werkzaamheden van de Parlementaire Onderzoekscommissie naar de 'terroristische aanslagen' van 22 maart 2016.[28]

Tussen juli 2020 en februari 2021 volgde een uitvoerige briefwisseling tussen het Vast Comité I, de (toenmalige) minister van Buitenlandse Zaken en Defensie, de voorzitter van de Nationale Veiligheidsoverheid en de voorzitter van het College van Procureurs-generaal. Er werd onder meer gevraagd een werkgroep op te richten om de vastgestelde dysfuncties te onderzoeken.

Het Vast Comité I diende vast te stellen dat weinig gehoor werd gegeven bij het aankaarten van de problemen aangaande de nationale veiligheid.[29] Gezien het daarmee aan het einde van zijn prerogatieven kwam, werd de situatie voor nuttig gevolg toevertrouwd aan de Kamer van volksvertegenwoordigers. De nuttige opmerkingen vanuit het Vast Comité I zouden zijn meegenomen in de werkzaamheden van verschillende werkgroepen die binnen de Nationale Veiligheidsoverheid werden opgericht. Daarin is er onder meer aandacht voor een structurele hervorming van de NVO.

I.5. DE OPVOLGING VAN SCHADELIJKE SEKTARISCHE ORGANISATIES EN CRIMINELE ORGANISATIES

Op vraag van de Begeleidingscommissie van de Kamer van volksvertegenwoordigers opende het Vast Comité I een toezichtonderzoek naar de wijze waarop de Veiligheid van de Staat (VSSE) twee van haar wettelijke opdrachten uitvoerde, i.e. de opvolging van schadelijke sektarische organisaties[30] en deze van criminele

---

28 BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS, *Onderzoekscommissie terroristische aanslagen 22 maart 2016. Beknopt overzicht van de werkzaamheden en aanbevelingen*, 2018.

29 De thematiek vormde het voorwerp van parlementaire vragen (cf. Vraag van C. Thibaut aan de minister van Buitenlandse Zaken over het 'uitblijven van antwoorden van de NVO aan het Comité I inzake veiligheidsmachtigingen' (*Vr. en Ant*. Kamer 2020-21, 15 juli 2021, QRVA59, 108, Vr. nr. 342)) en persartikelen (bijv. L. BOVÉ, *De Tijd*, 6 mei 2021 ('Kamer slaat alarm over veiligheidsscreenings').

30 In een streven naar objectiviteit wordt onder 'sekte', 'schadelijke sektarische organisatie' of 'schadelijke sektarische groep' verstaan 'elke groepering met een levensbeschouwelijk of godsdienstig doel, of die zich als dusdanig voordoet die als schadelijk wordt beschouwd en zo het voorwerp kan uitmaken van welke belangstelling ook vanwege de Veiligheid van de Staat (VSSE)'.

organisaties. In het verleden boog het Vast Comité I zich al eerder over verschillende aspecten van deze problematiek.[31]

I.5.1. CONTEXTUALISERING

I.5.1.1. De schadelijke sektarische organisaties

Gedurende lange tijd hebben de Belgische autoriteiten blijk gegeven van bijzondere terughoudendheid ten aanzien van bewegingen die werden geacht sektair te zijn. Die houding werd ingegeven door de moeilijkheid om een standpunt in te nemen op een domein dat raakte aan de fundamentele vrijheden van godsdienst, denken, meningsuiting en vereniging.

In de loop van de jaren 1980 brachten meerdere tragische en sterk gemediatiseerde gebeurtenissen dit fenomeen onder de aandacht van zowel de bevolking als van de autoriteiten, wat leidde tot heel wat initiatieven in België in de loop van de jaren 1990. Zo werd in 1996 een parlementaire onderzoekscommissie 'sekten' opgericht.[32] Een Informatie- en adviescentrum inzake de schadelijke sektarische organisaties (IACSSO) en een Administratieve coördinatiecel (ACC) werden bij Wet van 2 juni 1998 opgericht.[33] Een koninklijk besluit[34] kende het secretariaat van de ACC toe aan de Veiligheid van de Staat.

---

31 Wat betreft de schadelijke sektarische organisaties: VAST COMITÉ I, *Activiteitenverslag 1996*, pp. 88-100 ('Hoofdstuk 2. Toezichtsonderzoek inzake de doeltreffendheid van de inlichtingendiensten met betrekking tot de activiteit van sekten in België'); *Activiteitenverslag 2006*, pp. 63-65 ('II.6.2. Schadelijke sektarische organisaties en de bevoegdheid van de Veiligheid van de Staat'); *Activiteitenverslag 2007*, p. 41-42 ('II.10.9. Schadelijke sektarische organisaties'); *Activiteitenverslag 2010*, pp. 13-24 ('II.2. De opvolging van schadelijke sektarische organisaties') en *Activiteitenverslag 2014*, pp. 51-54 ('II.5. Een klacht van de Scientologykerk tegen de Veiligheid van de Staat').
Wat betreft criminele organisaties: VAST COMITÉ I, *Activiteitenverslag 2002*, 19-20 ('Hoofdstuk II.2.6. Toezichtonderzoek over de inlichtingen waarover de Veiligheid van de Staat beschikt inzake een affaire van visumfraude'); *Activiteitenverslag 2004*, 13-18 ('IV.2.2. Onderzoek naar de wijze waarop de Belgische inlichtingendiensten functioneren en samenwerken in het kader van hun nieuwe wettelijke opdracht betreffende de dreigingen van criminele organisaties').

32 *Parl. St.*, Kamer, 1995-1996, nr. 313/008.

33 Wet van 2 juni 1998 houdende oprichting van een informatie- en adviescentrum inzake de schadelijke sektarische organisaties en van een administratieve coördinatiecel inzake de strijd tegen schadelijke sektarische organisaties (*BS* 25 november 1998). Deze wet voorziet in actieve samenwerking tussen het IACSSO, de ACC en de andere openbare diensten die betrokken zijn bij deze strijd, zoals het Federaal Parket, de parketten-generaal, de parketten van aanleg, de politie, de Veiligheid van de Staat en de plaatselijke overheden.

34 Koninklijk besluit tot wijziging van het koninklijk besluit van 8 november 1998 houdende samenstelling, werking en organisatie van de Administratieve Coördinatiecel inzake de strijd tegen schadelijke sektarische organisaties (*BS* 9 december 1998).

I.5.1.2. Criminele organisaties

In 2019 werden in het kader van een studie bij de Federale Gerechtelijke Politie meer dan 600 criminele organisaties, verenigingen van misdadigers of groepen van daders in België geteld.[35]

In haar verslag van 2020[36] meldt de Cel voor Financiële Informatieverwerking (CFI) op haar beurt dat ze in 2020 31.605 meldingen had ontvangen. De cel verklaarde ook dat nog in 2020 1.228 nieuwe dossiers werden overgemaakt aan de gerechtelijke autoriteiten en dat informatie uit 2.765 meldingen werd doorgezonden naar en gebruikt door de parketten en het federaal parket, goed voor een totaalbedrag van 1.885,31 miljoen euro. Het rapport preciseert verder dat "*in 2020 de CFI opvallend veel doormeldingen heeft verricht waarbij er sprake is van georganiseerde misdaad*".[37]

I.5.2. DE MATERIËLE BEVOEGDHEID

De taakstelling van de VSSE binnen de opvolging van schadelijke sekten en criminele organisaties situeert zich binnen haar inlichtingenopdracht. Krachtens artikel 7, 1° W.I&V wordt deze omschreven als '*het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen, het wetenschappelijk of economisch potentieel, zoals gedefinieerd door de Nationale Veiligheidsraad, of elk ander fundamenteel belang van het land, zoals gedefinieerd door de Koning op voorstel van de Nationale Veiligheidsraad, bedreigt of zou kunnen bedreigen*'.

De wetgever heeft hierbij geopteerd om een limitatieve lijst op te stellen van veiligheidsdreigingen die behoren tot het bevoegdheidsdomein van de VSSE (m.n. terrorisme, extremisme, spionage, inmenging, proliferatie, schadelijke sektarische organisaties en criminele organisaties).

De *'schadelijke sektarische organisaties'* worden daarbij omschreven als '*elke groep met filosofische of religieuze inslag of die voorwendt dat te zijn en die qua organisatie of in haar praktijk schadelijke onwettige activiteiten uitoefent, individuen of de maatschappij nadeel berokkent of de menselijke waardigheid schendt*' (art. 8, 1°, tweede lid, e W.I&V).

Ook *'criminele organisaties'* werden door de wetgever omschreven als een nationale veiligheidsdreiging die onder de interessesfeer van de VSSE dient te vallen. Dit

---

35 Federale Politie, 'Diagnose - Eerste benadering van criminele organisaties', april 2020, p. 4. De FGP benadrukt dat "*de problematiek van terrorisme of de financiering ervan 20 keer wordt vermeld*".

36 https://www.ctif-cfi.be/images/documents/Dutch/Jaarverslagen/2020.pdf, 10.

37 https://www.ctif-cfi.be/images/documents/Dutch/Jaarverslagen/2020.pdf, 22.

begrip wordt in de Inlichtingenwet omschreven als *'iedere gestructureerde vereniging van meer dan twee personen die duurt in de tijd, met als oogmerk het in onderling overleg plegen van misdaden en wanbedrijven, om direct of indirect vermogensvoordelen te verkrijgen, waarbij gebruik gemaakt wordt van intimidatie, dreiging, geweld, listige kunstgrepen of corruptie, of waarbij commerciële of andere structuren worden aangewend om het plegen van misdrijven te verbergen of te vergemakkelijken.'* (art. 8, 1°, tweede lid, f W.I&V).

Vandaar dat de VSSE slechts bevoegd is voor de opvolging van criminele organisaties indien de criminele organisaties *'wezenlijk betrekking hebben op de activiteiten bedoeld in artikel 8, 1°, a) tot e) en g)'*- zijnde de activiteiten inzake terrorisme, extremisme, spionage, inmenging, proliferatie en schadelijke sekten – *'of die destabiliserende gevolgen kunnen hebben op het politieke of sociaal-economische vlak'*.

Niet alle schadelijke sektarische en criminele organisaties behoren zodoende tot de wettelijke interessesfeer van de VSSE. Daarnaast schrijft de Inlichtingenwet voor dat deze pas tot de bevoegdheid van de VSSE behoren, wanneer de activiteiten ervan een dreiging kunnen betekenen voor de inwendige of uitwendige veiligheid van de Staat en/of voor het wetenschappelijk of economisch potentieel van het land.

Wat betreft de opvolging van schadelijke sektarische organisaties, verklaarde het Comité in 2015 wat volgt: "*Er dient te worden onderstreept dat, algemeen, geen enkele andere buitenlandse inlichtingendienst als officiële opdracht heeft om toezicht uit te oefenen op schadelijke sekten. Deze specifieke opdracht van de Belgische Veiligheid van de Staat vormt dus een uitzondering in de wereld van de inlichtingendiensten.*[38] *De meeste democratische landen weigeren zelfs deze diensten te betrekken bij het toezicht op religieuze bewegingen. Deze maatregel wordt immers beschouwd als een inbreuk op de vrijheid van godsdienst*" (vrije vertaling).

I.5.3. DE PROCEDURELE BEVOEGDHEID

De procedurele bevoegdheid binnen de inlichtingenopdracht laat zich, in eerste instantie, bepalen door de in artikel 7, 1° W.I&V opgesomde activiteiten: *'het inwinnen, analyseren en verwerken van inlichtingen'*. Hieruit blijkt dat de VSSE schadelijke sekten en criminele organisaties gaat bestrijden via informatiegaring en inlichtingenanalyse en het vervolgens doorgeven van de bekomen inlichtingen (m.n. de verrijkte informatie) aan andere instanties (bijv. politionele of gerechtelij-

[38] Waaraan de VSSE toevoegt (14 april 2021): "*et le service, au surplus, se trouve privée d'échanges fructueux en la matière avec ses correspondents étrangers*" (en de dienst bovendien verstoken blijft van vruchtbare uitwisselingen op dit gebied met zijn buitenlandse correspondenten (vrije vertaling).

ke overheden). Laatstgenoemden nemen uiteindelijk de nodige tegenmaatregelen ter bescherming van de nationale veiligheid.

Om deze opdrachten uit te voeren, zette de VSSE, op het hoogtepunt van haar activiteiten in deze materies, volgend personeel in:

- Schadelijke sektarische organisaties (1999-2000): zes medewerkers in de 'Sectie Analyse' (waarvan drie niveau A) en negen medewerkers in de 'Operationele sectie';
- Criminele organisaties (jaren 2000): twee medewerkers in de 'Sectie Analyse' en twee medewerkers in de 'Operationele sectie'.

I.5.4. DE BELEIDSPRIORITEITEN

Artikel 7, 1° W.I&V vestigt een wettelijke verplichting tot handelen in hoofde van de VSSE. Dit wil evenwel niet zeggen dat er geen prioriteiten gelegd kunnen worden binnen de werkzaamheden van de VSSE. De dienst heeft immers onvoldoende capaciteit en middelen ter beschikking om alle tot zijn bevoegdheid behorende nationale veiligheidsdreigingen te detecteren, op te volgen en te beheersen (noch zou ze deze ooit kunnen hebben). Het leggen van prioriteiten is daarom een noodzaak, zelfs een plicht.

Een dergelijke lezing wordt bevestigd in diverse wettelijke en reglementaire bepalingen. Vooreerst bepaalt artikel 4 W.I&V dat de VSSE haar opdrachten verricht door tussenkomst van de minister van Justitie, doch *'overeenkomstig de richtlijnen van de Nationale Veiligheidsraad'*.

De opdracht van de Nationale Veiligheidsraad (NVR) is vastgelegd in artikel 3 van het Koninklijk besluit van 22 december 2020 'tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité Inlichtingen en Veiligheid en het Coördinatiecomité Inlichtingen en Veiligheid'. Deze stelt dat de NVR, *'(a)ls coördinerend beleidsorgaan'*, *'belast (is) met (…) de bepaling van de prioriteiten van de inlichtingen- en veiligheidsdiensten'*.

In juli 2015 heeft diezelfde Nationale Veiligheidsraad beslist dat de VSSE de schadelijke sektarische organisaties en criminele organisaties niet langer actief (onze onderlijning) opvolgt. Aangezien België het hoofd diende te bieden aan een golf van binnen- en buitenlandse aanslagen of pogingen daartoe, beslisten de ministers van Justitie en Defensie om de prioriteit van de opdrachten te herdefiniëren en aanpassingen door te voeren wat betreft de inzet van personeel en materiële middelen van de inlichtingendiensten.

Op 25 augustus 2015 verklaarde toenmalig minister van Justitie wat volgt: "*De Staatsveiligheid reorganiseert vanaf 1 september haar buitendienst met een ongeziene focus op het radicalisme en het terrorisme*." In verband hiermee liet de Veiligheid van de Staat ook nog weten: "*De Nationale Veiligheidsraad heeft het Actieplan 2015 van de Veiligheid van de Staat goedgekeurd. Op basis van dit plan heeft de directie*

van de Veiligheid van de Staat beslissingen genomen met betrekking tot haar organisatie" (vrije vertaling), en ook nog: "*Gevolg van deze nieuwe focus: andere bedreigingen zoals sekten en bedrijfsspionage worden op de achtergrond geplaatst"* (vrije vertaling).[39]

Dit werd in 2020 ook zo bevestigd door de VSSE, waarbij gesteld werd dat "*le suivi actif des organisations sectaires nuisibles a été mis en suspens, sauf au cas où une menace d'ingérence, d'espionnage, de prolifération, d'extrémisme ou de terrorisme y serait liée.*" Eenzelfde vaststelling geldt voor de opvolging van de criminele organisaties.

Tot slot bepaalt artikel 2 van het koninklijk besluit van 5 december 2006 betreffende het algemeen bestuur en de ondersteuningscel van de Veiligheid van de Staat dat de directie-generaal van de VSSE (m.n. de administrateur-generaal en de adjunct-administrateur-generaal) '*verantwoordelijk (zijn) voor de uitwerking en de uitvoering van een vierjaarlijks strategisch plan dat de prioriteiten bepaalt van de Veiligheid van de Staat en de operationele strategieën om deze prioriteiten uit te voeren*'. Artikel 3 schrijft voor dat de VSSE jaarlijks een actieplan dient voor te leggen aan de minister van Justitie en dit ter realisatie van het strategisch plan. Dit actieplan bevat, onder meer, de strategische doelstellingen en de middelen om deze te verwezenlijken. Uit deze plannen moet blijken dat sinds de aanslagen in Verviers (januari 2015), Parijs (november 2015) en Brussel (maart 2016) terrorisme en (islamitisch-, rechts- en links)extremisme, samen met spionage, de drie grote speerpunten vormen in het beleid van de VSSE en als dusdanig als belangrijkste dreigingen worden beschouwd. Zowel schadelijke sektarische organisaties als criminele organisaties komen niet voor in de prioriteitenlijst.

I.5.5. DE TOEGELATEN BELEIDSRUIMTE

Bij het vastleggen van beleidsprioriteiten worden de Nationale Veiligheidsraad en de minister van Justitie juridisch begrensd. Prioriteiten moeten zich vooreerst situeren binnen het door de wetgever vastgelegde bevoegdheidsdomein, zijnde binnen de te beschermen belangen en de bestrijden veiligheidsdreigingen.

Daarnaast zijn noch de Nationale Veiligheidsraad, noch de minister van Justitie, noch de VSSE bevoegd om een veiligheidsdreiging in zijn geheel, voor alle soorten inlichtingenactiviteiten en ten alle tijde, als niet op te volgen te kwalificeren. Een dergelijke maatregel komt neer op een door de uitvoerende macht gedane schorsing van artikel 7, 1° *i.o.* artikel 8, 1° W.I&V. Het leggen van prioriteiten binnen de inlichtingenopdrachten van de VSSE heeft betrekking op het bepalen van

[39] De minister van Justitie zal in 2016 deze beleidskeuze nog bevestigen in antwoord op een parlementaire vraag en verduidelijkt dat e*en ontwerp van KB tot wijziging wordt opgesteld en tot doel heeft de Veiligheid van de Staat te ontlasten van deze taak* (het secretariaat van de ACC, onze toevoeging) *en het toe te vertrouwen aan het secretariaat van het IACSSO.*

de aangelegenheden waarbij actief door de inlichtingendienst een informatiepositie dient opgebouwd te worden. Het betekent geenszins dat, indien de VSSE passief informatie van een derde verkrijgt waarin concrete aanwijzingen (*leads*) besloten liggen van mogelijke problematische activiteiten[40], de VSSE geen plicht zou hebben om deze aanwijzingen nader te beoordelen en desgevallend actief te onderzoeken. De VSSE heeft weliswaar de bevoegdheid om een opportuniteitsoordeel te nemen binnen haar onderzoeken, maar heeft eveneens een onderzoeksplicht t.a.v. de door de wetgever opgesomde veiligheidsdreigingen. Het zorgvuldigheidsbeginsel indachtig zal de beoordeling van *leads*, en de daaropvolgende beslissing om een *lead* al dan niet verder actief te onderzoeken, dienen te gebeuren a.d.h.v. vooraf bepaalde objectieve criteria. Het wettigheidsbeginsel indachtig, mogen dergelijke criteria er niet toe leiden dat in de praktijk een wettelijk bepaalde veiligheidsdreiging nooit verder wordt onderzocht.

I.5.6. DE ORGANISATORISCHE VERTALING VAN DE BELEIDSPRIORITEITEN

Aanvullend moet de vraag gesteld worden op welke wijze deze juridisch begrensde beleidsruimte gevolgen heeft voor de organisatorische vertaling van de beleidsprioriteiten? Anders gesteld: wat kan en wat kan niet binnen de creatie en de opheffing van diensten en secties? En dient er een gereserveerde capaciteit te worden voorzien?

De minister van Justitie (*cf*. art. 5, §3 W.I&V) en, in subsidiaire orde, de directie-generaal van de VSSE (*cf*. art. 2 KB 5 december 2006) zijn binnen de door de wetgever en de Koning bepaalde regels verantwoordelijk voor het bepalen van de organisatiestructuur van de VSSE.[41]

Binnen dit wetgevend en reglementair kader behoort het tot de discretionaire bevoegdheid van de uitvoerende macht om al dan niet een (analyse)dienst of (operationele) sectie voor een bepaalde veiligheidsdreiging in te richten. De in de VSSE gedane opheffing van de analysedienst Sekten en, eerder, van de operationele sectie Sekten, behoort dan ook tot de autonomie van vernoemde beleidsverantwoordelijken.

Wel dient de VSSE zich op een manier te organiseren dat ze kan voldoen aan de wettelijke plicht tot handelen wanneer ze passief informatie verkrijgt van een derde waarin concrete aanwijzingen besloten liggen van mogelijke problematische

---

40 Van bijv. schadelijke sektarische organisaties of criminele organisaties zoals wettelijk omschreven.

41 Op regeringsniveau werd in het Koninklijk besluit van 5 december 2006 (*supra*) bepaald dat de VSSE bestaat uit een directie Operaties, een directie Analyse en een Stafdirectie. Op wetgevend niveau werd bijvoorbeeld in de Classificatiewet bepaald dat de VSSE dient te beschikken over een veiligheidsofficier. In de Gegevensbeschermingswet werd dan weer vastgelegd dat de dienst een functionaris voor gegevensbescherming dient te hebben.

activiteiten van schadelijke sekten of van criminele organisaties. Er kan voorzien worden in een gereserveerde capaciteit (bijv. x aantal analisten én x aantal collecte-agenten) die verantwoordelijk zijn om dergelijk passief verkregen informatie te onderzoeken en om desgevallend bijkomende informatie erbij in te winnen.[42] Dergelijke VSSE-agenten kunnen nog belast zijn met andere door de VSSE-leiding bepaalde taken, doch oefenen een eerstelijnsrol uit wanneer problematische informatie over sekten of criminele organisaties aan de VSSE werd overgemaakt. Indachtig dat sommige activiteiten van schadelijke sektarische organisaties eveneens gekwalificeerd kunnen worden als extremistische en/of inmengingsactiviteiten, kan desgevallend geopteerd worden om dergelijke gereserveerde capaciteit in te richten bij de voor deze dreigingen bevoegde diensten en secties. Gelet op het transversaal karakter van de dreiging 'criminele organisaties' zou dit tot het additioneel takenpakket van andere diensten en secties kunnen behoren.

I.5.7. NOOD AAN VERSTERKING EN EEN BREDER MAATSCHAPPELIJK DEBAT

In de loop van het onderzoek kon het Vast Comité I vaststellen dat de prioritisering van de opdrachten conform was aan het wettelijk en reglementair kader.

Nadat in 2021 werd vastgesteld dat de VSSE slechts een eerder beperkt aantal openstaande dossiers kon opvolgen – en dat er voor deze administratie onmiskenbaar sprake was van een tekort aan personeel en bijgevolg de verplichting tot het maken van keuzes – herinnerde het Comité opnieuw aan de dringende vraag van de VSSE aangaande een verhoging van haar personeels- en financiële middelen en een nauwkeurige bepaling van haar wettelijke opdrachten.

---

42 Waarbij de VSSE laat optekenen (14 april 2021): *"La Sûreté de l'Etat applique déjà la recommandation de constituer une 'capacité réservée', à la fois opérationnelle et d'analyse, mobilisable le cas échéant pour assurer un traitement adéquat aux informations reçues relatives aux organisations sectaires nuisibles et aux organisations criminelles, au cas où elles intéresseraient la sûreté de l'Etat ou le potentiel scientifique ou économique de la Belgique".* (De Veiligheid van de Staat past reeds de aanbeveling toe om een "gereserveerde capaciteit" op te zetten, zowel operationeel als voor analyse, die indien nodig kan worden gemobiliseerd om een passende behandeling te garanderen van ontvangen informatie met betrekking tot schadelijke sektarische organisaties en criminele organisaties, indien deze van belang zouden zijn voor de veiligheid van de Staat of voor het wetenschappelijk of economisch potentieel van België" (vrije vertaling)

Het Comité stelde dan ook dat een breder maatschappelijk (lees parlementair?[43]) debat over het in de Inlichtingenwet van 1998 voorziene takenpakket van de civiele inlichtingendienst en de hieraan gekoppelde prioriteitenstelling, zich opdringt. En bijgevolg, dat de toekenning van voldoende capaciteiten en middelen om het geheel van bedreigingen voor de nationale veiligheid dat behoort tot het takenpakket van de VSSE, het voorwerp dient uit te maken van een grondige discussie.

I.6. AANDACHT VAN DE BELGISCHE INLICHTINGENDIENSTEN VOOR EEN ADIV-MEDEWERKER EN ZIJN RELATIES MET RUSSISCHE BURGERS[44]

In 2014-2015 stelden de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) een gezamenlijk onderzoek in naar een reserve-officier van de (toenmalige) Directie I (Inlichtingen) van de ADIV.

Betrokkene kwam al in 2008 onder de aandacht van de VSSE na een melding van een buitenlandse partner. In 2012 wordt hij opnieuw vermeld en gesitueerd als een 'perifere doelwit' van een Russische oligarch. Twee jaar later wordt de VSSE zich bewust van zijn hoedanigheid van reserve-officier bij de militaire inlichtingendienst. Er wordt een samenwerking met de ADIV opgestart en elementen in het bezit van beide inlichtingendiensten lijken te wijzen op spionage. In februari 2015 trekt de ADIV zijn veiligheidsmachtiging in. De beslissing wordt door het gevatte Beroepsorgaan bevestigd. Het dossier wordt begin juli 2015 door de VSSE afgesloten. Betrokkene bleek op de hoogte te zijn gebracht van het onderzoek naar zijn persoon.

---

43 De VSSE denkt in dezelfde richting (14 april 2021): "*C'est au Parlement, tant dans sa fonction de législation que de controle du pouvoir exécutif, qu'il appartiendra d'apprécier si (considérant les moyens humains et matériels limités dont elle dispose et la gravité parfois extrême des nombreuses menaces liées à l'extrémisme, au terrorisme, à l'ingérence, à l'espionnage et à la prolifération auxquelles elle est confrontée in concreto) il est opportun ou bien d'exiger de la Sûreté de l'Etat qu'elle assure à nouveau le suivi actif des organisations sectaires nuisibles, ou bien de l'en décharger, ou bien de valider la décision du Conseil nationale de sécurité du 13 juillet 2015 approuvant la mise en suspens du suivi actif des organisations sectaires nuisibles.*" (Het is aan het Parlement om, zowel in zijn wetgevende functie als in zijn controle op de uitvoerende macht, te beoordelen of (gelet op de beperkte personele en materiële middelen waarover het beschikt en de soms extreme ernst van de vele dreigingen in verband met extremisme, terrorisme, inmenging, spionage en proliferatie waarmee het *in concreto* wordt geconfronteerd) het al dan niet passend is de Veiligheid van de Staat of te verplichten de actieve opvolging op schadelijke sektarische organisaties te hervatten, ofwel haar van deze taak te ontheffen, ofwel het besluit van de Nationale Veiligheidsraad van 13 juli 2015 tot goedkeuring van de opschorting van de actieve monitoring van schadelijke sektarische organisaties te bekrachtigen (vrije vertaling)).

44 Het kortstondige onderzoek had tot doel de Begeleidingscommissie te informeren n.a.v. het verzoek om inlichtingen aan het adres van het Vast Comité I van 6 juni 2019 van een lid van de parlementaire Begeleidingscommissie.

Het Vast Comité I kon op basis van de door de ADIV en de VSSE verzamelde en aan het Comité meegedeelde informatie niet besluiten of er al dan niet sprake was van spionage in hoofde van betrokkene. Sinds de uitspraak van het Beroepsorgaan heeft betrokkene Defensie verlaten.

I.7. VEILIGHEIDSSCREENINGS VAN MILITAIREN EN BURGERPERSONEEL BIJ DEFENSIE

Jaarlijks onderzoeken de Veiligheid van de Staat en de Algemene Dienst Inlichtingen en Veiligheid meerdere duizenden personen die een of andere vergunning of toelating willen bekomen of die een bepaalde functie willen bekleden. Met deze onderzoeken willen ze nagaan of de betrokkenen voldoende garanties bieden op het vlak van betrouwbaarheid en veiligheid. Eerder opende het Comité een breder toezichtonderzoek naar de wijze waarop de inlichtingendiensten dergelijke veiligheidsscreenings[45] uitvoeren.[46]

In het verlengde van dit onderzoek kon worden vastgesteld dat bepaalde personeelsleden binnen Defensie bij hun kandidaatstelling, aanwerving of in de loop van hun carrière nooit of slechts éénmalig aan een dergelijke veiligheidsscreening worden/werden onderworpen. Daarop bestudeerde het Vast Comité I de screening van militairen en burgerpersoneel bij Defensie (I.7.1), alsook de screening van de studenten van de Koninklijke Militaire School (I.7.2.).

I.7.1. DE SCREENING VAN MILITAIREN EN BURGERS BIJ DEFENSIE

De Wet van 28 februari 2007 tot vaststelling van het statuut van de militairen en kandidaat-militairen van het actief kader van de Krijgsmacht beschrijft, onder meer, de wervingsprocedure.

Kandidaten moeten aan verschillende voorwaarden voldoen: ze moeten de burgerlijke en politieke rechten genieten en blijk geven van de onontbeerlijke morele kwaliteiten (artt. 8 en 9). Ook mogen ze geen negatief veiligheidsadvies hebben gekregen (na een veiligheidsverificatie) of deze veiligheidsverificatie niet

---

45 Onder 'veiligheidsscreenings' wordt begrepen: *"een door of krachtens de wet opgelegde beoordeling door een administratieve overheid op basis van eigen of aangeleverde (persoons)gegevens waarbij uitgemaakt wordt of een private (rechts)persoon een profiel vertoont waaruit een risico blijkt dat hij/zij een niet-geëigend gebruik zal of zou kunnen maken van een bepaalde toelating en daarbij of daardoor bepaalde fundamentele (staats)belangen in het gedrang kan brengen zodat diezelfde of een andere (buitenlandse) overheid geïnformeerd kan beslissen over de toekenning, intrekking of beperking van die toelating"*.

46 VAST COMITÉ I, *Activiteitenverslag 2019*, 2 e.v. ('De uitvoering van veiligheidsscreenings door de inlichtingendiensten').

hebben geweigerd. Dit betekent dat behoudens indien de loopbaan van betrokkene een wijziging van het veiligheidsniveau zou vereisen, de militairen van het departement Defensie slechts één veiligheidsscreening tijdens hun volledige militaire loopbaan ondergaan. Het Comité was de mening toegedaan dat de vraag diende te worden gesteld of een dergelijke veiligheidsverificatie niet periodiek zou moeten worden herhaald tijdens de loopbaan van het militair personeel.[47]

Een andere regeling geldt voor wat betreft de burger(kandidaten) bij Defensie.[48] De overgrote meerderheid van het burgerpersoneel (1100 personen) zijn statutair; deze ambtenaren zijn benoemd en hebben de eed afgelegd. Een tweede groep burgers bestaat uit contractuelen die, net als in de privésector, op basis van een arbeidsovereenkomst worden aangeworven. Daarnaast zijn er ook burgers die niet als Defensiepersoneel worden beschouwd (bijv. onderzoekers aangeworven door het Patrimonium, gedetacheerde docenten van de Gemeenschappen bij de Koninklijke School voor Onderofficieren…). Alle aanwervingen van burgers, met uitzondering van de Rosetta-contracten[49], verlopen verplicht via SELOR.

Enkele uitzonderingen niet te na gesproken[50], wordt het burgerpersoneel van het departement Defensie niet onderworpen aan een veiligheidsverificatie. Het Comité was de mening toegedaan dat dit verschil in behandeling slechts kan worden gerechtvaardigd indien het ongepaste gebruik van de functie die zij uitoefenen, de fundamentele belangen van de Staat niet in gevaar kan brengen.

Het Vast Comité I bracht in dat kader de gevolgen van de evolutie van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen onder de aandacht. Immers, naast een mogelijke of concrete dreiging in een gebouw of plaats, kunnen sommige sites inherent (en permanent) gevoelig zijn voor dreigingen: de tarmac van een luchthaven, een basis van Defensie, enz. Het ongeëigende gebruik van de mogelijkheid om toegang te verkrijgen tot een dergelijke site kan ernstige schade toebrengen aan fundamentele belangen van de Staat. Hetzelfde geldt voor personen die een specifieke functie of opdracht uitoefenen of die een specifieke toelating willen verkrij-

47 Het blijkt immers dat de integriteit van sommige militairen wel degelijk een probleem kan vormen. Dit betekent dat deze leden alleen als zodanig bekend zullen zijn wanneer zij een bedreiging vormen die door de ADIV werd opgespoord.

48 Met inbegrip van de leden van de Dienst voor religieuze en morele bijstand (DRMB).

49 Rosetta-contracten of 'startbaanovereenkomsten' zijn contracten van een jaar die worden aangeboden aan jongeren onder de 26 jaar. Defensie organiseert de aanwervingsgesprekken zelf naargelang van haar behoeften.

50 Bijv. diegenen die worden aangeworven of gedetacheerd bij de ADIV, aangezien houder zijn van een veiligheidsmachtiging een van de essentiële voorwaarden is om er te kunnen worden tewerkgesteld.

gen. Aanvankelijk stond de wet toe dat 'elke administratieve overheid' dergelijke (positieve) adviezen kon vragen.[51]

De Wet van 23 februari 2018 en het KB van 8 mei 2018[52] hebben de procedure voor het veiligheidsadvies hervormd, zowel op het niveau van de reglementaire beslissing van de administratieve overheid als op het niveau van het individuele beslissingsmechanisme.

I.7.2. EEN VEILIGHEIDSSCREENING VOOR DE (BUITENLANDSE) STUDENTEN VAN DE KONINKLIJKE MILITAIRE SCHOOL?

De Koninklijke Militaire School (KMS) is een militaire instelling voor universitair onderwijs belast met de academische, militaire en fysieke basisvorming van toekomstige officieren, en met de voortgezette vorming van officieren tijdens hun loopbaan bij Defensie.[53]

De KMS opent haar deuren voor buitenlande studenten. De Veiligheid van de Staat merkte evenwel opdat [54]: " *[u]niversiteiten doorgaans open staan voor internationale samenwerking, wat alleen maar kan worden toegejuicht. Maar deze openheid is niet zonder risico. Ook andere actoren zijn zich bewust van de kennis die aan onze universiteiten te rapen valt. […] Studenten van militaire onderzoeksinstituten, zoals het Chinese National University of Defense Technology, worden uitgestuurd naar verschillende westerse landen waaronder België, waar ze kennis verwerven die essentieel is voor bepaalde militaire ontwikkelingen. De kennis die ze er opdoen, nemen ze mee naar het leger in hun thuisland. Aan de Belgische universiteiten zijn momenteel enkele tientallen van deze militaire studenten actief.*"

Ook het Vast Comité I was de mening toegedaan dat Defensie een kwetsbaarheid vertoont bij het toelaten van studenten uit het buitenland. Er bestaat namelijk

---

51 De beslissing (van reglementaire aard) om een (individueel) veiligheidsadvies te eisen kon enkel worden genomen "*wanneer de uitoefening van een beroep, een functie, een opdracht of mandaat, of de toegang tot lokalen, gebouwen of terreinen, of het bezit van een vergunning, een licentie of een toelating door een niet-geëigend gebruik schade kon toebrengen aan de verdediging van de onschendbaarheid van het nationaal grondgebied en van de militaire defensieplannen, de vervulling van de opdrachten van de strijdkrachten, de inwendige veiligheid van de Staat, met inbegrip van het domein van de kernenergie, en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de Staat en de internationale betrekkingen van België, het wetenschappelijk en economisch potentieel van het land, de veiligheid van de Belgische onderdanen in het buitenland of de werking van de besluitvormingsorganen van de Staat*".

52 Wet van 23 februari 2018 houdende wijziging van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS*, 1 juni 2018) en Koninklijk besluit van 8 mei 2018 tot wijziging van het koninklijk besluit van 24 maart 2000 tot uitvoering van de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (*BS*, 1 juni 2018).

53 De KMS biedt onder meer een basisstafvorming (BStV), een vorming voor Kandidaat Hoofdofficieren (VKHO) en een Hogere Stafopleiding (HStO) aan. Zie www.rma.ac.be

54 https://www.vsse.be/sites/default/files/paragraphs/1-ra2020-nl-version10-single-light.pdf

een aanzienlijk risico van spionage en inmenging voor bepaalde personen, die bovendien toegang krijgen tot informatie van Defensie.

De toelating van buitenlandse studenten vereist volgens het Comité dan ook een voorafgaande en systematische risicoanalyse per geval van de kandidaat-leerling door de ADIV.

I.8. DE OPVOLGING VAN POLITIEKE MANDATARISSEN

I.8.1. INTRODUCTIE

Veelvuldig werd in (parlementaire) debatten[55] de vraag gesteld of en in welke mate de Belgische inlichtingendiensten politieke mandatarissen (mogen) opvolgen en welke regels ze daarbij in acht moeten nemen.[56] Vanaf begin 2018 wordt in deze binnen de VSSE een als 'vertrouwelijk' geclassificeerde dienstnota toegepast. Conform deze nota, die werd geactualiseerd in juni 2020[57], zendt de VSSE twee types van rapporten naar de minister van Justitie en de Premier, met kopie naar het Vast Comité I. Het betreft enerzijds punctuele rapporten over politieke mandatarissen die bijdragen aan de totstandkoming van een dreiging alsook een trimestrieel overzicht van het geheel van documenten waarin melding wordt gemaakt van deze mandatarissen.[58] De minister van Justitie stemde daarbij in met het *'principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991*'.[59]

Gezien nergens wordt vermeld wat het Comité wordt geacht aan te vangen met voormelde informatie, nam het zelf het initiatief een methodologie uit te werken

---

55 Zie recent nog: Vraag van S. Creyelman aan de minister van Justitie over de 'politieke dossiers bij de VSSE' (*Vr. en Ant*. Kamer 2019-20, 16 juli 2020, QRVA 23, 33, Vr. nr. 351).

56 VAST COMITÉ I, *Activiteitenverslag 2019*, 69-70 ('IV.3. Toezicht op de opvolging van politieke mandatarissen').

57 De dienstnota van 13 december 2017 werd in juni 2020 geactualiseerd om de rapportage ten aanzien van de directie inzake disruptieve activiteiten te verbeteren. Ondanks herhaaldelijk verzoek mocht het Comité van de ADIV – die net zoals de VSSE werd aangespoord tot aanname van een uniforme richtlijn met klare en eenduidige regels met betrekking tot de inwinning, verwerking, raadpleging, opslag en archivering aangaande politieke mandatarissen, geen informatie in die zin ontvangen. De ADIV beschikte niet over een specifieke procedure (SOP) om met deze informatie om te gaan noch werd bepaald hoe het Vast Comité I hiervan op de hoogte te brengen

58 De bedoelde politieke mandatarissen zijn de ministers van de diverse regeringen, de Belgische commissaris in de Europese Commissie en de leden van de verschillende Parlementen, inclusief de Belgische leden van het Europees Parlement. Het gaat niet om andere verkozenen of aangeduide mandatarissen (bijv. op gemeentelijk vlak, zoals schepenen, of op provinciaal vlak, bijv. de gouverneurs).

59 *'met het toezichtsbeginsel/beginsel van verificatie/ dat noodzakelijk blijkt conform de organieke wet van 18 juli 1991'* (vrije vertaling) In: Brief van de minister van Justitie gericht aan het Vast Comité I d.d. 26 juli 2018 over 'Le recueil d'informations par un service de renseignement concernant une persone exerçant un mandat politique'.

omtrent de 'problematiek van de opvolging van de politieke mandatarissen door de inlichtingendiensten en de rol van het Vast Comité I'. Deze methodologie werd in 2020 door de parlementaire Begeleidingscommissie goedgekeurd. In navolging van deze methodologie werd in 2020 een (periodiek) toezichtonderzoek opgestart.[60] Het onderzoeksveld hierbij was hoe vaak tijdens de referteperiode (van 1 september 2019[61] tot en met 31 augustus 2020) over een mandataris informatie werd verzameld, verwerkt en gerapporteerd. Tevens werd bestudeerd of de informatieverzameling al dan niet wettig of 'disproportioneel' was en of de eerder door het Comité geformuleerde aanbevelingen werden uitgevoerd.[62]

Daartoe stelde het Vast Comité I een lijst op van de (543) personen die tussen de referentieperiode een uitvoerend politiek mandaat bekleedden op Europees, federaal, gewestelijk en gemeenschapsniveau.[63]

Deze lijst werd respectievelijk eind oktober 2020 overgemaakt aan de VSSE en de ADIV. De VSSE bezorgde het Comité de lijsten van relevante documenten opgesteld door haar buitendiensten en de analysedienst. De ADIV meldde dat de dienst tijdens de referteperiode geen Belgische politieke mandatarissen had gevolgd of onderzocht.

I.8.2. VASTSTELLINGEN AANGAANDE DE UITVOERING VAN DE AANBEVELINGEN VAN HET VAST COMITÉ I

I.8.2.1. De uitwerking van richtlijnen met betrekking tot de inwinning, de verwerking, de raadpleging, de opslag en de archivering van gegevens

In 2008 beval het Vast Comité I de uitwerking aan van klare en eenduidige richtlijnen met betrekking tot de inwinning, de verwerking, de raadpleging (met inbegrip

---

60 Het Comité voerde hieromtrent eerder al toezichtonderzoeken uit. Zie VAST COMITÉ I, *Activiteitenverslag 1998*, 67 e.v. ; *Activiteitenverslag 1999*, 12 e.v., *Activiteitenverslag 2008*, 23 e.v. ; *Activiteitenverslag 2013*, 3 ('I.I.3. Een nieuwe dienstnota van de VSSE over de opvolging van parlementsleden').

61 Start van de huidige federale legislatuur - parlementaire zittingsperiode 55 (2019- 2024).

62 VAST COMITÉ I, *Activiteitenverslag 2013*, 3 ('I.I.3. Een nieuwe dienstnota van de VSSE over de opvolging van parlementsleden').

63 In concreto betreft het: a) de ministers van de Vlaamse regering, de *Fédération Wallonie-Bruxelles*, de Waalse gewestregering, de Duitstalige gemeenschapsregering, de Brusselse regering, de federale regering en de Belgische commissarissen in de Europese commissie; b) de leden van de gemeenschaps- en gewestparlementen (*Fédération Wallonie-Bruxelles*, Waals gewest, Brussels Hoofdstedelijk Gewest, Vlaams parlement en Duitstalige gemeenschap), het federaal parlement (Kamer en Senaat) en van de Belgische leden in het Europees Parlement; en c) met uitzondering van voorzitters van politieke partijen die geen lid zijn van een parlement en geen uitvoerend mandaat bekleden van eerdergenoemde niveaus, leden van de Koninklijke familie, ministers van Staat, lokale mandatarissen (burgemeesters, schepenen, gemeenteraadsleden, leden van intercommunales) voor zover ze geen regionaal/gemeenschaps-/federaal/Europees mandaat bekleden, gouverneurs en ex-mandatarissen zonder actueel mandaat.

van de eventuele interne afscherming), de opslag en de archivering van gegevens van bepaalde categorieën van personen die bijzondere verantwoordelijkheden dragen of droegen. [64]

In juni 2020 legde de VSSE nieuwe interne richtlijnen vast inzake de geactualiseerde procedures en '*de meldingsplicht van de VSSE aan de minister van Justitie zodra bepaalde politieke mandatarissen opduiken in documenten van de VSSE*'.[65] De dienstnota verving drie eerdere dienstnota's over hetzelfde onderwerp.[66] Begin december 2020 verstuurde de VSSE een nota aan onder meer de politieke partijen die vertegenwoordigd zijn in het Federale Parlement met toelichting over de gehanteerde procedure wanneer politieke mandatarissen genoemd worden in het kader van onderzoeken van de VSSE.[67]

Niettegenstaande zijn aanbevelingen uit 2013[68], mocht het Vast Comité I van de ADIV geen informatie ontvangen dat het in een specifieke procedure (SOP)

64 VAST COMITÉ I, *Activiteitenverslag 2013*, 3 ('I.I.3. Een nieuwe dienstnota van de VSSE over de opvolging van parlementsleden')

65 VSSE, Dienstnota van 11 juni 2020.

66 De dienstnota van 4 juli 2013 met als onderwerp '*Wijzigingen voor het opstellen van documenten die in VESTA opgeslagen zijn*', de dienstnota van 25 juli 2013 met als onderwerp '*Dienstnota omtrent het linken van parlementsleden en politieke mandatarissen in documenten van de VSSE*' en de dienstnota van 13 december 2017 met als onderwerp '*de meldingsplicht van de VSSE aan de minister van Justitie zodra bepaalde politieke mandatarissen opduiken in documenten van de VSSE*'.

67 Procedure politieke mandatarissen inzake: '*Vermelding van een politiek mandataris in de databank van de VSSE*', '*Indien de politiek mandataris het slachtoffer is van een dreiging*', '*De veronderstelde of bewezen betrokkenheid van een politiek mandataris bij de totstandkoming van een dreiging*' (Nota VSSE).

68 VAST COMITE I, *Activiteitenverslag* 2013, 112 ('IX.1.2. Een richtlijn over inlichtingenwerk t.a.v. personen met bijzondere verantwoordelijkheden en politieke partijen' en 'IX.1.3. Eénduidige richtlijnen omtrent het melden van de opvolging van politici').

voorzag om met deze informatie om te gaan, noch werd een procedure bepaald om het Vast Comité I op de hoogte te brengen.[69]

I.8.2.2. Bijzondere aandacht voor de positie van de vermelde politieke mandatarissen

Het Vast Comité I beval aan dat de inlichtingendiensten in hun rapportage de nodige aandacht moesten besteden aan de hoedanigheid van een in een verslag vermeld persoon ten aanzien van de dreiging (slachtoffer, actor, passant…). Politieke mandatarissen kunnen te allen tijde (in de uitvoering van hun mandaat/in de marge van een dreiging) voorkomen in de informatie die de inlichtingendiensten verzamelen. Ze kunnen genoemd worden door menselijke bronnen, opduiken in berichten van partnerdiensten, voorkomen in lijsten die ontstaan door toepassing van technische middelen (bijv. telefonielijsten). In dergelijke gevallen loopt de politicus eerder toevallig door het beeld van de inlichtingendiensten.

De dienstnota van de VSSE bevat de bepaling dat politieke mandatarissen die voorkomen in documenten van de VSSE enkel 'gelinkt' mogen worden indien ze rechtstreeks in verband te brengen zijn met een dreiging als slachtoffer of als dader zoals bedoeld in de Inlichtingenwet.

Uit nazicht van de bedoelde documenten bleek evenwel dat de hoedanigheid van de vermelde politieke mandatarissen onvoldoende duidelijk stond aangegeven.

---

[69] Op 30 november 2017 meldde de ADIV het Vast Comité I dat sinds de aanbevelingen van 2013 de Organieke Wet van 1998 enkele malen geamendeerd of gewijzigd werd, stellende dat geen politieke of wetgevende autoriteit te kennen gegeven hadden dat er dergelijke regels dienden te worden opgesteld met betrekking tot het opvolgen van politieke verantwoordelijken. De opvolging van politieke verantwoordelijken door de ADIV had volgens deze laatste nog geen schade toegebracht aan de vrijheid van vereniging of meningsuiting en indien dit wel het geval zou zijn, zou dit gebaseerd zijn op de Organieke Wet die in overeenstemming is met de Universele Verklaring van de Rechten van de Mens en met de uitspraken van het Europees Hof voor de Mensenrechten, in die zin dat voorzien wordt dat in bepaalde speciale, welomschreven situaties kan worden ingegaan tegen één of ander fundamenteel recht. Ondanks deze vaststelling was de ADIV van mening dat alle initiatieven die de democratische controle op de inlichtingendiensten konden versterken dienden te worden aangemoedigd en dat ook de ADIV zelf in deze versterking een cruciale rol kon spelen. Vanuit deze optiek nam de ADIV het initiatief om contact op te nemen met de VSSE om zich te beraden over de genoemde aanbeveling(en). Aanvullend meldde de ADIV het Vast Comité I op 6 december 2017 dat het het voornemen had om in de loop van 2018 gelijkaardige procedures als die van de VSSE uit te werken om de democratische controleorganen te informeren, met dien verstande dat het uitwerken van dergelijke procedures ook gekoppeld moest worden aan het uitwerken van interne procedures betreffende het opslaan en archiveren van informatie over de betreffende politieke mandatarissen en organisaties. Het uitwerken van deze procedures diende deel uit te maken van een ruimer project dat voorziet in het opstellen van een aantal interne richtlijnen voor het functioneren van (kader)personeel van de ADIV. De audit van het Vast Comité I naar het functioneren van de Directie CI en van de ADIV, in februari en maart 2018, en de publicatie van de resultaten van deze audit op 15 mei 2018, doorkruisten de plannen van de ADIV om de genoemde procedures uit te werken. De ADIV oordeelde evenwel dat het verstandig zou zijn de conclusies af te wachten van het Business Process Re-engineering (BPR), het interne hervormingsproces van de ADIV dat er kwam als gevolg van de audit van het Vast Comité I. Op 6 januari 2020 ging de ADIV van start met zijn nieuwe structuur.

I.8.2.3. De uitwerking van artikel 19 W.I&V[70]

Bovenvernoemde dienstnota bepaalt dat een overzicht van alle documenten waarin politieke mandatarissen opduiken om de drie maanden door de VSSE aan het Vast Comité I wordt overgemaakt. Het overzicht bevat referenties van documenten die ruwe informatie bevatten en analysedocumenten. Het overzicht geeft ook aan welke nota's (zie verder) aan de minister van Justitie en de Premier werden overgemaakt.[71]

Ook wat de ADIV betreft, beveelde het Vast Comité I aan om haar driemaandelijks een overzicht te bezorgen van alle documenten waarin politieke mandatarissen worden vermeld.

I.8.3. DE COLLECTE, DE ANALYSE EN DE VERSPREIDING VAN INLICHTINGEN OVER POLITIEKE MANDATARISSEN TUSSEN 2019 EN 2020

I.8.3.1. Collecte en analyse

Tijdens de referentieperiode, werden van de 543 politieke mandatarissen:
- 267 of 49,17% niet opgenomen in de VSSE-databank;
- 124 of 22,84% opgenomen in de VSSE-databank, maar zonder link met een dreiging;
- 152 of 28% opgenomen in de VSSE-databank met vermelding in door de VSSE opgestelde (828) analysedocumenten over een dreiging.

Van de 828 documenten, zijn 53% (439) onderzoeksrapporten, 25% (206) documenten afkomstig van een externe (inter)nationale partner, 6% (53) nota's aan de Belgische autoriteiten en 16% (130) voornamelijk synthesefiches waarbij een interne analyse gemaakt wordt van een dossier en notulen van een vergadering.

---

70 "Art. 19 W.I&V : "*De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook aan de instanties en personen die het voorwerp zijn van een dreiging bedoeld in de artikelen 7 en 11.*
Met eerbiediging van de persoonlijke levenssfeer van de personen en voor zover de voorlichting van het publiek of het algemeen belang dit vereist, mogen de administrateur-generaal van de Veiligheid van de Staat en de chef van de Algemene Dienst Inlichting en Veiligheid, of de persoon die elk van hen aanwijst, inlichtingen aan de pers mededelen.".

71 De minister van Justitie en de Premier worden niet geïnformeerd over het louter accidenteel opduiken van politieke mandatarissen in documenten van de VSSE.

I.8.3.2. De verspreiding van inlichtingen

De VSSE bezorgt elke trimester aan de Premier en de minister van Justitie, met kopie aan het Vast Comité I, een overzicht van alle documenten in dewelke politieke mandatarissen voorkomen.

Daarnaast worden, zodra er op basis van beschikbare informatie een 'vermoeden' van betrokkenheid van een politieke mandataris bestaat bij de totstandkoming van een dreiging, de minister van Justitie en de Premier, met kennisgeving aan het Vast Comité I, geïnformeerd (meldingsfiches). Deze fiches kunnen worden vervolledigd met gedetailleerde geanalyseerde en geverifieerde informatie dat de notificatie aan de overheden rechtvaardigt. Tijdens de referentieperiode werden vijf van dergelijke meldingsfiches opgesteld voor evenveel mandatarissen.

Verder deelt de VSSE ook informatie mee over politieke mandatarissen wiens naam verschijnt in sommige documenten, zonder dat deze evenwel betrekking hebben op een concrete dreiging. Deze informatie, die wordt gedeeld via de zogenaamde '*notes aux autorités*, vermeldt de VSSE (minstens) de beschrijving van de wijze waarop de politieke mandataris bijdraagt tot de totstandkoming van de dreiging, een inschatting van de mogelijke gevolgen die deze betrokkenheid kan doen ontstaan of heeft doen ontstaan (voor zover daar zicht op is) en hoe het dossier verder zal worden opgevolgd door de VSSE.

Tijdens de referentieperiode maakten 17 op 543 politieke mandatarissen (3,13%) het voorwerp uit van 53 *notes aux autorités* (21 i.v.m. extremisme, 25 i.v.m. spionage en inmenging, en 7 andere, zoals bijv. criminele organisaties en corruptie).

I.8.4. RESPECT VOOR DE GRONDRECHTEN VAN POLITIEKE MANDATARISSEN

Het Vast Comité I vond geen aanwijzingen dat de VSSE politieke mandatarissen viseerde om redenen buiten de wettelijk opgesomde belangen en bedreigingen om, noch dat zij anders worden behandeld dan andere beroepsgroepen.

Uit het onderzoek van de *notes aux autorités* bleek niet dat bij de informatievergaring, -analyse en -verspreiding de grondrechten van de politieke mandatarissen niet werden gerespecteerd.

Steunend op de criteria opgenomen in de door de Begeleidingscommissie goedgekeurde methodologie, bleek uit het onderzoek dat politieke mandatarissen niet op disproportionele wijze voorkomen in de documenten van de VSSE.

I.9. HET OPSPOREN EN OPVOLGEN VAN DE RADICALISERING VAN EEN MILITAIR: DE ZAAK-JÜRGEN CONINGS

Midden mei 2021 verliet Jürgen Conings, door het Coördinatieorgaan voor de dreigingsanalyse (OCAD) gelabeld als 'potentieel gewelddadig extremist (PGE)[72]' in het bezit van wapens de kazerne van Leopoldsburg. Op het ogenblik van zijn verdwijning was betrokkene als korporaal-chef tewerkgesteld bij Defensie. Al snel wordt duidelijk dat betrokkene al bekend was bij de politie-, inlichtingen- en veiligheidsdiensten (*infra*). De zaak beroert de publieke opinie en roept, terecht, heel wat (parlementaire) vragen op.[73]

Op verzoek van de minister van Defensie opende het Vast Comité I het *'toezichtonderzoek naar het opsporen en opvolgen – door de twee inlichtingendiensten – van de radicalisering van een militair werkzaam bij Defensie, en anderzijds naar hun samenwerking met hun partnerdiensten, waaronder Defensie, onder meer wat betreft hun informatie-uitwisseling'*.

De minister van Defensie had daarbij drie opdrachten voor ogen: (a) de betrouwbaarheid na te gaan van informatie over personen die verdacht worden van radicalisering binnen Defensie en (b) een samenwerking bewerkstelligen met de inspecteur-generaal van Defensie belast met een audit die meer in het bijzonder betrekking had op de aspecten van het personeelsbeheer, en c) een reeks aanbevelingen te formuleren om de goede werking van de ADIV, maar ook van Defensie in haar geheel, te garanderen.

Wat betreft de rol van het OCAD in deze, werd samen met het Vast Comité P een '*gezamenlijk toezichtonderzoek naar de rol van het OCAD in de opvolging van Jürgen Conings, met name voor wat betreft het ingestelde vooronderzoek, de dreigingsevaluatie niveau 3 en de gevolgen daarvan, en de informatie-uitwisseling over betrokkene*' opgestart.[74] De onderzoeksrapporten werden begin juli 2021 besproken met de parlementaire Begeleidingscommissie.

---

72 De 'PGE' vormen één van de categorieën van de gemeenschappelijke gegevensbank Terrorist Fighters waarvan het OCAD operationeel beheerder is. De als PGE ingeschreven entiteiten moeten voldoen aan een aantal criteria zoals gedefinieerd in het KB van 20 december 2019 tot wijziging van het Koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank terrorist fighters en van het Koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis 'Het informatiebeheer' van hoofdstuk IV van de wet op het politieambt, *BS* 27 januari 2020. Hierover : *VAST COMITÉ I, Activiteitenverslag 2020*, 128 ('VI.1.1. De toevoeging van potentieel gewelddadige extremisten in de GGB TF').

73 Zie bijv. Actualiteitsdebat over de voortvluchtige militair (Commissie voor Landsverdediging), *Hand.* Kamer 2020-21, 26 mei 2021, CRIV55COM490 en de debatten naar aanleiding van het verlag van de Inspecteur-generaal: *Hand.* Kamer 2020-2021, 16 juni 2021, CRIV55COM519.

74 Zie 'I.10. De rol van het OCAD in de opvolging van de militair Jürgen Conings'.

I.9.1. EEN BEELD VAN DE PROFESSIONELE LOOPBAAN VAN JÜRGEN CONINGS

Het professionele parcours van Jürgen Conings is een kluwen van affectaties en mutaties, buitenlandse missies[75], opleidingen allerhande[76] en bijklussen in de private bewakingssector. De carrière van de militair, aangevangen in 1992, wordt gekenmerkt door verschillende affectaties tot aan zijn mutatie in juni 2020, op zijn vraag, naar de *Cel Pre-Deployment Training for Individual Augmentees* (PDT-IA[77]) een eenheid in Leopoldsburg die instaat om militairen voor te bereiden op buitenlandse missies. Hij was er logistiek medewerker en in die hoedanigheid onder meer verantwoordelijk voor het uithalen van wapens en munitie voor schietoefeningen.

In 2015 komt hij voor het eerst in het vizier van de Veiligheid van de Staat. Betrokkene kreeg in de schoot van Defensie steeds goede evaluaties, ondanks een sanctie (een arrest van vier dagen) voor racistische uitlatingen op Facebook in november 2019.[78] Het rapport van het Inspectoraat-generaal van Defensie maakt ook melding van psychosociale factoren.[79]

In maart 2020 solliciteert hij bij de Federale Politie voor de functie van veiligheidsagent, maar wordt afgekeurd op basis van zijn persoonlijkheidstest. Parallel met zijn affectaties bij Defensie, loopt zijn parcours in de private veiligheidssector als bewakingsagent.

Op 31 augustus 2020 wordt zijn veiligheidsmachtiging niet verlengd. Dezelfde dag wordt hij door het OCAD in 'vooronderzoek potentieel gewelddadig extremist' (PGE) geplaatst. Op 17 februari 2021 krijgt hij het full statuut 'PGE niveau 3' (art. 6, §1, 1°/2 KB TF). Op 3 maart 2021 wordt zijn sociale promotie geannuleerd. Op 17 mei 2021 kan hij ongestoord de kazerne in Leopoldsburg verlaten in het bezit van wapens en de volgende dag wordt zijn verdwijning gesignaleerd. Sinds 21 mei 2021 werd een onderzoeksrechter gevorderd voor 'moordpoging in een terroristische context' en 'verboden wapenbezit in een terroristische context'. De procedure voor ambtsontheffing werd opgestart. Op 20 juni 2021, vijf weken na zijn verdwijning, wordt hij levenloos aangetroffen.

Jürgen Conings maakte deel uit van een dertigtal[80] militairen die wegens hun extreemrechts gedachtengoed werden opgevolgd door de militaire inlichtingen-

---

75 Onder meer in ex-Joegoeslavië (BELBAT), in Afghanistan (Resolute Support Mission) en in Jordanië (Operation Desert Falcon).

76 Onder meer opleidingen voor rollend materiaal, technische opleidingen (*technic worker*, magazijnbeheer, radio herstelling…) en diverse wapenopleidingen.

77 Deze cel van de Landcomponent is verantwoordelijk voor de voorbereiding van militairen uit heel Defensie die als individu zullen deelnemen aan operaties. Hierbij kan worden gedacht aan militairen die ingezet worden in bepaalde opdrachten, los van een groot detachement gelinkt aan hun eigen eenheid of zelfs component.

78 Het motief luidt: *"Betrokkene heeft op sociale media een mening geuit die niet strookt met de waarden van Defensie en schade toebrengt aan het imago van Defensie"*.

79 Inspectoraat-generaal, Eindrapport E2103, Intern onderzoek PDT-IA, Beperkte verspreiding.

80 Ter vergelijking, de politiediensten volgen bijna 2500 personen op in het rechts-extremistische milieu.

dienst.[81] Bij zijn verdwijning kreeg hij de steun van ex-militair Tomas Boutens, voortrekker van de neonazigroepering Bloed, Bodem, Eer & Trouw.[82] Op een van zijn Facebookprofielen verwees hij naar de 'Siegrune', een runenteken dat in nazi-Duitsland werd gehanteerd. Meer nog dan de sporadische contacten met Boutens, bleek hij opgemerkt in de kringen van het Vlaams Legioen[83], waar hij gevechtstraining zou hebben gegeven. Jürgen Conings dook ook op op de Facebookgroep *Knights of Flanders*, een vereniging van extreemrechtse signatuur.

I.9.2. HET JURIDISCH EN BELEIDSMATIG KADER

Alvorens de informatiepositie van de inlichtingendiensten aangaande Jürgen Conings te evalueren, was het van belang de bevoegdheden van de VSSE en de ADIV te duiden in het kader van het detecteren, opvolgen en bestrijden van het terrorisme, extremisme en radicalisme.

I.9.2.1. De inlichtingenopdracht van de VSSE en de ADIV

De taakstelling van de VSSE binnen de strijd tegen het terrorisme, extremisme en radicalisme situeert zich in hoofdorde binnen haar inlichtingenopdracht (art. 7, 1° W.I&V). De wetgever heeft hierbij geopteerd om een limitatieve lijst op te stellen van veiligheidsdreigingen die behoren tot het bevoegdheidsdomein van de VSSE. Art. 8, 1°, tweede lid, b en c W.I&V definiëren de dreigingen die het voorwerp van het toezichtonderzoek uitmaakten, te weten terrorisme en extremisme.

Ook de werkzaamheden van de ADIV binnen de aanpak van het terrorisme, extremisme en radicalisme situeren zich in hoofdorde binnen zijn inlichtingenopdracht zoals gedefinieerd in artikel 11, §1, 1° W.I&V. Net zoals bij de VSSE dient de ADIV bepaalde fundamentele belangen van het land te vrijwaren door middel van de detectie, opvolging en bestrijding van bepaalde bedreigingen tegen deze belangen. Er bestaan ook verschillen met de bevoegdheidsomschrijving van de VSSE. Het belangrijkste verschil bestaat in de vereiste aanwezigheid van een militair as-

---

81 Extreemrechtse invloeden in militaire rangen is geen uniek Belgisch fenomeen en evenmin nieuw. In de Duitse elite-eenheid *Kommando Spezialkräft* (KSK) zijn sinds 2017 vijftig militairen verdacht van rechts-extremistische activiteiten. Recent was er in Frankrijk ongerustheid over een staatsgreep door ex-generaal uit (extreem-)rechtse kringen en ook in Nederland verlieten de afgelopen vijf jaar meerdere militairen de Krijgsmacht na extreemrechtse uitingen of gedragingen. Eind jaren '90 van vorige eeuw waarschuwde de toenmalige minister van Defensie al dat een para-bataljon nabij Antwerpen niet mocht worden aangetast door fascistische en racistische tendensen.

82 Boutens werd samen met zestien andere personen (zowat twee derden van de toenmalig gearresteerden bleken beroepsmilitair) veroordeeld tot vijf jaar gevangenisstraf wegens het plannen van terreuracties en het verspreiden van geweldsverheerlijkende ideologie. Boutens was één van de eersten die op Facebook zijn steun aan de voortvluchtige betuigde.

83 Een rechts-extremistische groupuscule die 'strijdt voor het Vlaamse volk en voor Vlaanderen'.

pect, ofwel in het te beschermen belang (bijv. de militaire defensieplannen, de vervulling van de militaire opdrachten), ofwel in de wijze waarop de te beschermen belangen aangetast kunnen worden, zijnde met middelen van militaire aard (bijv. militaire wapens, defensiepersoneel).

De door beide diensten verkregen inlichtingen, of met andere woorden de gecollecteerde en geanalyseerde informatie, worden vervolgens tijdig en doelgericht doorgegeven aan andere instanties.[84] Deze (in hoofdzaak politieke, administratieve, gerechtelijke, politionele, diplomatieke en militaire) instanties nemen uiteindelijk de nodige tegenmaatregelen ter bescherming van de nationale veiligheid.

De ruime wettelijke inlichtingenopdracht noodzaakt de inlichtingendiensten en hun beleidsverantwoordelijken om prioriteiten te leggen binnen de werkzaamheden. De VSSE en de ADIV hebben immers onvoldoende capaciteit en middelen ter beschikking om alle tot hun bevoegdheid behorende nationale veiligheidsdreigingen te detecteren, op te volgen en te beheersen (noch zou ze deze ooit kunnen hebben). De opdracht tot prioritisering is weggelegd voor de Nationale Veiligheidsraad (NVR).[85]

De NVR is eveneens belast met het bepalen van de nadere regels opdat de verschillende veiligheidsactoren zouden komen tot een effectieve samenwerking. Het Nationaal Strategisch Inlichtingenplan (NSIP), gezamenlijk opgesteld door de VSSE en de ADIV en in 2018 gevalideerd door de Nationale Veiligheidsraad *'beoogt'*, onder meer, *'de samenwerking tussen de twee inlichtingendiensten te optimaliseren om te komen tot een zo doeltreffend mogelijke uitvoering van een inlichtingenbeleid ten bate van de bevoegde instanties en van de bevolking.'*[86] In het (geclassificeerde) onderdeel 'Taakverdeling', worden de respectievelijke opdrachten van de VSSE en de ADIV bepaald wat betreft de aanpak van het terrorisme, extremisme en radicalisme.

---

84 Krachtens artikel 19 W.I&V zijn de bestemmelingen van de inlichtingen *'de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, (..) de politiediensten en (…) alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook (…) de instanties en personen die het voorwerp zijn van een dreiging bedoeld in de artikelen 7 en 11.'* De bestemmelingen van de informatie van de inlichtingendiensten zijn bijgevolg bepaalde politieke, bestuurlijke, gerechtelijke, politionele, diplomatieke en militaire overheidsinstanties. Daarnaast kunnen ook bedreigde personen of bedreigde instanties (bijv. een werkgever) in kennis gesteld worden van nuttige informatie.

85 Zoals voorzien in art. 10 W.I&V en art.2 van het koninklijk besluit van 22 december 2020 tot oprichting van de Nationale Veiligheidsraad, het Strategisch Comité voor inlichtingen en veiligheid en het Coördinatiecomité voor inlichtingen en veiligheid, *BS* 29 december 2020.

86 Nationaal Strategisch Inlichtingenplan, p. 4.

I.9.2.2. Het uitvoeren van veiligheidsscreenings door de twee inlichtingendiensten

Naast inlichtingenopdrachten hebben de VSSE en de ADIV ook veiligheidsopdrachten. In eerste orde moet hierbij het uitvoeren van veiligheidsscreenings vermeld worden.

Beide diensten voeren veiligheidsonderzoeken uit, te weten onderzoeken ten dienste van een veiligheidsoverheid (vnl. de Nationale Veiligheidsoverheid – NVO) waarin wordt nagegaan of een persoon aan de voorwaarden inzake geheimhouding, loyauteit en integriteit voldoet die aanwezig dienen te zijn voor het verkrijgen of behouden van een veiligheidsmachtiging.[87] Verder zijn beide inlichtingendiensten belast met het uitvoeren van veiligheidsverificaties met het oog op het toekennen van een veiligheidsattest of -advies.

Binnen de Krijgsmacht vervult de ADIV eveneens de functie uit van veiligheidsoverheid. Dit wil zeggen dat ze, naast het uitvoeren van de veiligheidsonderzoeken en -verificaties, eveneens belast is met de afgifte van veiligheidsmachtigingen en veiligheidsadviezen. Het Comité stelde echter vast dat er binnen de Krijgsmacht geen algemene instructie bestaat waarbij op exhaustieve wijze de functies binnen Defensie worden opgesomd die houder moeten zijn van een veiligheidsmachtiging.

Krachtens de Wet van 28 februari 2007 tot vaststelling van het statuut van de militairen en kandidaat-militairen van het actief kader van de krijgsmacht wordt wel een positief veiligheidsadvies vereist voor elke kandidaat-militair (*cf.* art. 9, 9°). De wet legt evenwel geen periodieke veiligheidsscreening voor militairen op.

I.9.2.3. De verantwoordelijkheid van de ADIV inzake militaire veiligheid[88]

Naast de inlichtingenopdracht en het uitvoeren van veiligheidsonderzoeken en -verificaties, is de ADIV eveneens belast met *'het zorgen voor het behoud van de militaire veiligheid van het personeel dat onder de Minister van Landsverdediging ressorteert, de militaire installaties, wapens en wapensystemen, munitie, uitrusting,*

---

87 De veiligheidsonderzoeken vinden plaats overeenkomstig de (gedateerde en weinig aangepaste) richtlijnen van 16 februari 2000 van het Ministerieel Comité voor inlichting en veiligheid (heden: de Nationale Veiligheidsraad). Het Comité bracht nogmaals de urgentie onder de aandacht om de richtlijnen van het Ministerieel Comité voor inlichting en veiligheid handelend over allerhande veiligheidsvoorschriften te actualiseren (omvang veiligheidsonderzoeken; classificatieregels; bewaring geclassificeerde stukken; infosec; taken veiligheidsofficieren). Betrokken richtlijnen dateren allen van 2001 en behoeven aanpassing.

88 Het Comité brengt in herinnering dat het reeds in 1999 en 2003 – telkenmale n.a.v. een omvangrijke wapen- en/of munitiediefstal op een militaire site – verslag uitbracht van een t.g.v. deze incidenten geopend toezichtonderzoek. Deze handelden over *'de doeltreffendheid van (ADIV) en de samenwerking van de twee inlichtingendiensten in verband met de wapendiefstal te Houthulst in 1997'* (VAST COMITÉ I, *Activiteitenverslag 1999*, pag. 83 ev.) en over *'de veiligheid en de bewaking van de militaire wapenopslagplaatsen (Thuin)'* (VAST COMITÉ I, *Activiteitenverslag 2003*, pag. 206 ev.).

plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen' (art. 11, §1, 2° W.I&V). Het begrip militaire veiligheid omvat zodoende, naast de veiligheid van inlichtingen, ook *'de veiligheid van de personen, van het materieel en van de installaties*'.[89]

Daartoe werden door de ADIV verschillende richtlijnen opgesteld en verspreid, zoals bijvoorbeeld deze over de opslag van wapens en munities (de Reglementen IF5 en IF5 bis).[90] De bevoegdheden van de ADIV bestaan erin het militair commando te adviseren inzake de aangewezen beschermingsmaatregelen, het verifiëren van de uitvoering ervan, het bij deze gelegenheden vaststellen van eventuele lacunes, het overmaken van de geconstateerde tekortkomingen aan het vermelde militair commando en het doen van de nodige aanbevelingen om eraan te verhelpen.

I.9.3. ONDERZOEKSVASTSTELLINGEN

De zaak-Conings is illustratief voor de vaststellingen die het Vast Comité I de afgelopen jaren doorheen zijn toezichtsonderzoeken deed.[91] Het lijkt alsof deze zaak een knooppunt vormt van alle eerdere constateringen, in het bijzonder wat betreft de militaire inlichtingendienst ADIV. Ook de aansluitend geformuleerde aanbevelingen bleven hun actualiteitswaarde houden. Dat gold tevens voor de aanbevelingen van de Parlementaire onderzoekscommissie 'terroristische aanslagen'.[92]

I.9.3.1. De informatiepositie van de VSSE

Jürgen Conings kwam voor het eerst onder de aandacht van de Veiligheid van de Staat in september 2015 in het kader van een Facebookgroep die fondsen inzamelde voor Dwekh Nawsha, een christelijke paramilitaire organisatie die de Assyrische gemeenschap in Irak verdedigde tegen de Islamitische Staat.[93] Hij trok een tweede maal de aandacht van de VSSE in oktober 2018.

---

89 Wetsontwerp houdende regeling van de inlichtingen- en veiligheidsdienst, *Parl. St.* Kamer 1995-1996, nr. 49-638/001, 11-12.

90 De ADIV heeft de laatste jaren meerdere malen aan het Vast Comité I te kennen gegeven dat het Reglement IF5(-bis) geactualiseerd zal worden. De meest recente versie van het Reglement overgemaakt aan het Comité is deze van het jaar 2016. Het Comité heeft geen kennis van een meer actuele globale versie.

91 Zie bijv. VAST COMITÉ I, *Activiteitenverslag 2020*, 38-53 ('De opvolging van extreemrechts door de Belgische inlichtingendiensten'); *Activiteitenrapport 2019*, 2-13 ('De uitvoering van veiligheidscreenings door de inlichtingendiensten'); *Activiteitenrapport 2016*, 70-73 ('Individuele evaluaties door het OCAD'); *Activiteitenrapport 2011*, 7-14 ('Een audit bij de militaire inlichtingendienst') en 25-33 ('De informatiestromen tussen het OCAD en de steundiensten').

92 *Parl. St.* Kamer, 2016-17, 54DOC1752/008 (15 juni 2017).

93 Volgens open bronnen zouden *foreign fighters* uit onder andere de Verenigde Staten, Frankrijk, het Verenigd Koninkrijk en Australië zich hebben aangesloten bij Dwekh Nawsha.

In beide documenten van 2015 en 2018 wordt vermeld dat betrokkene een militair is. Het Vast Comité I stelde vast dat de informatie uit 2015 door de VSSE niet werd gedeeld met de ADIV, aangezien ze op dat moment als onvoldoende relevant werd beschouwd door de VSSE. De informatie uit 2018 werd gedeeld met de ADIV tijdens een vergadering met de Werkgroep Extreemrechts, waar in algemene bewoordingen de naam van de organisatie en de voornaamste figuren werden gedeeld. Deze informatie werd in 2020 ook gedeeld met het OCAD.

Tussen juli 2020 en mei 2021 stelde de VSSE een aantal informatieverslagen op waarin de deelname van Conings aan activiteiten van de extreemrechtse groeperingen *Knights of Flanders* en Vlaams Legioen wordt gemeld. Ook stelde de VSSE vast dat Conings contacten onderhield met Tomas Boutens, de in 2014 voor feiten van terrorisme veroordeelde ex-militair en leider van de neonazigroepering Bloed, Bodem, Eer en Trouw (BBET).

Eind juni 2020 richtte de VSSE een nota aan onder andere het OCAD, het Federaal Parket en de ADIV waarin de VSSE gewag maakt van een extremistisch Facebookprofiel van Conings en de door hem geuite bedreigingen aan het adres van viroloog Marc Van Ranst. Begin augustus 2020 stelt de VSSE een aantal specifieke vragen aan de ADIV. Voor zover het Vast Comité I kon nagaan, werd door de ADIV nooit formeel geantwoord op deze vragen van de VSSE.

I.9.3.2. De informatiepositie van de ADIV

Vanaf juli 2020, kort nadat Conings via politionele informatie in verband werd gebracht met mogelijke bedreigingen aan het adres van Marc Van Ranst, wordt intern de ADIV gemeld dat betrokkene extra aandacht dient te krijgen. Deze informatie werd op dat moment niet door de ADIV meegedeeld aan het OCAD, hoewel er met betrekking tot Conings reeds een vooronderzoek liep in het kader van zijn mogelijke opname als PGE in de GGB TF.

In februari 2021 keurt de ADIV een inlichtingenoperatie goed, t.t.z. de inzet van bijzondere inlichtingenmethoden, met Conings als één van de doelen. Het onderzoek van het Comité kon evenwel aantonen dat tot 17 mei 2021 geen enkele bijzondere inlichtingenmethoden effectief werd ingezet. De ADIV verklaarde dit als zijnde een gevolg van de te grote werklast en de afwezigheid van voldoende medewerkers belast met het beheer van de BIM's.[94]

Er werd geen beroep gedaan op de tussenkomst van de VSSE in deze, omdat het een militair betrof.

[94] Bij afwezigheid of verhindering van medewerkers, wordt niet automatisch in hun vervanging voorzien. Op die wijze kon het gebeuren dat de operatie met o.m. Conings tot voorwerp, een vertraging opliep gezien de afwezigheid door ziekte van de *case manager* die de operatie moest leiden alsook de afwezigheid van de vertegenwoordiger van de ADIV op de cruciale LTF van 24 februari 2021 waarop de vermelding gebeurde dat Conings werd ingeschreven als PGE in de GGB TF en de toekenning van dreigingsniveau 3 (*infra*).

Uit de gesprekken die door het Vast Comité I werden gevoerd met de medewerkers van de ADIV is gebleken dat deze medewerkers niet of nauwelijks vertrouwd zijn met het gebruik en de finaliteit van de GGB TF.[95] Voor hen verandert de opname van een entiteit niets aan de opvolging van deze entiteit op het vlak van inlichtingenwerk.

Niettegenstaande een vijftigtal medewerkers van de ADIV een rechtstreekse toegang hebben tot de GGB TF, werden er voor de periode tussen november 2020 en april 2021, amper een dertigtal loggings door slechts enkele medewerkers vastgesteld.[96] Wat specifiek Jürgen Conings betreft, werd zijn inlichtingenfiche geraadpleegd op 15 januari en 19 februari 2021 (op 17 februari krijgt hij PGE niveau 3). De inlichtingenoperatie die de ADIV wilde opstarten met betrekking tot betrokkene in dezelfde periode, had geen verband met het gegeven dat betrokkene door het OCAD werd geëvalueerd als PGE en er voor hem een dreigingsniveau 3 werd vastgesteld.

Er kon worden geconcludeerd dat er binnen de ADIV geen rekening wordt gehouden met het bestaan van het Plan R en de GGB TF. Er bleek dat noch het feit dat betrokkene het voorwerp uitmaakte van een vooronderzoek PGE, noch dat hij als PGE werd opgenomen in de GGB TF, noch dat het OCAD aan hem een dreigingsniveau 3 toekende, een impact had op de opvolging van betrokkene door de militaire inlichtingendienst.

De ADIV voldeed niet aan zijn verplichtingen aangaande de werking van de *Lokale Task Forces* (LTF).[97] Na de opname in vooronderzoek van betrokkene in de GGB werd geen bijkomende informatie aangeleverd door de ADIV (gegeven het militaire statuut van betrokkene), en werd door de dienst geen aanzet gegeven tot een debat over eventueel te nemen maatregelen. Op de bijeenkomst van de betrokken LTF van 24 februari 2021 waarop de opname van Conings in de GGB FTF en het dreigingsniveau 3 werd meegedeeld, was bovendien geen vertegenwoordiger van de ADIV aanwezig.

---

95 Zij bleken niet op de hoogte van wat de betekenis en de gevolgen zijn van een opname van een entiteit in één van de categorieën van de GGB TF en van een bepaald dreigingsniveau dat aan een dergelijke entiteit is toegekend.

96 Uit de gesprekken bleek dat niemand van de analyse- of collectedienst noch de hiërarchie op de hoogte was dat Jürgen Conings was opgenomen in de GGB TF, en dus ook niet van het feit dat betrokkene sinds eind februari 2021 als PGE niveau 3 stond geficheerd.

97 Bijkomend probleem is dat de bijeenkomsten van de betrokken LTF in de beginperiode van de COVID 19-pandemie voor enige tijd werden opgeschort (maart en april 2020) en daarna plaatsvonden in een 'hybride' vorm, waarbij sommige diensten fysiek deelnamen aan de vergaderingen, terwijl andere diensten enkel deelnamen via videoconferentie. Omwille van de onbeveiligde communicatie via videoconferentie, kon geen geclassificeerde informatie tussen de deelnemers worden uitgewisseld.

I.9.3.3. Gebrekkige communicatie

Naast sommige dysfuncties in de communicatie met de VSSE[98] en het OCAD[99], zette de zaak-Jürgen Conings de blijvende communicatieproblemen in de schoot van de ADIV zelf in het voetlicht. Reeds in eerdere toezichtonderzoeken alsook door de parlementaire onderzoekscommissie terroristische aanslagen, werd vastgesteld dat de dienst het hoofd moet bieden aan grote uitdagingen inzake interne communicatie, informatiedoorstroming en -beheer en werden hierover aanbevelingen geformuleerd.

De in januari 2020 uitgetekende nieuwe structuur om tegemoet te komen aan de aanbevelingen, kon deze problemen uit het verleden (vooralsnog) niet verhelpen. Uit het onderzoek bleek dat vooral medewerkers van de ADIV op de 'hiërarchisch lagere echelons' de huidige structuur van de dienst als complex en onduidelijk percipiëren. Er bleek onduidelijkheid over de bevoegdheden en de communicatielijnen.

Daarnaast kon het Comité vaststellen dat er zich binnen het analyseplatform PF6, belast met de opvolging van extreemrechts, een aantal problemen hebben voorgedaan tussen juli 2020, het moment waarop Jürgen Conings onder de aandacht kwam omwille van bedreigingen tegen viroloog Marc Van Ranst, en februari 2021, het moment waarop betrokkene wordt opgenomen in de GGB TF.

Ook over de precieze werking van de *Defence Intelligence & Security Command and Control* (DISCC) bestaat er veel onduidelijkheid. De DISCC bestaat onder meer uit een Steering Committee, verantwoordelijk voor de operationele aansturing van het inlichtingenwerk en dat onder bevel staat van het hoofd van de ADIV. Een belangrijk onderdeel van de DISCC is het *Collection Coordination Intelligence Requirements Management* (CCIRM), dat een cruciale rol heeft in de coördinatie en behandeling van alle inkomende (*Requests for Information* (RFI), HUMINT-rapporten) en uitgaande (*Requests for Collect* (RFC), nota's aan autoriteiten) informatie.

Meerdere medewerkers spraken hun twijfel uit over de kennis van de werking van de dienst en de ervaring met inlichtingenwerk van de medewerkers die deel uitmaken van de DISCC (maar meer in het bijzonder van het CCIRM). Door deze gebrekkige kennis en ervaring zou informatie vaak te traag en verkeerd worden georiënteerd. De twijfels die bij bepaalde medewerkers bestaan over de goede wer-

---

98 In 2018 communiceerde de VSSE de informatie aangaande Jürgen Conings op een vergadering van de Werkgroep extreemrechts (Plan R). De ADIV antwoordde niet formeel op een nota van 8 januari 2021, waarin de VSSE haar bezorgdheid uitte ten aanzien van Jürgen Conings. De ADIV zou de vraag opgeworpen hebben tijdens een bilaterale vergadering die plaatsvond op 15 januari 2021.

99 Zie hierover het gemeenschappelijk toezichtonderzoek van de Vaste Comités I en P (I.10.). De medewerkers van de ADIV onderlijnden dat het niveau 3 van de dreiging niet aan de ADIV werd overgemaakt in een afzonderlijke evaluatie. Het OCAD liet dan weer opmerken dat de dreigingsevaluaties van personen opgenomen in de GGB TF enkel kunnen geconsulteerd worden via dat kanaal.

king van de DISCC, zorgt ervoor dat informatie buiten de DISCC om circuleert, waardoor parallelle informatiestromen ontstaan.

In voorliggend dossier verklaarden de medewerkers van het analyseplatform PF6 dat zij de belangrijke nota van de VSSE van begin januari 2021, waarin deze dienst zijn bezorgdheid uitspreekt over Jürgen Conings en een aantal vragen stelt aan de ADIV, nooit ontving, en dus ook niet werd beantwoord. Deze bewuste nota werd volgens PF6 door de DISCC niet ingevoerd in het *Request for Information Management*-systeem, dat normalerwijze gebruikt wordt voor inkomende vragen van externe diensten.

In de schoot van de DISCC zijn de leden van het Steering Committee, die verondersteld worden operationele beslissingen te nemen, onvoldoende op de hoogte van de inhoud van de dossiers. Er werd ook vastgesteld dat de beslissingen van het Steering Committee zelden officieel worden neergeschreven, waardoor verwarring ontstaat.

Een derde essentieel onderdeel van de DISCC zijn de zogenaamde *Case Managers* (CaMa) en *Collection Managers* (CoMa) belast met de vertaling van de informatiebehoeften van de analyseplatforms naar de inzet van collectemiddelen, wanneer er gebruik dient te worden gemaakt van bijzondere inlichtingenmethoden (BIM). Door het feit dat de CaMa en CoMa organisatorisch deel uitmaken van de DISCC, vallen zij buiten de structuren (Directies) waar de analyseplatformen en collectediensten zijn ondergebracht. Deze Directies kennen dan weer hun eigen structuur en hiërarchie, wat leidt tot discussies over bevoegdheden en prioriteiten. Zo is bijvoorbeeld het hoofd van de sectie C6/Investigations (dewelke deel uitmaakt van de Directie Collecte) in de huidige structuur niet bevoegd om te beslissen waarvoor zijn medewerkers inhoudelijk worden ingezet.

Het onderzoek toonde eveneens aan dat de provinciale detachementen[100], belast met de deelname aan de maandelijkse vergaderingen van de *Local Task Force* (LTF) en het onderhouden van contacten met de korpscommandanten (CO's) en de veiligheidsofficieren van de eenheden, te weinig worden gevaloriseerd. Het Comité stelde vast dat deze 'nabijheid' te weinig wordt benut door de centrale diensten uit Evere. Meer bepaald worden de provinciale detachementen te weinig aangestuurd. [101]

Verder is ook is gebleken dat er weinig overleg is tussen de provinciale detachementen en het hoofdkwartier, waardoor de medewerkers in de provinciale detachementen zich enigszins aan hun lot overgelaten voelen, en zelf hun prioriteiten stellen. Zo kon het gebeuren dat Jürgen Conings op 18 februari 2021 als

---

100 De provinciale detachementen zijn als het ware een antenne van de ADIV in elke provincie en staan dus veel dichter bij de militaire eenheden dan de centrale diensten in Evere. In deze positie zijn ze dan ook in staat om bepaalde ontwikkelingen snel te detecteren of om van dichtbij bepaalde zaken/gebeurtenissen op te volgen. Maar ook zijn zij vaak de best geplaatsten om op de vragen van de centrale diensten te antwoorden omdat ze ter plaatse de contacten hebben en de omgeving kennen.

101 Ook hierop werd in het verleden door het Vast Comité I reeds herhaaldelijk op gewezen.

potentieel gewelddadig extremist (PGE) werd opgenomen in de GGB TF met dreigingsniveau 3, en dat hierover geen overleg plaatsvond tussen het bevoegde analyseplatform en de medewerker van het provinciaal detachement Limburg, die namens de ADIV aan de betrokken LTF deelnam.

Het is het detachement Limburg dat in november 2019 voor het eerst melding maakt van Jürgen Conings, meer bepaald zijn betrokkenheid bij de extreemrechtse groepering *Belgian Commandery of Knights Templar*. Vervolgens is er, tot einde juni 2020, het moment waarop andermaal het provinciaal detachement de centrale diensten inlicht dat zij door de Federale Politie en het Parket werd gecontacteerd omdat betrokkene zich via Facebook informeert naar het adres van Marc Van Ranst, geen andere communicatie geweest tussen de centrale diensten in Evere en het provinciaal detachement. Het detachement werd niet gevraagd om bijkomende informatie te verzamelen.

I.9.3.4. De 'watchlist extreemrechts'

De minister van Defensie verzocht het Comité de betrouwbaarheid van de door de ADIV opgestelde *'watchlist'* te beoordelen. In de loop van zijn onderzoek heeft het Vast Comité I vastgesteld dat de *'watchlist'* in feite een intern proces binnen de ADIV was. Om tegemoet te komen aan voorgaande aanbevelingen van het Comité[102] werd een in april 2021 een nieuwe *'watchlist'* opgesteld, te weten een verzameling van individuele fiches met betrekking tot personen die door de ADIV werden opgevolgd in het kader van de extreemrechtse dreiging.

Doel van dit proces is om op basis van een periodieke herbeoordeling het niveau van individuele dreigingen uitgaande van extreemrechts te bepalen, alsook de *follow-up* die daaraan moet worden gegeven (extra informatieverzameling, uitwisseling van informatie met andere diensten, vaststelling van curatieve maatregelen, schrapping van de betrokkene van de *'watchlist'* wanneer blijkt dat hij of zij niet langer een bedreiging vormt…).

De *'watchlist'* is aldus geen volledig afgewerkte verzameling van gegevens over de personen die binnen de reikwijdte van de dreiging in verband met rechts-extremisme vallen en die behoren tot de bevoegdheid van de ADIV. De lijst moet gecombineerd worden met andere informatie. Als een intern proces is het niet de bedoeling dat deze als zodanig wordt meegedeeld aan derden. Aangezien het begrip 'betrouwbaarheid' waaraan de minister van Defensie vroeg de *'watchlist'* te toetsen als zodanig niet verankerd zit in de regeling van de werkzaamheden van de ADIV, heeft het Vast Comité I besloten de in de *'watchlist'* opgenomen (persoons) gegevens te toetsen aan de wettelijke kwaliteitsnorm van de verwerkte (persoons) gegevens, zoals bepaald in het art. 75, derde en vierde lid, en art. 83, eerste lid, van de Wet op de gegevensbescherming. Het is inderdaad zo dat, des te meer de

102 Zie VAST COMITÉ I, *Activiteitenverslag 2020*, 169-171 ('Diverse aanbevelingen naar aanleiding van het toezichtonderzoek naar de opvolging van extreemrechts').

verwerkte gegevens adequaat, ter zake dienend, niet buitensporig, volledig en bijgewerkt zijn overeenkomstig het doel van de *'watchlist'*, hoe meer deze *'watchlist'* als 'betrouwbaar' kan worden beschouwd.

In dit normatieve kader was het Vast Comité I - gelet op het doel van de *'watchlist'*, namelijk een intern werkproces in ontwikkeling voor het signaleren en monitoren van de dreiging van extreemrechts dat onder de bevoegdheid van de ADIV valt - van oordeel dat de overeenstemming van de *'watchlist'* met artt 75. lid 3 en 4, en 83, lid 1, van de Wet op de gegevensbescherming geen aanleiding gaf tot bijzondere opmerkingen. Het Vast Comité I achtte het desalniettemin noodzakelijk een reeks aanbevelingen aan de ADIV te formuleren, met het oog op de voortzetting, voltooiing en documentering van het werkproces inzake de *'watchlist'*.

I.9.3.5. De opeenvolgende veiligheidsmachtigingen van Jürgen Conings

Jürgen Conings was sinds 21 augustus 2006 in het bezit van een veiligheidsmachtiging niveau GEHEIM.[103] Zijn machtiging werd herhaaldelijk vernieuwd, en dit ondanks diverse politieberichten over betrokkene (aangaande bedreigingen en opzettelijke slagen en verwondingen).

In de loop van de procedure tot aanvraag van vernieuwing door zijn veiligheidsofficier in 2019, maakt de VSSE melding van een 'hit' naar aanleiding van twee feiten van gerechtelijke aard, waarvan er één betrekking had op het bezit van een illegaal wapen. Na contact met de ADIV vond een mondeling gesprek plaats dat aanleiding gaf tot het opstellen van een interne e-mail, waarin werd vermeld dat Jürgen Conings bekend was als lid van een Facebook-groep die de Assyrische belangen in Irak verdedigt. De feiten van 2015 worden vermeld, maar niet de feiten van 2018... Op basis van deze informatie lanceert de ADIV een eerste SOCMINT-analyse. Deze bracht mogelijke banden met extreemrechtse bewegingen aan het licht. Naar aanleiding van een gesprek met betrokkene, concluderen de onderzoekers dat de ontdekte feiten in verband met extreemrechts niet van dien aard zijn dat zij zijn veiligheidsmachtiging aantasten, maar bevelen een waarschuwing aan.

Op 24 juni 2020 krijgt Conings een verlenging van zijn machtiging. Twee dagen later werden bedreigingen geuit aan het adres van Marc Van Ranst; een analist van de ADIV identificeerde Jürgen Conings op de bewakingsvideo's en een administratief verslag (RAR) van de politie vervolledigde het beeld. Een tweede SOCMINT-analyse werd uitgevoerd en bracht nieuwe en meer verontrustende banden

[103] Art. 4 W.C&VM onderscheidt drie classificatieniveaus, te weten VERTROUWELIJK, GEHEIM en ZEER GEHEIM.

met extreemrechts aan het licht. Op basis van deze elementen, heeft de ADIV geweigerd de veiligheidsmachtiging op 31 augustus 2020 te verlengen.[104]

I.9.3.6. De opdracht van de veiligheidsofficier

Op 2 juni 2020 werd Jürgen Conings overgeplaatst naar zijn nieuwe eenheid (PDT-IA) in een functie waarvoor niet langer een veiligheidsmachtiging vereist was. De veiligheidsofficier die verantwoordelijk was voor zijn nieuwe eenheid heeft het verzoek om verlenging niet beëindigd. In bepaalde gevallen en in het kader van de inzet is een dergelijke toestemming inderdaad noodzakelijk.

Begin september 2020 werd hij door de ADIV op de hoogte gebracht van de niet-verlenging. Gezien de COVID-omstandigheden werd betrokkene telefonisch van deze weigering in kennis gesteld. De mondelinge kennisgeving werd schriftelijk bevestigd op 12 november 2020, d.w.z. twee en een halve maand na de weigering.

Het IF5-reglement bij ADIV beschrijft de verantwoordelijkheden van de veiligheidsofficier, onder meer belast met het opstellen van permanente beveiligingsorders en met het toezicht op de uitvoering ervan. Er wordt echter geen melding gemaakt van samenwerking of interactie met het ADIV-personeel.

Het geval van de veiligheidsofficier van Jürgen Conings is bijzonder. Als verantwoordelijke voor een groot aantal kleine onafhankelijke entiteiten, is hij gedelokaliseerd van de eenheden. Deze delokalisatie laat hem zeker geen effectieve controle over de veiligheidsrichtlijnen toe.

Het Vast Comité I stelde vast dat de ADIV niet met de veiligheidsofficier had gecommuniceerd in verband met de weigering van een machtiging aan Jürgen Conings. Het Comité heeft ook vastgesteld dat de veiligheidsofficier niet in staat was controle uit te oefenen op alle gebouwen die onder zijn verantwoordelijkheid vielen.

I.9.3.7. Het wapendepot en de rol van de ADIV

Op 18 mei 2021 merkte een collega van Jürgen Conings op dat wapens en munitie ontbraken uit het wapen- en munitiedepot van de PDT-IA cel. Hij meldde het incident onmiddellijk aan zijn hiërarchie en stelde een intern onderzoek in op het niveau van de Directie Veiligheid (Dir S) van de ADIV. De interne richtlijnen van de ADIV (meer in het bijzonder het Reglement IF5*bis*), sluiten immers uit dat eenzelfde persoon zowel wapen- als munitiebeheerder is. Het IF5-reglement kent ook een speciale status toe aan deze depots. Zo bijvoorbeeld moeten de beheerders van munitiedepots en wapendepots over een veiligheidsmachtiging beschikken.

[104] Gelet op de termijnen was Jürgen Conings vanaf 17 juli 2020 niet langer gerechtigd dit te doen. Ter herinnering: deze afwezigheid of weigering had geen gevolgen voor zijn nieuwe functie bij Defensie.

Het onderzoek bracht aan het licht dat de regels niet werden gerespecteerd binnen de PDT-IA-cel.

De veelvuldige aanpassingen van de regels, gekoppeld aan de COVID-situatie, stelde Jürgen Conings in staat te beschikken over het arsenaal waarmee hij op de vlucht was geslagen.

I.9.4. CONCLUSIES

De zaak-Conings is exemplarisch voor de vaststellingen van de mankementen die het Vast Comité I de afgelopen tien jaar deed bij de inlichtingen- en veiligheidsdiensten in het algemeen en bij de militaire inlichtingendienst in het bijzonder.

Er kan niet worden ontkend dat met de zaak-Conings de militaire inlichtingendienst in het oog van de storm kwam te staan. Het is onmiskenbaar dat er op alle niveaus binnen de ADIV, maar ook in de gehele hiërarchische lijn bij Defensie, (ernstige) fouten werden gemaakt: een structureel personeelsgebrek in de verschillende diensten en op alle niveaus, het grote personeelsverloop, het verlies van kennis en ervaring, een beperkte supervisie in de eenheid van Conings, een manifest gebrek aan informatiedoorstroming (*bottom up* en *top down*), een nieuwe en complexe werkingsstructuur bij de ADIV, te weinig aansturing, personeelsproblemen, geen eenduidig beleid met betrekking tot extremisme, gebrekkige informatie-uitwisseling binnen Defensie en tussen de diverse veiligheidsactoren…. Maar mogelijks kunnen ook bij andere actoren (politie, parketten, onderzoeksrechters…) eveneens fouten worden vastgesteld. Die studie hiervan viel evenwel buiten het bevoegdheidsdomein van het Vast Comité I.

Er kon worden vastgesteld dat de feiten *in casu* wel tijdig door de inlichtingen- en veiligheidsdiensten werden gedetecteerd, maar onvoldoende actief opgevolgd. Dat er een ruime marge voor verbetering is, is duidelijk.

Voor het Vast Comité I staat het buiten kijf dat de ADIV noodzakelijk is in de algemene veiligheidsarchitectuur, zowel in België als in het buitenland. Niettemin moet de werking ervan grondig worden gewijzigd, evenals de structuur. Idealiter zouden de taken van de ADIV moeten worden teruggebracht en zou het verwachte *change management* moeten worden verwezenlijkt in het kader van een professionalisering ten dienste van de veiligheid van de burger.

I.10. DE ROL VAN HET OCAD IN DE OPVOLGING VAN DE MILITAIR JÜRGEN CONINGS

Ter vervollediging van het toezichtonderzoek naar het opsporen en opvolgen van Jürgen Conings door de twee inlichtingendiensten[105], onderzocht het Vast Comité I, samen met het Vast Comité P, "*de rol van het OCAD in de opvolging van Jürgen Conings, met name voor wat betreft het ingestelde vooronderzoek, de dreigingsevaluatie niveau 3 en de gevolgen daarvan, en de informatie-uitwisseling over betrokkene.*" De Vaste Comités P en I bestudeerden de informatiepositie van het coördinatieorgaan, het proces van de dreigingsevaluatie van betrokkene en de informatie-uitwisseling tussen de verschillende partners.[106]

I.10.1. ANALYSE VAN HET WETTELIJK KADER

De Wet betreffende de analyse van de dreiging van 10 juli 2006 (W.OCAD) kent aan het OCAD de opdracht toe om op punctuele basis een gemeenschappelijke evaluatie uit te voeren die moet toelaten te oordelen of dreigingen inzake terrorisme en extremisme zich voordoen en welke maatregelen in voorkomend geval noodzakelijk zijn.

Om de dreiging te evalueren, baseert het OCAD zich op de inlichtingen afkomstig van de ondersteunende diensten (bijvoorbeeld de Veiligheid van de Staat (VSSE), de Algemene Dienst Inlichting en Veiligheid (ADIV) of nog, de Federale Politie). Volgens de W.OCAD zijn de ondersteunende diensten (op straffe van een penale sanctie) verplicht, behoudens het bestaan van een embargoprocedure, ambtshalve of op vraag van de directeur van het OCAD, alle inlichtingen waarover zij in het kader van hun wettelijke opdrachten beschikken en die relevant zijn voor het vervullen van de opdrachten het OCAD, mee te delen binnen de termijnen zoals voorzien in het koninklijk besluit van 28 november 2006 tot uitvoering van de Wet betreffende de analyse van de dreiging. De informatieflux tussen het OCAD en zijn ondersteunende diensten verschilt naargelang het al dan niet geclassificeerde documenten betreft. Het OCAD en de ondersteunende diensten kunnen de geclassificeerde documenten uitwisselen via een geëncrypteerd informaticasysteem (BINII). De geclassificeerde informatie wordt daarna door het OCAD geregistreerd in hun databank PROTEUS. Een functionele mailbox van het OCAD wordt gebruikt voor alle niet-geclassificeerde informatie-uitwisseling.

In artikel 11§6 van het uitvoeringsbesluit op de W.OCAD wordt bepaald dat iedere evaluatie het niveau van de dreiging zal bepalen door zich te steunen op een beschrijving van de ernst en de waarschijnlijkheid van het gevaar of van de drei-

105 Zie 'I.9. Het opsporen en opvolgen van de radicalisering van een militair: de zaak-Jürgen Conings'.

106 De referteperiode liep tot 17 mei 2021, de dag van de verdwijning van Jürgen Conings.

ging.[107] Volgens artikel 10 van de W.OCAD worden de punctuele dreigingsevaluaties gericht tegen personen, groeperingen of gebeurtenissen, die op initiatief van het OCAD worden uitgevoerd, meegedeeld aan de leden van de Nationale Veiligheidsraad, de ondersteunende diensten, de Algemene Directie Crisiscentrum, het Federaal Parket en het lid van het College van procureurs-generaal dat specifiek belast is met terrorisme en extremisme, de Nationale Veiligheidsoverheid evenals aan ieder lid van de regering waarvan de directeur van het OCAD het noodzakelijk oordeelt het te informeren.

De dreigingsevaluatie aangaande een persoon wordt dan weer geregeld overeenkomstig het koninklijk besluit betreffende de gemeenschappelijke gegevensbank Terrorist Fighters van 21 juli 2016 (KB GGB) en de Omzendbrief van 22 mei 2018 van de minister van Veiligheid en Binnenlandse Zaken en de minister van Justitie betreffende de informatie-uitwisseling rond en de opvolging van *terrorist fighters* en haatpropagandisten (beperkte verspreiding) (MO GGB). De Vaste Comités I en P legden zich in dit onderzoek eerder toe op de oprichting en voeding van de gemeenschappelijke gegevensbank *Terrorist Fighters* (GGB TF).

I.10.2. HET OCAD EN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN

Na de aanslagen in 2016, werd met Wet van 27 april 2016 inzake aanvullende maatregelen ter bestrijding van terrorisme een wijziging aangebracht in de Wet van 5 augustus 1992 op het Politieambt (WPA) om een wettelijk basis te voorzien voor de oprichting van een gemeenschappelijke gegevensbank met het oog op de preventie en de strijd tegen het terrorisme en het extremisme dat tot terrorisme kan leiden.

Met het KB GGB werd de gemeenschappelijke gegevensbank *foreign terrorist fighters* in het leven geroepen. Met een wijzigingsbesluit van 23 april 2018 werd deze databank omgedoopt tot de gemeenschappelijke gegevensbank *terrorist fighters* (GGB TF) omwille van de toevoeging van een nieuwe categorie *homegrown terrorist fighters* naast de reeds bestaande categorie van *foreign terrorist fighters*. Daarnaast werd met een nieuw koninklijk besluit van dezelfde datum een

---

[107] De verschillende dreigingsniveaus zijn:
- het " Niveau 1 of LAAG " indien blijkt dat de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse niet bedreigd is;
- het " Niveau 2 of GEMIDDELD " indien blijkt dat de dreiging tegen de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse weinig waarschijnlijk is;
- het " Niveau 3 of ERNSTIG " indien blijkt dat de dreiging tegen de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse mogelijk en waarschijnlijk is;
- het " Niveau 4 of ZEER ERNSTIG " indien blijkt dat de dreiging tegen de persoon, de groepering of de gebeurtenis die het voorwerp uitmaakt van de analyse ernstig en zeer nabij is.

onderscheiden gemeenschappelijke gegevensbank voor haatpropagandisten (GGB HP) opgericht.[108]

Ten slotte werden, met het koninklijk esluit van 20 december 2019 twee nieuwe categorieën toegevoegd aan de gemeenschappelijke gegevensbank *terrorist fighters*, m.n. de potentieel gewelddadige extremisten en de terrorismeveroordeelden.[109] In toepassing van het KB FTF en de wijzigingsbesluiten van 2018 en 2019, beoogt de gemeenschappelijke gegevensbank *terrorist fighters* de opvolging van de *foreign terrorist fighters* (FTF), de *homegrown terrorist fighters* (HTF), de potentieel gewelddadige extremisten (PGE) en de terrorismeveroordeelden (TV).

In de lijn van het achterliggende idee om aan informatie-uitwisseling te doen, voorziet de wet in een verplichting tot het voeden van de GGB voor de diensten die een directe toegang hebben tot de gegevensbanken. De gegevens over een in de GGB-geregistreerde entiteit moeten immers voortdurend worden bijgewerkt. Vandaar dat de GGB een dynamische databank wordt genoemd. Enkel de basisdiensten (OCAD, VSSE, ADIV en de geïntegreerde politie) kunnen een nieuwe entiteit en, na validatie van het OCAD, iemand in vooronderzoek plaatsen en dit voor een periode van maximaal zes maanden. Voor elke geregistreerde entiteit waken de diensten die rechtstreeks toegang hebben tot de GGB erover de persoonsgegevens en informatie toe te voegen waarover ze beschikken. De dienst die een persoonsgegeven of een informatie geregistreerd heeft, is de enige die dit persoonsgegeven of deze informatie kan wijzigen, verbeteren of uitwissen.

Als verantwoordelijke voor het operationeel beheer van de GGB, is het OCAD belast de beoordeling van de gegevens van de inlichtingenfiche (*infra*) en het valideren van een entiteit in de GGB op basis van de beschikbare informatie.

---

108 Koninklijk besluit van 23 april 2018 tot wijziging van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Foreign Terrorist Fighters en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt en tot omvorming van de gemeenschappelijke gegevensbank Foreign Terrorist Fighters naar de gemeenschappelijke gegevensbank Terrorist Fighters en het koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten en tot uitvoering van sommige bepalingen van de afdeling 1bis "Het informatiebeheer" van hoofdstuk IV van de wet op het politieambt, *BS* 30 mei 2018.

109 Koninklijk besluit van 20 december 2019 tot wijziging van het koninklijk besluit van 21 juli 2016 betreffende de gemeenschappelijke gegevensbank Terrorist Fighters, *BS* 27 januari 2020.

I.10.2.1. De inschrijvingsprocedure

De inschrijvingsprocedure voor de categorie potentieel gewelddadige extremisten (PGE)[110], toegevoegd door het KB van 20 december 2019, en waarin Jürgen Conings was opgenomen, werd uitgewerkt in de omzendbrief van de minister van Veiligheid en Binnenlandse Zaken en de minister van Justitie aangaande de uitwisseling van informatie en de opvolging van TF en HP (MO GGB).[111] Terwijl de omzendbrief de informatie-uitwisseling beschrijft aangaande de categorieën FTF, HTF en HP, wordt deze naar analogie toegepast op de potentieel gewelddadige extremisten.

De fase van 'vooronderzoek' (de zgn. 'verrijkingsfase') heeft tot doel de inzameling van gegevens en informatie, *à charge et à décharge*, die nodig zijn om een entiteit als PGE al dan niet te valideren. De MO GGB moedigt de diensten aan om, in de schoot van de LTF's en in het kader van hun respectievelijke wettelijke opdrachten, samen de strategie van informatiegaring te bepalen met het oog op het verrijken van de inlichtingen ('wie doet wat'). Na afloop van deze periode, dewelke maximaal zes maanden kan duren) zal het OCAD, op basis van de beschikbare informatie/inlichtingen, evalueren of de wettelijke criteria al dan niet vervuld zijn. Indien deze niet vervuld zijn, worden de gegevens van de persoon in vooronderzoek automatisch geschrapt.

Conform aan wat werd bepaald in de MO GGB, bestaat de GGB uit inlichtingenfiches dewelke niet-geclassificeerde persoonsgegevens en informatie bevatten afkomstig van alle diensten die de GGB voeden. Deze fiches moeten het mogelijk maken niet alleen de mogelijk potentiële dreiging te beoordelen die deze entiteiten vertonen, maar voornamelijk er een opvolging van te verzekeren met het oog op

---

110 De categorie potentieel gewelddadige extremisten, behelst de natuurlijke personen die een aanknopingspunt met België hebben en die voldoen aan volgende cumulatieve criteria:
a) ze hebben extremistische opvattingen die het gebruik van geweld of dwang als actiemethode in België legitimeren;
b) er zijn betrouwbare aanwijzingen dat ze de intentie hebben om geweld te gebruiken, en dit in verband met de opvattingen vermeld in a);
c) ze voldoen aan minstens een van de volgende criteria die het risico op geweldpleging verhogen: 1) ze hebben systematisch sociale contacten binnen extremistische milieus; 2) ze hebben een psychische problematiek, vastgesteld door een daartoe gekwalificeerde deskundige; 3) ze pleegden daden of stelden antecedenten die beschouwd kunnen worden als ofwel a) een misdaad of wanbedrijf die de fysieke of psychische integriteit van derden aantast of bedreigt; ofwel b) onderrichtingen of een opleiding voor de vervaardiging of het gebruik van explosieven, vuurwapens of andere wapens of schadelijke of gevaarlijke stoffen, dan wel voor andere specifieke methoden en technieken nuttig voor het plegen van terroristische misdrijven bedoeld in artikel 137 van het Strafwetboek, ofwel c) bewuste handelingen die als materiële steun voor een terroristische/extremistische organisatie of netwerk gelden; ofwel d) feiten die door hun aard wijzen op een verontrustend veiligheidsbewustzijn in hoofde van betrokkene.

111 De algemene doelstelling van de omzendbrief is *"vanuit een veiligheidsobjectief de informatiehuishouding, het nemen van maatregelen en de gecoördineerde samenwerking tussen de diensten regelen en dit met het oog om de openbare veiligheid tegen de potentiële dreiging maximaal te beschermen door het verstoren van bedreigende activiteiten uitgaande van de Terrorist Fighters (FTF/HTF) en Haatpropagandisten (HP)."*

het anticiperen en het verhinderen van mogelijke terroristische acties. Eenmaal het statuut in de gegevensbank werd gevalideerd, maakt het OCAD een individuele dreigingsevaluatie op, daarbij rekening houdend met alle pertinente informatie waarover het beschikt. Deze evaluatie, die wordt opgenomen in de individuele inlichtingenfiche, zal richtinggevend zijn voor de door te partners te nemen maatregelen.

Om de criteria voor het toekennen van een statuut en de dreigingsanalyse te evalueren, doet het OCAD beroep op zijn eigen risico-evaluatietool RooT37. Op basis van een vaste set, door wetenschappelijk onderzoek onderbouwde, risico-indicatoren wordt een richtinggevende score verkregen. Deze score wordt gecontroleerd door een evaluator van het OCAD, en vervolgens door het 'kwaliteitsteam' binnen het OCAD alvorens een entiteit te kunnen valideren in de GGB.

I.10.2.2. De informatie-uitwisseling met de partners

In het kader van het Plan R(adicalisme)[112] wordt de uitwisseling van informatie georganiseerd in de schoot van de *Lokale Task Forces* (LTF), de beleidsmatige en operationele overlegplatformen van onder meer politie- en inlichtingendiensten binnen de geografische afgebakende zone van het gerechtelijk arrondissement[113], en de lokale integrale veiligheidscellen inzake radicalisme, extremisme en terrorisme (LIVC-R), een gemeentelijk overlegplatform dat moet instaan voor de realisatie van coherente preventieve, repressieve en nazorg-acties. Deze lokale integrale veiligheidscellen zijn, zoals de LTF's, overlegplatformen waar informatie-uitwisseling tussen de sociale- en preventiediensten, de LTF en bestuurlijke autoriteiten moet plaatsvinden inzake radicalisme, extremisme en terrorisme.

Zoals voorgeschreven in de MO GGB, is er voor de LTF een belangrijke rol weggelegd inzake het bepalen van het geheel van veiligheidsmaatregelen. Deze LTF-vergaderingen spelen een cruciale rol bij het prioritiseren en het bepalen van het geheel van veiligheids- en begeleidingsmaatregelen, en dit alles in een geest van onderling overleg.

112 In september 2021 verworden tot 'Strategie Terrorisme en Extremisme' (Strategie TER).

113 Zij verzekeren de opvolging van radicaliserende individuen en groeperingen op lokaal niveau en stellen maatregelen voor om de impact van deze individuen en groepen te reduceren door o.m. informatie, inlichtingen en analyses uit te wisselen en te bespreken.

I.10.3. DE ROL VAN HET OCAD IN DE OPVOLGING VAN JURGEN CONINGS: DE OPNAME IN DE GEMEENSCHAPPELIJKE GEGEVENSBANK

In augustus 2020 opende het OCAD een vooronderzoek PGE over Jürgen Conings. Deze beslissing was gebaseerd op de analyse van sinds juni 2020 door de politie- en inlichtingendiensten doorgestuurde informatie. Het OCAD ging tevens over tot een analyse van zijn activiteiten op de sociale media. De gegevens die werden opgeslagen in de gegevensbank van OCAD, PROTEUS, betroffen voornamelijk door de betrokkene geuitte dreigingen en zijn contacten in het extreemrechtse milieu. Op basis van de beschikbare informatie, waren de Vaste Comités P en I van oordeel dat de opname van betrokkene in vooronderzoek gerechtvaardigd was.

Vanaf de opening van een vooronderzoek bestaat de verplichting voor de basisdiensten om alle relevante informatie naar de GGB te zenden om deze te verrijken. De opvolging dient vanaf dan te gebeuren binnen bevoegde LTF. De analyse van de processen-verbaal van de vergaderingen van deze LTF en van de Werkgroep Extreemrechts (Plan R) bevestigde de agendering van de opvolging van Jürgen Conings vanaf september 2020.

Naar het einde van het vooronderzoek en met behulp van zijn instrument Root37, werd door het OCAD een evaluatie gemaakt van de elementen waarover ze beschikten in het kader van de valideringscriteria zoals omschreven in het KB GGB. Zijn statuut als PGE werd bevestigd en het dreigingsniveau van Jürgen Conings werd ingeschaald op niveau 3 (ernstig). Deze beoordeling werd bevestigd door de evaluator van het OCAD alsook door het kwaliteitsteam halfweg februari 2021.

I.10.4. INFORMATIEUITWISSELING

Het OCAD bracht de verschillende partners van de bevoegde LTF tijdens een vergadering eind februari 2021 op de hoogte van de opname van Jürgen Conings in de gegevensbank alsook van de dreigingsevaluatie. Op deze vergadering was ADIV niet vertegenwoordigd. Het verslag van de vergadering maakt gewag van uitwisseling van informatie over betrokkene.

De opame van Jürgen Conings in de gegevensbank werd onder meer gemeld aan de Federale Politie (voor opname in de ANG), aan BELPIU alsook aan de betrokken LIVC-R (en dus de burgemeester). Het OCAD stuurde evenwel geen bijkomend signaal naar de basisdiensten en de partners aangaande de evaluatie niveau 3 van betrokkene, ervan uitgaande dat de opname in de gegevensbank volstond.

Na zijn opname in de gegevensbank, wordt de opvolging van Jürgen Conings geagendeerd op alle navolgende LTF-vergaderingen en in de Werkgroep Extreem-

rechts, hoewel er niet steeds nieuwe informatie beschikbaar was (*infra*). De enige bijkomende informatie die aan het OCAD werd toegestuurd vóór 17 mei 2021, liet niet toe een wijziging door te voeren aangaande het dreigingsniveau.

Een gevolg van de opname als PGE/niveau 3 in de GGB is dat alle diensten die enkel een toegang *Hit/No Hit* hebben bij consultatie er ook op gewezen worden dat een persoon gekend is. In het geval van Jürgen Conings voerde bijv. de Algemene Directie veiligheid en preventie (ADVP) van de FOD Binnenlandse Zaken een consultatie uit met positief resultaat ("Hit") in het kader van een identificatiekaart als bewakingsagent.

Conform de MO GGB, wordt bij de registratie in de GGB ook een categorie toegekend aan de persoon (A, B of C) die betrekking heeft op de wijze waarop de LTF de persoon verder zal opvolgen. Voor Jürgen Conings werd "B" toegekend, m.n. "dreiging niet extreem groot". De beide Comités wezen op de incoherentie tussen het dreigingsniveau 3 (ernstig) zoals bepaald door het OCAD enerzijds en categorie van opvolging in de LTF anderzijds. Het OCAD preciseerde dat de opvolgingsmaatregelen voor de categorieën A, B en C gelijklopend zijn, maar attendeerde, meer algemeen, op de moeilijke toepassing van de maatregelen zoals voorzien in de MO GGB.[114]

Wat de andere maatregelen betreft zoals de 'aanklampende opvolging' stelt het OCAD vast dat dit ook met de FTF niet altijd even evident is om te realiseren, gelet op het feit dat dit niet afdwingbaar is en dat de MO GGB op het vlak van maatregelen tegen zijn limieten aanloopt. Als er geen inlichtingenonderzoek of strafrechtelijk terrorismeonderzoek kan geopend worden, dan is er niet veel mogelijk. In het geval van Jürgen Conings was er een gerechtelijk onderzoek lopende voor de bedreigingen tegen Marc Van Ranst. Het OCAD stelde dat buiten wat er medegedeeld werd op de LTF, ze geen andere informatie kreeg over het lopende gerechtelijke onderzoek.

Een verder gevolg van het statuut PGE/niveau 3 is dat hij op elke LTF zou besproken worden om te zien welke informatie er naar boven komt en om eventueel te zien of er maatregelen kunnen genomen worden om de dreiging te verminderen. Volgens het OCAD is het evident dat het initiatief bij de ADIV lag, Niettemin werd aan alle diensten een informatie-inspanning gevraagd. Op de LTF-vergaderingen van maart en april 2021 stond betrokkene wel geagendeerd, maar werd hij door geen enkele dienst besproken en werd er dus ook geen informatie gedeeld.

De nota seiningen die werd uitgewerkt door DJSOC/Terro, voorziet voor elke PGE in de ANG in een seining 'discrete controle'. Volgens het OCAD heeft deze maatregel geen resultaat gegeven wat informatie-inwinning betreft, want anders was deze informatie zeker minstens besproken geweest op een LTF.

---

114 Voor het OCAD wil het toekennen van deze categorie B niet zeggen dat er een bijkomende evaluatie gebeurt. De categorie B dient immers ook van dichtbij opgevolgd te worden.

I.10.5. CONCLUSIES

Zich beperkend tot de rol van het OCAD in de opvolging van Jürgen Conings, konden de Vaste Comités I en P de uitwisseling van informatie met het OCAD door de basisdiensten in de fase van het vooronderzoek vanaf augustus 2020 bevestigen. Op basis van deze in PROTEUS geregistreerde informatie en met behulp van het Root37-inistrument, kon het statuut van Jürgen Conings als potentieel gewelddadige extremist worden bevestigd en het dreigingsniveau ingeschaald op niveau 3.

Het is het OCAD dat het initiatief nam om Jürgen Conings eerst in vooronderzoek PGE te zetten en hem vervolgens ook de status PGE/niveau 3 toe te kennen. De Vaste Comités I en P vonden de beslissing tot vooronderzoek gerechtvaardigd.

De dreigingsevaluatie van Jürgen Conings werd verspreid door het OCAD volgens de modaliteiten voorzien in de W.OCAD. Niettegenstaande hij door het OCAD werd ingeschaald op niveau 3 (ernstig), werd hij slechts opgenomen in de categorie B (dreiging niet extreem groot). Beide parameters zijn inderdaad onafhankelijk van mekaar.

I.11. DE OPVOLGING VAN EEN REGERINGSCOMMISSARIS DOOR DE VSSE

Bij koninklijk besluit van 17 mei 2021 werd Ihsane Haouach benoemd als regeringscommissaris bij het Instituut voor de gelijkheid van vrouwen en mannen (IGVM). In die hoedanigheid vertegenwoordigde ze de regering in de raad van bestuur van het IGVM. Ze lag evenwel van bij haar aanstelling onder vuur: eerst omwille van haar hoofddoek, vervolgens omwille van een uitspraak over de scheiding tussen kerk en staat. Op 9 juli 2021 diende Ihsane Haouach haar ontslag in. Dezelfde dag werd in de media gesuggereerd dat een nota van de Veiligheid van de Staat (VSSE) hiervan mogelijks aan de basis zou liggen.[115]

I.11.1. EEN NOTA VAN DE VEILIGHEID VAN DE STAAT

In de loop van 2020 werd door de Analysedienst counterextremisme (CE) van de VSSE een synthesenota opgesteld over de Moslimbroederschap in België.[116] Op het ogenblik van de controverse in de pers omtrent de benoeming van

---

115 B. DEMONTY, *Le Soir*, 9 juli 2021 ('Ihsane Haouach démissionne, le gouvernement en possession d'informations sur de potentiels liens avec les Frères musulmans'). Het rapport in kwestie van de VSSE ('Beperkte verspreiding'/ 'Vertrouwelijk') verscheen ook integraal in de pers (bijv. M. VERBERGT, *De Standaard*, 14 juli 2021 ('Dit zegt de Staatsveiligheid letterlijk over Ihsane Haouach')).

116 Hierover 'I.12. Een vernieuwde aandacht voor de Moslimbroederschap' (*infra*).

Ihsane Haouach als regeringscommissaris, herinnert men zich binnen de VSSE dat haar naam voorkwam in deze synthesenota. Betrokkene vormde geen target van de dienst. Evenwel volgt de VSSE acties ten overstaan van verschillende vormen van extremisme op die als dusdanig passen binnen zijn wettelijke opdrachten (art. 8 W.I&V, 'extremisme').

De VSSE achtte het opportuun de minister van Justitie en de Premier hierover schriftelijk te informeren. Daartoe werd een geclassificeerde nota opgesteld. Ihsane Haouach bleek *'gekend* (is) *omwille van haar nauwe contacten met de Moslimbroeders. Deze contacten tussen de Moslimbroeders en Ihsane Haouach kunnen worden gekaderd binnen een bredere strategie van de Moslimbroeders, waarbij deze proberen te wegen op het publieke debat en de beleidsvorming […]'*. Er werd tevens vermeld dat betrokkene *'voor zover ons bekend zelf geen lid is van de Moslimbroeders en zelf nooit de aandacht heeft getrokken omwille van concrete extremistische stellingnames' […] Het is dan ook niet uit te sluiten dat Ihsane Haouach er zichzelf niet (ten volle) van bewust is dat ze nauwe contacten onderhoudt met de Moslimbroeders. We stellen dan ook voor om de bevoegde Staatssecretaris of haar Beleidscel, net als eventueel mevrouw Haouach zelf, een sensibiliserende briefing aan te bieden'*. [117]

I.11.2. ONDERZOEKSVASTSTELLINGEN

I.11.2.1. Een vernieuwde aandacht voor de Moslimbroederschap (en Ihsane Haouach)?

Niettegenstaande de strijd tegen het terrorisme hoog op de prioriteitenlijst bleef staan, richtte de VSSE haar aandacht de afgelopen jaren opnieuw op andere dossiers. In het kader van de dreigingen 'extremisme' en 'inmenging' werd in 2020 beslist een synthesenota op te stellen over de Moslimbroederschap in België, één van de prioriteiten van de VSSE in haar Actieplan. De naam van Ihsane Haouach kwam in het kader van deze nota voor als een persoon die, al dan niet bewust, in contact stond met deze beweging. De betrokkene was echter geen doelwit van de VSSE.

Via (de beroering in) de pers vernam de VSSE de benoeming van Ishane Haouach als regeringscommissaris. De dienst nam zelf het initiatief om een nota op te stellen, omdat hij van mening was dat de minister van Justitie in kennis moest worden gesteld van het feit dat de betrokkene bekend was in het kader van de opvolging van de wettelijke bevoegdheden in verband met extremisme. Aangezien niet kon worden uitgesloten dat ze niet (volledig) op de hoogte was van haar nauwe banden met de Moslimbroederschap, werd voorgesteld dat de minister een sensibiliserende briefing organiseerde voor de bevoegde staatssecretaris of haar beleidscel, net als voor Ihsane Haouach zelf in een later stadium.

---

117 Citaat uit de in de pers (M. VERBERGT, *l.c.*) gepubliceerde vertrouwelijke nota van de VSSE.

I.11.2.2. Het zorgvuldigheidsbeginsel

In een inlichtingencontext is er weinig zekerheid, en daar moet rekening mee worden gehouden bij de beslissing of en hoe informatie moet worden verstrekt (in dit geval aan de minister van Justitie). Het Comité had eerder verklaard dat "*wil de openbaarmaking van informatie als rechtmatig worden beschouwd, zij voldoende moet worden gestaafd door betrouwbare informatie. Het moet ook met zorg worden geformuleerd. Er kan bijvoorbeeld geen ongenuanceerd beeld worden gegeven van de onderliggende informatie, of een bepaald item kan worden gepresenteerd als een "beeld van" of een "indruk van". In die zin moet de verstrekte informatie ook "accuraat" zijn door een objectief beeld te geven van het beeld dat de inlichtingendienst heeft van de dreiging en de rol van de betrokkene, zonder "manipulatief" te zijn [...]*".[118] Het Comité was van oordeel dat de nota in overeenstemming was met het voormelde voorzorgsprincipe en dat de VSSE in haar mededeling aan de regering voldoende had uitgelegd waarom de banden van de regeringscommissaris met de Moslimbroederschap een bedreiging zouden kunnen vormen.

Hoewel een schriftelijke nota werd voorbereid, werd besloten deze niet meteen te verzenden. De VSSE was zich ervan bewust dat de nota politiek gevoelig en onvolledig was, en dat hij niet mocht uitlekken. Er werd besloten de minister van Justitie mondeling in te lichten, maar het onderhoud vond niet plaats. In artikel 19 W.I&V is niet bepaald hoe de informatie door de VSSE moet worden verstrekt. In het verleden was het Comité van mening dat de mededeling om redenen van rechtszekerheid (behalve in uiterst dringende gevallen) schriftelijk diende te geschieden, om latere discussies te voorkomen en parlementaire (of zelfs juridische) controle mogelijk te maken. De bevoegde staatssecretaris werd niet rechtstreeks ingelicht. De VSSE ging ervan uit dat de Premier of minister van Justitie dat zou doen.

I.11.2.3. Geen verdere onderzoeksbevindingen?

De VSSE was zich bewust van de politieke gevoeligheid van de benoemingskwestie, niet het minst na de plenaire zitting begin juni 2021 in het Parlement. Er werd echter besloten te wachten met de verzending van de nota op de bevestiging van de erin vervatte elementen. De nota werd uiteindelijk meer dan een maand ingehouden, omdat de VSSE niet wou geïnstrumentaliseerd worden. Niettemin leek het erop dat er geen wijzigingen werden aangebracht in de nota die uiteindelijk in juli aan de Premier, de Vice-eersteministers en de minister van Binnenlandse Zaken werd toegezonden. Met andere woorden, er waren geen verdere onderzoeksbevindingen.

---

118 VAST COMITÉ I, Toezichtonderzoek naar de manier waarop de Belgische inlichtingendiensten communiceren met een private of publieke werkgever over een werknemer, 2020.

Op basis van de resultaten van het onderzoek kon het Comité zich niet uitspreken over een oorzakelijk verband tussen de nota en het ontslag van regeringscommissaris Ishane Haouach.

I.11.2.4. Het lekken van een geclassificeerde nota

De nota over Ihsane Haouach werd geclassificeerd als "Vertrouwelijk Wet 11.12.1998". Hij werd evenwel volledig in de pers gepubliceerd, nauwelijks een dag nadat de nota werd toegezonden aan de Premier, de Vice-eersteministers en de minister van Binnenlandse Zaken. Aangezien het strafbaar is om een geclassificeerd document aan een derde te overhandigen, diende de VSSE, terecht aldus het Comité, een klacht tegen onbekenden bij het Brusselse parket.

Het Vast Comité I herinnerde eraan dat het de verantwoordelijkheid is van de veiligheidsofficieren in de verschillende ministeriële kabinetten om toe te zien op het correcte gebruik van geclassificeerde documenten. Ook ontvangers van geclassificeerde nota's dienen uiterst voorzichtig te zijn met deze informatie. In de eerste plaats moeten zij zich ervan bewust zijn dat de overdracht aan een onbevoegde derde een strafbaar feit is. Ten tweede kan het schade toebrengen aan de personen op wie de nota betrekking heeft. Ten derde is het schadelijk voor de inlichtingen- en veiligheidsdiensten zelf en ondermijnt het terechte vertrouwen van het publiek in deze diensten.

I.11.2.5. Een 'verstoringsactie'?

In de nota aan de minister van Justitie wordt voorgesteld een 'bewustmakingsbriefing' te organiseren voor Ihsane Haouach. Het onderliggende doel was tweeledig. Het was niet uitgesloten dat betrokkene zelf niet (volledig) op de hoogte was van haar nauwe banden met de Moslimbroederschap, in welk geval bewustmaking noodzakelijk/nuttig was. Indien zij echter op de hoogte was, kon het doel van een dergelijke briefing zijn een ontwrichtend (in dit geval 'afschrikkend') effect te bewerkstelligen. In dit verband verklaarde de VSSE dat zij voornemens was in de toekomst een disruptieve aanpak te realiseren door procedures en samenwerkingsovereenkomsten te ontwikkelen. De vraag die rees was of het initiatief om te verstoren van een inlichtingen- en veiligheidsdienst moet/kan komen. Deze kwestie, evenals de naleving van de dienstnota 'disruptie' (er was uiteindelijk geen verstoring), was niet het voorwerp van onderzoek.

I.11.2.6. De noodzaak van een screening voor functies met een openbaar karakter?

Nam de VSSE het (spontane) initiatief om de regering in te lichten toen zij kennis nam van de benoeming van Ihsane Haouach tot regeringscommissaris, of moest zij dat doen? Geldt dit ook voor andere openbare functies?[119] En kan iedereen worden gecontroleerd of is een uittreksel uit het strafregister (vroeger de verklaring van goed gedrag) voldoende? De VSSE controleert niet systematisch elke benoeming van een regeringscommissaris of een ander openbaar ambt. Het is juist dat in de loop van de door de dienst verrichte onderzoeken van tijd tot tijd een persoon opduikt die een openbaar ambt bekleedt. In dergelijke gevallen moet worden overwogen of over deze persoon een nota moet worden geschreven. De VSSE wordt in dit verband niet verzocht systematisch advies uit te brengen. Dit is een besluit dat, indien nodig, op politiek niveau moet worden genomen.[120]

Het risico van instrumentalisering moet altijd in gedachten worden gehouden wanneer een politiek gevoelig onderwerp wordt behandeld. De structuur van de nota's moet hieraan worden aangepast (hieraan wordt nog gewerkt): de analisten moeten uitleggen wat het doel van een nota is, wat de leemten zijn, wat moet worden verduidelijkt, aan wie de nota moet worden verstrekt, enz.

I.12. EEN VERNIEUWDE AANDACHT VOOR DE MOSLIMBROEDERSCHAP

Op 19 juli 2021 verzocht de Begeleidingscommissie het Vast Comité I een toezichtonderzoek te openen met als doel enerzijds te bepalen of de Moslimbroederschap wordt opgevolgd door de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) en, anderzijds, of deze beweging volgens de inlichtingendiensten een bedreiging vormt in België.[121] Het onderzoek volgde op het toezichtonderzoek naar de wijze waarop de VSSE de toenmalige regeringscommissaris, Ihsane Haouach, had opgevolgd (zie I.11).

---

119 Zie in die zin de problemen in verband met de benoeming/verwijdering van Salah ECHALLOUI uit de Grote Moskee van Brussel en de moslimexecutieve (negatief advies van de VSSE).

120 *Cf.* de geclassificeerde nota (VERTROUWELIJK Wet 11.12.1998) van de VSSE van 25 augustus 2021 gericht aan de Voorzitter van het Vast Comité I.

121 Het Vast Comité I voerde eerder al twee toezichtonderzoeken ter zake: In 2001 naar de manier waarop de inlichtingendiensten informatie over terrorisme en de radicale islam verzamelden en analyseerden, alsook naar de manier waarop zij de burgerlijke en gerechtelijke autoriteiten informeerden over dit fenomeen. Dit onderzoek had met name betrekking op de aanwezigheid van de Moslimbroeders in België en op de opvolging daarvan door de VSSE (VAST COMITÉ I, *Activiteitenverslag 2001*, 89-143). In 2007 voerde het Comité een onderzoek om na te gaan of de geformuleerde aanbevelingen (opvolging van de radicale islam) door de inlichtingendiensten, waren opgevolgd (VAST COMITÉ I, *Activiteitenverslag 2007*, 7-29).

I.12.1. DE MOSLIMBROEDERS: CONTEXTUALISERING

I.12.1.1. Ontstaan en internationalisering van de beweging

De wortels van de Moslimbroederschap (afgekort 'de Moslimbroeders') liggen in Egypte, waar de beweging in 1928 werd opgericht door Hassan Al-Banna. Bij haar ontstaan heeft de organisatie twee doelstellingen: Egypte bevrijden van de Britse overheersing en de waarden van de islam opnieuw invoeren in de Egyptische samenleving. In 1948 wordt de beweging in Egypte verboden na een reeks confrontaties tussen een deel van de beweging en de overheid. Zeer snel na haar ontstaan internationaliseert de beweging als gevolg van de ballingschap van meerdere politieke leiders. In België zijn de Moslimbroeders aanwezig sinds de jaren 1960 waar ze zich geleidelijk aan engageerden in sociale, religieuze en jeugdactiviteiten.

I.12.1.2. De omvang van het fenomeen in België?

Om de omvang van een fenomeen te kunnen bepalen, is het noodzakelijk dit duidelijk te definiëren. Het Vast Comité I kon vaststellen dat de term 'Moslimbroeders' zich moeilijk laat definiëren en dat er geen precieze definitie bestaat die algemeen wordt aanvaard door de Belgische inlichtingendiensten en de partners van de strafrechtelijke keten in de ruime betekenis. Het gaat om een entiteit met vage omtrekken, met antennes die grote autonomie genieten in vele landen en die de vorm aannemen van verschillende organisaties die op discrete of zelfs geheime wijze handelen binnen diverse domeinen van de samenleving, met doelstellingen op lange termijn die onverenigbaar zijn met de democratische orde. Aangezien het erg moeilijk is om deze beweging duidelijk te omschrijven, is de studie ervan – en meer bepaald de analyse van haar aanwezigheid en beïnvloedingsmacht in België – bijzonder ingewikkeld. Het is ook zeer moeilijk om te bepalen of een persoon al dan niet deel uitmaakt van deze groepering, aangezien deze laatste als zodanig niet over duidelijke structuren beschikt en geen lidkaarten verdeelt.[122]

[122] Het Comité had al op deze moeilijkheid gewezen in zijn activiteitenverslag 2001 (cf. VAST COMITÉ I, *Activiteitenverslag 2001*, p.113.)

De VSSE maakte echter de volgende raming van de aanwezigheid van deze beweging in België: "*De 'internationale moslimbroeders' in ons land worden vertegenwoordigd door de Ligue des Musulmans de Belgique (LMB), die naar schatting een 50-tal leden telt en enkele honderden aanhangers of sympathisanten. Bij ons bevindt zich ook het hoofdkwartier van een Europese koepelvereniging, de Council of European Muslims (CEM; voordien FIOE) die de belangen verdedigt van de moslimbroeders ten aanzien van de Europese instellingen.*"[123]

Op basis van deze cijfers kwalificeerde de minister van Justitie de aanwezigheid van de beweging in België als 'vrij bescheiden'.[124] Niettemin stelden de minister en de VSSE dat de Moslimbroeders "*invloedrijker zijn en belangrijker lijken dan men zou verwachten op basis van hun beperkte ledenaantal*", als gevolg van hun intense sociale en politieke activisme, hun benadering en het profiel van hun leden.[125]

I.12.1.3. Een beweging die in het buitenland als een bedreiging wordt beschouwd?

De verschillende landen nemen sterk uiteenlopende posities in met betrekking tot deze beweging. In sommige landen behoren politieke partijen die beweren deel uit te maken van de Moslimbroederschap tot de regering of de oppositie in het parlement (bijv. Turkije, Marokko, Algerije, Libië). In andere landen wordt de beweging beschouwd als een criminele organisatie.[126] Met de goedkeuring van de nieuwe Antiterrorismewet van 8 juli 2021 is Oostenrijk het eerste Europese land dat de Moslimbroeders verbiedt als organisatie omwille van hun 'religieus geïnspireerde

123 VSSE, *Jaarrapport 2020,* p. 13.

124 Antwoord van de vice-eersteminister en minister van Justitie en Noordzee d.d. 10 mei 2021 op schriftelijke vraag nr. 7 – 1140 van senator Tom ONGENA van 5 maart 2021.

125 *Ibid*.; VSSE, *Jaarrapport 2020*, p. 13.

126 In Egypte, Rusland, Saoedi-Arabië, de Verenigde Arabische Emiraten en ook in Bahrein wordt ze officieel beschouwd als een terroristische organisatie.

criminaliteit'. Hoewel de beweging in andere Europese landen niet verboden is, wordt er recent de nodige aandacht aan besteed in onze buurlanden.[127]

I.12.2. ONDERZOEKSVASTSTELLINGEN

I.12.2.1. Maakt de beweging voorwerp van opvolging uit door de inlichtingendiensten?

Beide inlichtingendiensten volgen de Moslimbroeders op, zij het vanuit zeer verschillende invalshoeken en met de inzet van zeer verschillende middelen.

De VSSE volgt de beweging prioritair op in het kader van haar bevoegdheid inzake de opvolging van extremisme (art. 7, 1° en art. 8, 1°, c W.I&V) en conform de 'Strategische doelstellingen 2021-2024'[128] en de akkoorden afgesloten met de

---

127 In Nederland werd er in 2019-2020, op initiatief van het parlement, een onderzoek gevoerd naar de invloed die bepaalde buitenlandse staten uitoefenen in het kielzog van de Moslimbroeders, inzonderheid in een poging hun democratie een andere richting uit te sturen. Tweede Kamer der Staten-Generaal, (*On)zichtbare invloed, Verslag parlementaire ondervragingscommissie naar ongewenste beïnvloeding uit onvrije landen*, Den Haag, 25 juni 2020, beschikbaar online: https://www.tweedekamer.nl/kamerstukken/detail?id=2020Z12034&did=2020D25817 De resultaten van deze studie bevestigen dat er sprake is van uitoefening – in diverse vormen – van invloed door meerdere bewegingen, waaronder die van de Moslimbroeders, in het land. Het onderzoek verwijst naar meerdere studies die de Nederlandse inlichtingendienst, i.e. de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), in verband met de Moslimbroeders heeft gevoerd. De AIVD kwam in 2011 tot het besluit dat er van de Moslimbroeders geen directe dreiging uitging voor de democratie of de nationale veiligheid, maar dat de activiteiten van de beweging op lange termijn een risico konden vormen, aangezien de Moslimbroeders antidemocratisch zijn en gekant tegen het integratieproces.
De aanwezigheid van de beweging in Frankrijk en de bedreiging die ze er vertegenwoordigt, werden eveneens bestudeerd in het kader van een onderzoekscommissie van de Franse Senaat die in november 2019 een onderzoek voerde naar '*de antwoorden vanwege de autoriteiten op de ontwikkeling van de radicale islam en de middelen om die te bestrijden*' (vrij vertaald) Verslag nr. 595 (2019-2020), 7 juli 2020, nr. 595, beschikbaar online: https://www.senat.fr/rap/r19-595-1/r19-595-1_mono.html#toc62 In het verslag, dat in juli 2020 werd gepubliceerd, staat dat de Broederschap in Frankrijk ca. 50.000 leden telt.
In Duitsland blijkt uit de antwoorden van de federale regering op meerdere parlementaire vragen dat organisaties die banden onderhouden met de Moslimbroeders in het oog worden gehouden door de nationale veiligheidsdienst, i.e. de *Bundesambt für Verfassungsschutz* (BfV), en door alle bureaus van de deelstaten (*Ländesamts für Verfassungsschutz)*. Er werd vastgesteld dat het aantal leden en sympathisanten van de Moslimbroederschap in het land is gestegen, van 1.040 in 2018 tot 1.350, in: Bundesamt für Verfassungsschutz, *Verfassungsschutzbericht 2019*, www.verfassungsschutz.de/SharedDocs/publikationen/DE/2020/verfassungsschutzbericht-2019.pdf?_blob=publicationFile&v=10, pp. 180-181.

128 Er wordt vermeld dat de strijd tegen terrorisme een prioriteit blijft, maar dat de VSSE beoogt om de aandacht ook meer te vestigen op andere dossiers. Hiertoe zal de VSSE de beschikbare personeelsleden en middelen herverdelen, rekening houdend met de actuele dreiging.

ADIV.[129] De VSSE verzamelt informatie over de Moslimbroeders, de organisaties en de personen die ermee zijn verbonden, inzonderheid door middel van gewone inlichtingenmethoden (meer bepaald menselijke bronnen), maar ook met behulp van bijzondere inlichtingenmethoden. Hieruit worden inlichtingen geëxtraheerd die vervolgens worden verspreid naar de overheden en partners ter informatie en sensibilisatie. De problematiek wordt op de voet gevolgd en de capaciteiten werden herverdeeld voor de uitoefening van deze opdracht.[130]

De ADIV op zijn beurt bestudeert de beweging enkel in het kader van de invloed die deze zou kunnen uitoefenen binnen Defensie en dit conform zijn bevoegdheden (art. 11 W.I&V) en de strategische plannen. De dienst doet aan actieve monitoring door informatie te ontvangen die derden produceren, maar verzamelt zelf geen informatie – op proactieve wijze – over de beweging in haar geheel. Na afloop van het onderzoek was het moeilijk zich uit te spreken over de kwaliteit van de informatiepositie van de ADIV. Het is duidelijk dat de voor de verzameling en analyse ingezette middelen minder omvangrijk zijn dan die van de VSSE aangezien dat – in tegenstelling tot de VSSE die het fenomeen in zijn geheel opvolgt – de ADIV de beweging alleen bestudeert in het kader van de invloed die zij zou kunnen uitoefenen binnen Defensie. Het Comité stelde echter vast dat het niveau van prioriteit dat de ADIV toekent aan de opvolging van het fenomeen niet overeenstemt met de middelen die deze dienst inzet om gegevens te verzamelen en te analyseren. Ten slotte stelt het Comité op basis van de verkregen informatie vast dat de ADIV geen inlichtingen met betrekking tot de Moslimbroeders op eigen initiatief heeft meegedeeld aan de overheden of partners tijdens de afgelopen drie jaren.

I.12.2.2. Wordt de beweging geïdentificeerd als een bedreiging voor België?

De VSSE en de ADIV komen tot gelijkaardige conclusies. Er wordt geen bedreiging tegen een specifieke instelling geïdentificeerd die rechtstreeks verbonden is met de Moslimbroeders. Niettemin omschrijft de VSSE de Moslimbroeders als een extremistische beweging[131]en beschouwt ze de beweging van de Moslimbroeders als een hoge en prioritaire dreiging die aanleiding zou kunnen geven tot antidemocratische gedragingen, tot polarisering of nog, tot schending van fundamentele rechten. De VSSE verduidelijkt: "*Ogenschijnlijk respecteren de Moslimbroeders*

---

129 De akkoorden tussen de VSSE en de ADIV leggen vast dat binnen de domeinen van terrorisme, radicalisme en extremisme, de VSSE over een algemene bevoegdheid beschikt in België, en de ADIV over een bevoegdheid beperkt tot de aspecten van terrorisme en extremisme die betrekking hebben tot de militaire belangen of Belgische militairen.

130 In het dossier werd kort voor 2020 opnieuw geïnvesteerd nadat capaciteiten, tot dusver ingezet op dossiers 'terrorisme en extremisme', werden vrijgegeven.

131 Onder extremisme wordt verstaan "*racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat*" (art. 8, 1°, c W.I&V).

de democratische en wettelijke regels. Op korte termijn streven ze ook doelstellingen na die legitiem lijken. Maar hun intern discours en hun visie en doelstellingen op langere termijn staan haaks op de goede werking van de grondwettelijke orde en democratie."[132] "*Het geijkte middel daartoe is proselitisme ('dawa'), onder meer via prediking en (religieus) onderwijs. De Moslimbroeders beschouwen zichzelf daarbij als een elitaire voorhoede die de verschillende moslimgemeenschappen moet verenigen en leiden. Ze streven ernaar om maatschappelijk invloedrijke posities in te nemen, om zo de westerse samenleving van binnenuit te kunnen veranderen. Bovendien trachten ze op verschillende manieren het overheidsbeleid te beïnvloeden.*"[133]

De ADIV is van oordeel dat: "*Les Frères musulmans promeuvent par certains aspects une vision extrémiste de la religion. Ils représentent un danger en ce qu'ils militent activement, et souvent de façon non transparente, en faveur d'une vision identitaire de l'Islam et renforcent ainsi les clivages au sein de la société et des institutions.*"[134] De ADIV stelt ook nog dat de dienst bijzonder oplettend is voor het risico van infiltratie van de Moslimbroeders binnen Defensie.[135] Het was voor het Comité onbekend of het risico op entrisme hoog ingeschat werd door de ADIV.

I.12.2.3. Samenwerking

I.12.2.3.1. Samenwerking tussen de inlichtingendiensten

In de loop van het onderzoek kon worden vastgesteld dat beide Belgische inlichtingendiensten zowel bilateraal als multilateraal inlichtingen over het Moslimbroederschap uitwisselden met buitenlandse inlichtingendiensten.

Op nationaal niveau, diende te worden vastgesteld dat de samenwerking vooral een éénrichtingsverkeer betrof, te weten het delen van informatie door de VSSE met de ADIV.

I.12.2.3.2. Samenwerking met het OCAD

Gelet op de kwalificatie en het dreigingsniveau zoals toegekend door de VSSE, wenste het Comité na te gaan – zonder zich te verliezen in de details – of ook het OCAD de Moslimbroederschap bestudeert.[136]. Hierover bevraagd, antwoordde

---

132 *Ibid.*, p. 13.

133 *Ibid.*, p. 12.

134 "*De Moslimbroeders promoten door bepaalde aspecten een extremistische visie van religie. Ze vormen een gevaar daar ze actief militeren, en vaak op ondoorzichtige wijze, voor een identitaire visie van de islam en versterken aldus de breuklijnen die bestaan binnen de samenleving en de instellingen*" (vrij vertaald). *Ibid*.

135 Nota van de ADIV van 26 augustus 2021 aan de voorzitter van het Vast Comité I.

136 Het OCAD is immers bevoegd voor de evaluatie van de dreiging inzake extremisme wanneer deze dreiging de inwendige en uitwendige veiligheid van de Staat, de Belgische belangen en de veiligheid van de Belgische onderdanen in het buitenland of elk ander fundamenteel belang van het land zou kunnen aantasten (art. 3 W.OCAD).

het OCAD dat het nooit een nota of een studie had geschreven met betrekking tot de Moslimbroeders. Het OCAD identificeert bovendien geen rechtstreekse dreiging die deze beweging voor België vormt en heeft het dus niet over een dreiging op korte of middellange termijn of bevestigt evenmin het hoge niveau van de dreiging, in tegenstelling tot de analyse van beide inlichtingendiensten.

Geïnterpelleerd door het ontbreken van een gezamenlijke visie tussen enerzijds de VSSE en de ADIV en anderzijds het OCAD wat betreft de dreiging die de Moslimbroeders vertegenwoordigen, concludeerde het Comité dat een overleg tussen deze diensten noodzakelijk is. Het Comité verbaasde zich erover dat dit overleg nog niet had plaatsgevonden, gelet op de prioriteit die de VSSE en de ADIV aan dit dossier toekennen.

I.12.2.4. Welke strategieën hanteren de inlichtingendiensten om de geïdentificeerde dreiging in te dammen?

Om te strijden tegen de strategie van de Moslimbroeders en te vermijden dat de beweging de positie kan innemen van bemiddelaar tussen de moslimgemeenschappen en overheden, is de VSSE van mening dat het van groot belang is om te investeren in sensibilisering van de overheden en de administraties. De reeds genomen en toekomstige initiatieven getuigden dat deze strategie wordt gevolgd door de Veiligheid van de Staat. De dienst heeft twee nota's verspreid; één bestemd voor de inlichtingendiensten en de geassocieerde partners van de strafrechtsketen, de andere voor de bevoegde ministers, met als doel te informeren en te sensibiliseren.

De ADIV stelt dat de bewustmaking van de institutionele actoren voor de pogingen tot beïnvloeding door de Moslimbroeders buiten België deel uitmaakt van de doelstellingen van de briefings die door hen worden gegeven in verband met de terroristische dreiging en het risico dat verbonden is aan radicale religieuze bewegingen. Het Comité beschikt over geen bijkomende informatie op basis waarvan het zich kan uitspreken over de kwantiteit of de kwaliteit van deze bewustmakingsbriefings.

Het Comité is van mening dat deze sensibiliseringsstrategie versterkt kan worden door het organiseren van een structureel overleg tussen de inlichtingendiensten en hun partners (onder andere het OCAD) aangaande deze thematiek. Het sensibiliseren van de politieke overheden en de administraties zal meer effectief zijn als dit wordt gedragen door de drie diensten die voorafgaand overeenstemming hebben bereikt over een gezamenlijke definitie van het fenomeen, zijn samenstellende delen, en de dreiging die ze vertegenwoordigt voor België.

I.13. INFORMATIE- EN COMMUNICATIETECHNOLOGIE IN HET INLICHTINGENPROCES BIJ DE DIRECTIE CYBER VAN DE ADIV EN BIJ DE VSSE

I.13.1. DE *CORE BUSINESS* VAN EEN INLICHTINGENDIENST

Informatie-en communicatietechnologieën (ICT) spelen een steeds belangrijkere rol in de inlichtingenprocessen, zowel bij het verzamelen en de analyse van de basisinformatie als bij de verspreiding van de inlichtingen. De informatie is afkomstig van steeds grotere gegevensstromen, ongeacht de bron. Informatie kan afkomstig zijn van menselijke bronnen (Humint), van partners of van digitale bronnen zoals met name open bronnen of *open sources* (Osint), afluisteroperaties (Sigint) of beeldmateriaal (GeoInt)… De constante groei van de gegevensstromen vereist passende systemen die geschikt zijn om die stromen te absorberen en om een correcte, snelle en doeltreffende analyse mogelijk te maken. De informatica-omgeving moet dus een stabiele en toekomstgerichte tool zijn die ondersteuning kan bieden aan de verschillende actoren die een rol spelen in de inlichtingencyclus. Deze omgeving, zowel de *hardware* als de *software*, moet beantwoorden aan de normen ter zake en de goede IT-praktijken, en moet tegelijk rekening houden met de nieuwe en toekomstige technologische ontwikkelingen[137] zoals 'big data'.[138]

In eerdere onderzoeken stelde het Vast Comité I vast dat de inlichtingendiensten het hoofd moeten bieden aan grote uitdagingen in dit domein. Vooral wat betreft de ADIV is in het verleden al gebleken dat ICT een teer punt is. Het Comité stelde vast dat de inlichtingenactiviteiten niet (langer) voldoende werden ondersteund door ICT. De voorwaarden voor een goed beheer van de informatie werden niet (langer) volledig vervuld.[139] [140]

Daarop startte het Vast Comité I in mei 2019 een 'Toezichtonderzoek betreffende de informaticamiddelen die de Belgische inlichtingendiensten gebruiken om

---

137 Ook voor de toezichthouders is op dat vlak een belangrijke rol weggelegd. Hierover: K. VIETH en T. WETZLING, *Data-driven Intelligence Oversight. Recommendations for a System Update*, Stiftung Neue Verantwortung, November 2019, 63 p.

138 Het begrip '*big data*' verwijst naar de wetenschap van het verzamelen en analyseren van grote volumes gegevens met als doel bepaalde interessante '*patterns*' te ontdekken op basis van een rangschikking ('*clustering*') en statistische analyses die zo hulp kunnen bieden bij de besluitvorming. Deze gegevens worden gewoonlijk gekenmerkt door een grote verscheidenheid, een grote snelheid en een groot volume.

139 VAST COMITÉ I, *Activiteitenverslag 2011*, 7-14 ('II.1. Een audit bij de militaire inlichtingendienst'); *Activiteitenverslag 2018*, 2-18 ('I.1. De werking van de Directie Counterintelligence (CI) van de ADIV').

140 Ook werd in het verslag van de parlementaire onderzoekscommissie naar de aanslagen in Zaventem en Maalbeek de aanbeveling geformuleerd om het informatiebeheer van de diensten te verbeteren om meer bepaald de 'infobesitas' onder controle te houden. Zie 'Onderzoekscommissie naar de terroristische aanslagen van 22 maart 2016. *Parl. St.* Kamer, 2016-2017, nr. 54-1752/008, 15 juni 2017, p. 53 en 180 e.v.

informatie te verzamelen, te analyseren en te communiceren in het kader van de inlichtingencyclus'. Het onderzoek spitste zich toe op de informaticamiddelen die specifiek worden gebruikt ter ondersteuning van de inlichtingencyclus. Het gaat om systemen die worden gehanteerd om gegevens te verzamelen of ook om specifieke analysetools en databanken.[141] Het Vast Comité I voerde geen onderzoek naar de (generieke/standaard) faciliteiten inzake kantoorautomatisering die de diensten gebruiken (bijv. Windows, Word, Excel ...), voor zover ze niet specifiek zijn voor de inlichtingendiensten. Het Comité voerde evenmin een gedetailleerd onderzoek naar het informaticamateriaal (*hardware*) waarover de diensten beschikken, tenzij het specifiek was voor de betrokken inlichtingendienst. Het onderzoek had tot doel de risico's[142] te identificeren waarmee de diensten te maken kregen en die risico's te verminderen door gepaste aanbevelingen te formuleren.

In een eerste luik maakte de ADIV voorwerp uit van onderzoek, en dit omwille van de impact van de herstructurering van deze dienst op het vlak van ICT-tools en werkmethoden. Het onderzoek werd gefinaliseerd in mei 2020 en de resultaten werden opgenomen in het Activiteitenverslag 2020.[143]

Een tweede luik betrof de Directie Cyber van de ADIV en een derde luik de VSSE. De onderzoeksbevindingen van deze laatste twee luiken maken het voorwerp uit van voorliggend onderdeel.

De onderzoeksvragen die werden voorgelegd aan de Directie Cyber van de ADIV en aan de VSSE, luidden als volgt:

– Welke technologieën en tools op het vlak van ICT gebruikt de ADIV/VSSE om zijn activiteiten mee te ondersteunen?
– In hoeverre worden de instrumenten intern ontwikkeld of door externe partners aangeleverd?
– Worden de 'goede praktijken' die inzake ICT gangbaar zijn (hierna 'ITIL')[144] toegepast (meer bepaald: *'change management'*, *'inventory management'*, *'business continuity'*, *'incident management'*, *'problem management'* …)?

---

141 Bij de ADIV worden deze systemen *'weapon systems'* genoemd – naar analogie met bijvoorbeeld systemen die zijn geïntegreerd in de defensieplatformen bij Landsverdediging (bijv. de *software* voor de radarsystemen of *'battle management'*).

142 Een 'risico' werd gedefinieerd als het eventuele bestaan van een min of meer voorzienbare tekortkoming of een bedreiging die een impact kan hebben op de verwezenlijking van de doelstellingen van een organisatie of de efficiënte uitvoering van die doelstellingen, gekoppeld aan de waarschijnlijkheid dat er zich als gevolg van deze tekortkoming of bedreiging een schadelijke gebeurtenis voordoet.

143 VAST COMITÉ I, *Activiteitenverslag 2020* ('I.6. Informatie- en communicatietechnologie in het inlichtingenproces bij de ADIV').

144 ITIL is het acroniem voor '*Information Technology Infrastructure Library*', wat kan worden vertaald als 'Bibliotheek voor de infrastructuur van de informatietechnologieën'. Het gaat om goede praktijken voor het beheer van de IT-diensten die wereldwijd het meest worden gebruikt (bron: www.heflo.com/fr/blog/technologie/definition-itil).

– Is er een *'business continuity plan'*-beleid (BCP) en bestaan er *'disaster recovery plan'*-procedures (DRP) met inbegrip van *back-ups* en zijn die actueel?[145]

Het onderzoek had dus tot doel de risico's te identificeren waarmee de ADIV/VSSE te maken kregen en die risico's te verminderen door aanbevelingen te formuleren. Daarbij was het zogenaamde 'CIA-model'[146] van toepassing en werden drie types risico's onderscheidden:
– *Confidendiality*: het risico van kennisname van al dan niet geclassificeerde gegevens;
– *Integrity*: het risico van ongeoorloofde wijziging van al dan niet geclassificeerde gegevens;
– *Availability*: het risico dat de gegevens niet beschikbaar zijn, wat een obstakel zou vormen voor de goede uitvoering van de opdrachten van de dienst.

I.13.2. DE ICT-OMGEVING EN -ORGANISATIE BIJ DE DIRECTIE CYBER VAN DE ADIV

I.13.2.1. Context

I.13.2.1.1. Equipe en personeel

De informatica voor de Cyber-directie van de ADIV wordt beheerd door een team dat speciaal daarvoor werd samengesteld, aangezien dit de *core business* is van deze directie. Het team is opgesplitst in diverse onderdelen die zich over specifieke materies bekommeren.

Eind maart 2021 beschikte de ICT-cyberafdeling over te weinig personeel: slechts 80% van het totale aantal ICT-medewerkers dat was voorzien, werd aangeworven. Het aanzienlijk personeelsverloop is voornamelijk toe te schrijven aan de personeelswijzigingen in het Egov-kader[147], maar ook aan het vertrek van burgerpersoneel.[148]

---

145 Er bestaan algemeen aanvaarde goede praktijken over hoe het best *back-ups* worden genomen en over welke procedures in geval van een ramp moeten gevolgd worden. Het beheer van *back-ups* is, net als de DRP-procedures (*'disaster recovery plan'*), opgenomen in een algemeen *'business continuity plan'* (BCP).

146 Het gebruik van het CIA-model wordt aanbevolen als basis voor de risicoanalyse volgens de internationale normen ISO 270 betreffende de veiligheid van de informatie, en meer bepaald de norm 27005 die het beheer definieert van risico's in verband met de veiligheid van de informatie. Dit model wordt ook gebruikt door tal van andere normen zoals TCSEC – Orange Book (1983 – VS) of nog Common Criteria (1994 – internationaal).

147 Egov staat in voor de rekrutering en selectie van gespecialiseerde ICT-ers voor overheidsdiensten en instellingen.

148 Het Cyber-personeel bestaat immers uit militairen, ambtenaren met het Camu-statuut en externe medewerkers die via Egov Select worden aangeworven.

De 'servercapaciteit' (fysieke *resources*) volstond op het ogenblik van het onderzoek, maar beantwoordde niet aan de ambities op lange termijn van de dienst (*management plan*). Er werden nieuwe *resources* aangekocht, maar de beslissingen daarover waren afhankelijk van de budgetten die eraan worden toegewezen en dus van de prioriteiten die aan de dienst worden opgelegd.

Wat het beroep op onderaanneming en overheidsopdrachten betreft: aangezien het overgrote deel van de gebruikte *software* afkomstig is van de *opensourcewereld*, wordt er niet systematisch een beroep gedaan op onderaannemers of overheidsopdrachten voor de aankoop van *software*. De ontwikkelingen binnen Cyber gebeuren intern.

I.13.2.1.2. Servers en netwerken

De toegang tot de serverlokalen wordt beheerd door een beveiligd mechanisme. Er worden regelmatig *back-ups* uitgevoerd.

Een *Component Management Database* (CMDB)[149] is voorzien en wordt manueel geüpdatet. Het zou beter zijn als die CMDB automatisch zou worden geüpdatet – niet alleen omdat op die manier de juistheid van de gegevens zou worden gewaarborgd, maar ook omdat op die manier onregelmatigheden zouden worden gedetecteerd.

De monitoring wordt uitgevoerd door verschillende softwareprogramma's. Het gebruik van steeds meer verschillende softwareprogramma's zou echter wel een negatief effect kunnen hebben op de reactiviteit na een waarschuwing. Het zou dan ook aangewezen zijn om zich te concentreren op een centrale *software*.

I.13.2.1.3. Softwaresystemen in de inlichtingenopdracht

Voor wat betreft de belangrijkste softwaresystemen die te maken hebben met de collecte, analyse en verspreiding van inlichtingen (inlichtingencyclus), kon het Comité vaststellen dat de Cyber-divisie haar volledige infrastructuur heeft opgebouwd op basis van een strategisch plan op lange termijn en precieze actieterreinen. Bovendien levert ze zowel op het vlak van de *hardware* als van de *software* de nodige inspanningen om de 'goede ITIL-praktijken' op het terrein toe te passen.

De divisie Cyber gebruikt een aanzienlijk aantal vakspecifieke applicaties, die samen het volledige spectrum van haar opdrachten omvatten. Het Vast Comité I heeft een representatief deel van die applicaties gekozen met verzoek om demonstratie of uitleg.[150]

---

149 Een databank waarin alle ICT-componenten zijn opgenomen – zowel netwerken (switches, routers enz.) als systemen (*servers*, pc's enz.) en *software* (met versienummer).

150 De applicaties die niet werden gekozen voor een demonstratie zijn ofwel vergelijkbaar met de applicaties die wel worden getoond, of zijn bekend in de IT-wereld. De voorkeur werd ook gegeven aan de intern ontwikkelde applicaties of de apparatuur waarvoor het personeel van de Cyber-divisie specifieke scripts moet aanmaken.

De belangrijkste vaststellingen waren de volgende:

- Er zijn slechts weinig *tools* voor *big data* en *datamining*, aangezien Cyber deze in het kader van zijn opdrachten niet nodig heeft: deze divisie houdt zich immers bezig met het opzoeken en het analyseren van bedreigingen, bewustmaking, bescherming van netwerken, enz. Toch beschikken bepaalde *tools* over interne mechanismen die erop lijken.
- Voor de applicaties die door de Cyber-directie worden beheerd, werd een verwerkingsregister samengesteld dat wordt vermeld in de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens.[151] Het register was nog niet volledig operationeel, maar de aanpassingen die eraan moeten worden aangebracht, waren slechts beperkt. Voor die tekortkomingen hoefden dus geen dwingende maatregelen te worden getroffen.
- Het Comité heeft vastgesteld dat het Cyber-netwerk stabiel is en snel werkt. Er werd een monitoringsysteem voor het netwerk en de infrastructuur in het algemeen ingevoerd waarmee storingen kunnen worden gedetecteerd.
- Er worden regelmatig *back-ups* uitgevoerd. Voor de belangrijkste applicaties bestaat een *Disaster Recovery Process* (DRP) met een niet-gestructureerde documentatie. Dat zou moeten worden aangevuld en bijgewerkt naarmate wijzigingen in de infrastructuur worden aangebracht.

I.13.2.1.4. Vulnerability testing en veiligheid

Het Vast Comité I kon vaststellen dat zowel bij de intern ontwikkelde *tools* als bij de aangekochte *tools* bijzondere aandacht wordt besteed aan de veiligheid en de applicatietests. De applicaties ondergaan een hele reeks automatische standaardtests en in voorkomend geval manuele tests, waarbij gebruik wordt gemaakt van producten die algemeen worden erkend om hun doeltreffendheid.

Ook bij de fysieke implementatie van de infrastructuur wordt met de veiligheid rekening gehouden.

Bovendien worden de analyses van potentieel offensieve elementen (bijv. mogelijke *malware*) in beveiligde omgevingen uitgevoerd.

I.13.2.2. Evaluatie van de risico's

Voor elke ICT-onderdeel van de Directie Cyber van de ADIV werden een aantal aandachtspunten opgesomd. In de loop van het onderzoek detecteerde het Comité een aantal risico's, de waarschijnlijkheid dat deze risico's zich voordoen en een

[151] Dit register moet de gegevensbeschermingsautoriteit die het Vast Comité I is in staat stellen om op elk moment op de hoogte te blijven van de manier waarop de persoonsgegevens worden verwerkt, om welke soorten gegevens het gaat, hoelang die gegevens worden bewaard en wie verantwoordelijk is voor de verwerking.

aantal pistes voor beheersing ervan (*mitigation).*[152] De belangrijkste risico's voor de dienst waren:
- het personeelstekort en de rotatie van het personeel;
- de versterking van de fysieke infrastructuur;
- netwerkbewakingstools;
- en de samenwerking met externe diensten.

I.13.3. DE ICT-OMGEVING EN -ORGANISATIE BIJ DE VSSE

I.13.3.1. Context

I.13.3.1.1. Equipe en personeel

Informatica wordt bij de VSSE door een beperkt team beheerd. Dit team vervult een centrale rol, aangezien de steun verleent aan verschillende diensten en bureaus, die de informatie en de inlichtingen verzamelen, analyseren en verspreiden.

Op 1 juni 2021 was het aantal ICT-personeelsleden onvoldoende. Dat geldt des te meer voor het bijzonder beperkte aantal *developpers*.

Wat het inzetten van onderaannemers en het uitschrijjven van overheidsopdrachten betreft, eist de VSSE een veiligheidsmachtiging voor de inschrijvers. De *software* wordt meestal via overheidsopdrachten door externe partijen ontwikkeld of door de dienst aangekocht. De ontwikkelingen die via overheidsopdrachten worden besteld, leveren echter niet noodzakelijkerwijs de gewenste resultaten op ten gevolge van vertragingen op de termijnen, veranderende specificaties, overschrijding van de budgetten, veranderende technologieën, enz.

I.13.3.1.2. Servers en netwerken

De serverlokalen en de back-upsystemen beantwoorden aan strenge veiligheidsnormen, werken efficiënt en werden ontworpen op basis van een specifieke risicoanalyse die regelmatig wordt geüpdatet.

Er is een CMDB voorzien die manueel wordt geüpdatet. Het zou beter zijn als die CMDB automatisch zou worden geüpdatet – niet alleen omdat op die manier de juistheid van de gegevens zou worden gewaarborgd, maar ook omdat op die manier onregelmatigheden beter zouden worden gedetecteerd.

Het beheer van de configuraties en de monitoring worden uitgevoerd door een commerciële tool die in de volledige architectuur is geïntegreerd en gebeuren op de meest kritieke controlepunten (applicaties, *hardware*, netwerk, enz.). Het systeem

[152] Omwille van het vertrouwelijke karakter kon geen gedetailleerde analyse worden gepubliceerd in het openbare activiteitenverslag.

werkt erg goed, maar zou meer performant kunnen zijn voor wat betreft de proactieve detectie van onregelmatigheden.

I.13.3.1.3. Softwaresystemen in de inlichtingenopdracht

Wat betreft de belangrijkste *software*systemen die te maken hebben met de collecte, analyse en verspreiding van inlichtingen (inlichtingencyclus), kon het Comité vaststellen dat de VSSE één enkele 'gespecialiseerde' databank gebruikt. Het is mogelijk dat er andere databanken bestaan die deel uitmaken van applicaties, maar dit zijn slechts technische databanken die de werking van die applicaties mogelijk maken. Deze gespecialiseerde databank werd regelmatig verbeterd en onlangs naar een recentere technologie gemigreerd.

De optie die begin 2020 werd genomen voor de modernisering van de gespecialiseerde databank was een consolidatie en een reorganisatie van de databanken (van het SQL-type) met de toevoeging van zoekindexen. Die methode is relatief goedkoop (*hardware*, implementatietijd) en levert resultaten op voor de vaakst uitgevoerde SQL.

Het Atlas-project werd in 2015 (budgetdossier) en 2017 (ontwikkeling) opgestart met de bedoeling om de laatste levering tegen eind 2021 uit te voeren. Het doel van dit project was om alle gegevens van de VSSE te centraliseren, ongeacht of ze van een externe verzender afkomstig zijn of binnen de dienst werden aangemaakt. Zoekopdrachten zullen hierdoor niet langer per entiteit gebeuren, maar wel op basis van relevantie ten opzichte van de inhoud (van een bestaande fiche, een document, een rapport…).[153] Dit project, uitgewerkt met het bedrijf Smals, beantwoordt ook aan de vereisten van de analyse van *big data*. Nog niet alle componenten zijn geleverd of in productie genomen. Het Vast Comité I kon een demonstratie bijwonen van de reeds ontwikkelde stabiele functionaliteiten. Er werden aan het Comité problemen gemeld in verband met de behandeling van bepaalde behoeften van de gebruikers en zorgen in verband met de planning.[154]

Wat betreft de applicaties die door de VSSE worden beheerd, was het verwerkingsregister dat wordt vermeld in de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, in uitvoering. Het Comité kon vaststellen dat dit register niet volledig operationeel was, maar de aanpassingen die eraan moesten worden aangebracht, slechts beperkt waren. Deze tekortkomingen vereisten geen specifieke maatregelen.

---

153 De gegevens worden dan onderling met elkaar in verband gebracht via een correlatiegrafiek die een weging toekent op basis van de vermelde relevante thema's of woorden.

154 Daaruit blijkt dat de communicatie tussen het projectteam en de essentiële gebruikers over specifieke behoeften (en dan meer bepaald in verband met BIM) veel te beperkt is, als ze al plaatsvindt. Het Atlas-project lijdt ook in zijn geheel aan vertragingen, terwijl ook het voorziene budget al is overschreden. Er moesten dan ook keuzes in verband met de implementatieprioriteit worden gemaakt.

Het Comité heeft vastgesteld dat het netwerk stabiel is en snel werkt. Er werd een monitoringsysteem voor het netwerk en de infrastructuur in het algemeen ingevoerd waarmee storingen kunnen worden gedetecteerd. Deze monitoring doet aan detectie van problemen die zich hebben voorgedaan, eerder dan proactief te werken.

De *back-ups* worden dagelijks vakkundig gemaakt. Voor de belangrijkste applicaties bestaat een *Disaster Recovery Process* (DPR). Aangezien de andere applicaties meer *support*-elementen zijn die in *standalone* werken op vaste stations, volstaat de documentatie die door de firma wordt geleverd. Het DRP-proces past in het kader van een algemener *Business continuity plan* (BCP).

Tot slot heeft het Comité verschillende bestaande of in ontwikkeling zijnde softwarepakketten bekeken, waaronder het Tardis-project (ook Bavak genoemd), dat eind 2016 van start is gegaan. Deze te ontwikkelen software moest online acties op de verschillende sociale netwerken automatiseren, informatie extraheren (met automatische vertaling van de informatie), analyseren en in een rapport exporteren. Na verloop van tijd werd het project complexer omdat verschillende functies werden toegevoegd. Het project werd uiteindelijk begin 2021 door de VSSE stopgezet, nadat duidelijk was geworden dat het niet aan de verwachtingen voldeed. De sociale netwerkaccounts waarop de *software* actief was, werden snel verwijderd omdat de aanwezigheid van de *software* was ontdekt. [155]

I.13.3.1.4. Vulnerability testing en veiligheid

Het Vast Comité I kon vaststellen dat op de intern ontwikkelde programma's veiligheidstests worden uitgevoerd. De andere *applicaties* zijn afkomstig van de *opensource*-wereld, of zijn commerciële oplossingen. Voor sommige is een certificatie aanwezig; voor andere bestaat geen enkele waarborg dat een penetratietest werd uitgevoerd. Er worden frequent updates aangeleverd dewelke door de VSSE worden toegepast. De VSSE werkt voornamelijk op een 'secure' netwerk dat niet met het internet is verbonden en onderworpen is aan een homologatie van de NVO.

Een ander punt in verband met de beveiliging betreft het *loggen*. Elke applicatie wordt gelogd (toegangen en acties van de gebruikers).

[155] Zie hierover in het bijzonder de Vraag van S. THEMONT aan de minister van Binnenlandse Zaken over 'Le logiciel de détectage de menaces terroristes ou de radicalisation' (Vr. en Ant., Kamer, 2020-2021, 3 mei 2021, n°50, p.306, Vr. nr.456) ; de Vraag van V. SCOURNEAU aan de minister van Buitenlandse Zaken en Defensie over 'OSINT' (Vr. en Ant., Kamer, 2019-2020, 5 augustus 2020, n°24, p.465, Vr. nr. 407).

I.13.3.2. Evalutie van de risico's

Voor elke ICT-onderdeel van de VSSE werden een aantal aandachtspunten opgesomd. In de loop van het onderzoek detecteerde het Comité een aantal risico's, de waarschijnlijkheid dat deze risico's zich voordoen en een aantal pistes voor beheersing ervan (*mitigation).*[156] De belangrijkste risico's voor de dienst waren:
- het personeelstekort en enkele specifieke profielen in het bijzonder;
- de beveiligde communicaties;
- het project Atlas en meer in het bijzonder de aan het Comité gemelde problemen aangaande het te weinig rekening houden met de noden van het personeel alsook omtrent de timing.

I.14. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2021ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2021 WERDEN OPGESTART

I.14.1. DE TOEPASSING VAN NIEUWE (BIJZONDERE) INLICHTINGENMETHODEN

Het Comité kreeg een aantal controlemogelijkheden bij voor wat betreft sommige 'gewone' methoden. Het betreft onder meer het toezicht op de identificatie van de gebruiker van telecommunicatie (art. 16/2 W.I&V), de toegang tot passagiersgegevens (Passenger Name Record) (art. 16/3 W.I&V), de toegang tot politionele camerabeelden (art. 16/4 W.I&V), of nog, de controle voorafgaand aan intercepties, intrusies in een informaticasysteem en de opname van bewegende beelden (art. 44/3 W.I&V).

Het Comité besliste om deze thematiek te bestuderen in zijn in 2019 geopende '*toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten de recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld*'.

In 2020 kwam het accent te liggen op de ontwikkeling van een methodologie in het kader van de controle op de identificatie van de gebruik van telecommunicatie (art. 16/2 W.I&V) alsook de toegang tot PNR-gegevens (art. 16/3 W.I&V).

Eind 2020 begin 2021 werd het methodologische luik aangaande de controle voorafgaand aan intercepties, intrusies in een informaticasysteem en de opname van bewegende beelden (art. 44/3 W.I&V) gefinaliseerd.

---

156 Omwille van het vertrouwelijke karakter kon geen gedetailleerde analyse worden gepubliceerd in het openbare activiteitenverslag.

In 2021 boog het Comité zich over de operationalisering van artikel 16/4, §2 W.I&V. Dit artikel regelt de retroactieve opvraging van politionele camerabeelden door de inlichtingendiensten. De wetsbepaling kent een algemene werking. Dit zorgt ervoor dat de erin gestelde procedurele vereisten zowel van toepassing zijn op de gerichte opvragingen van politionele camerabeelden via een rechtstreekse (*online*) toegang tot de betrokken politionele gegevensbanken alsook op de gerichte opvragingen via een schriftelijke bevraging van de bevoegde politiedienst (i.c. de Directie van de politionele informatie en de ICT-middelen bij de Federale Politie (DRI)).[157] Omwille van een DPA-klacht werd het onderzoek opgeschort. De klacht vormde de aanleiding tot de '*Verwerkingsinstructie van het Vast Comité I (DPA) m.b.t. de door de inlichtingendiensten ingestelde retroactieve opvragingen van politionele camerabeelden gegrond op artikel 16/4, §2 W.I&V*'. Na ontvangst en analyse van de statistieken van de twee inlichtingendiensten met betrekking tot de inzet van deze methode, wordt het onderzoeksrapport geredigeerd.

I.14.2 DE OPVOLGING VAN VRIJGELATEN TERRO-VEROORDEELDEN DOOR DE VSSE

In België werden tussen 2015 en 2020 zowat 500 personen veroordeeld voor feiten die verband hielden met terroristische activiteiten.[158] Sommigen onder hen werden veroordeeld bij verstek, en konden dus ook niet in hechtenis worden genomen. Een aantal van die veroordeelden genieten van penitentiair verlof, hebben inmiddels hun straf in de gevangenis uitgezeten of werden, na beslissing van de strafuitvoeringsrechtbank, voorwaardelijk (voor het strafeinde) vrijgelaten.

Gezien het door de Belgische en Europese inlichtingendiensten ingeschatte potentiële gevaar voor recidive, besliste het Comité halfweg 2019 een toezichtonderzoek te openen naar '*de wijze waarop de Belgische inlichtingen- en veiligheidsdiensten de opvolging verzekeren van enerzijds personen die in België verdacht worden van terroristische misdrijven die in België of elders zijn gepleegd en die genieten van een maatregel bedoeld in de Wet van 20 juli 1990 en anderzijds personen, die in België veroordeeld zijn voor terroristische misdrijven en die de Belgische gevangenis verlaten in het kader van één van de maatregelen bedoeld in de Wet van 17 mei 2006, hetzij die definitief vrijgelaten werden (art. 71 van genoemde wet)*'.

Er wordt bestudeerd op welke wijze beide inlichtingendiensten (VSSE en ADIV) deze thematiek opvolgen, welke middelen en methoden er daartoe worden ingezet en hoe de samenwerking verloopt met de partners (o.m. het OCAD, het

---

157 Koninklijk besluit tot wijziging van het koninklijk besluit van 12 oktober 2010 houdende uitvoering van diverse bepalingen van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en het koninklijk besluit van 3 juli 2016 houdende uitvoering van artikel 21 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, *B.S.*, 4 november 2019.

158 *Parl. St*. Kamer 2021-22, CRIV55PLEN148, 25.

Directoraat-generaal Penitentiaire Inrichtingen, de Justitiehuizen, de Lokale en de Federale Politie…) en binnen welke structuren (*Local Task Forces,* de Werkgroep gevangenissen…). Ten slotte werd via *benchmarking* de Franse en Engelse manier van aanpak bestudeerd.

In 2021 werd, na de eerste resultaten, beslist het spectrum van het onderzoek te verruimen. Om het wijze van aanpak van de opvolging van deze gedetineerden *na* hun vrijlating te doorgronden, zag het Comité zich genoodzaakt om zich ook te verdiepen in hun opvolging door de inlichtingendiensten *tijdens* de detentie. Er diende eveneens rekening te worden gehouden met wetgevende evoluties en nieuwe reglementeringen, zoals bijvoorbeeld de publicatie in september 2021 door het OCAD van de 'Strategie Extremisme en Terrorisme' (kortweg Strategie TER). Het onderzoek wordt gefinaliseerd in het eerste semester van 2022.

I.14.3. HET RISICO OP INFILTRATIE BIJ DE TWEE INLICHTINGENDIENSTEN

Afgelopen jaren werd de internationale inlichtingenwereld opgeschrikt door een aantal *cases* van infiltratie (en *insider threat*). Het Comité nam het initiatief een toezichtonderzoek op te starten naar de wijze waarop de twee inlichtingendiensten met het risico op infiltratie omgaan: welke risico's worden onderkend, welke tegenmaatregelen worden genomen om ze te beheersen en om er op te reageren indien ze zich voordoen?

Er vonden diverse werkvergaderingen met de ADIV en de VSSE plaats over de thematiek 'cartografie en risico-evaluatie van infiltratie in de schoot van de inlichtingendiensten'. Het proces van risicomanagement zoals hernomen in de ISO 31000-norm vormde daarbij de vertrekbasis.[159] De verwerking van de verzamelde informatie liep vertraging op, en dit in hoofdzaak omwille van de gezondheidscrisis en zijn impact op de effectieven van het Comité, maar ook omwille van andere, meer dringende dossier (de zaak-Conings, *supra*).

I.14.4. MOGELIJKE DREIGINGEN VOOR HET BELGISCHE WETENSCHAPPELIJK EN ECONOMISCH POTENTIEEL (PRISM/WEP): OPVOLGONDERZOEK

In 2016 werd een toezichtonderzoek afgerond naar de bescherming van het wetenschappelijk en economisch potentieel naar aanleiding van de zgn. 'Snowden-

[159] www.iso.org:fr/iso-31000-risk-management.html

onthullingen'.[160] Deze onthullingen gaven een inkijk in onder meer het bestaan van het PRISM-programma waarbij de Amerikaanse *National Security Agency* (NSA) (meta)data van telecommunicatie verkreeg en brachten verder aan het licht dat Amerikaanse maar ook Britse diensten inlichtingenoperaties hadden opgezet ten aanzien van bepaalde internationale instellingen en samenwerkingsverbanden (VN, EU en G20) waarbij ook 'bevriende landen' werden geviseerd. Het onderzoek behandelde de mogelijke implicaties van buitenlandse programma's op de bescherming van het wetenschappelijk en economisch potentieel van het land. Het ging na of de Belgische inlichtingendiensten aandacht besteedden aan dit fenomeen; een reële of mogelijke bedreiging detecteerden voor het Belgische wetenschappelijk en economisch potentieel; er de bevoegde overheden van in kennis hadden gesteld en beschermingsmaatregelen hadden voorgesteld; en over voldoende en adequate middelen beschikken om deze problematiek op te volgen. Ook werd bestudeerd welke de gevolgen waren van het PRISM-programma en/of andere analoge systemen voor het wetenschappelijk en economisch potentieel van het land.

Eind november 2019 verzocht de parlementaire Begeleidingscommissie het Vast Comité I om dit toezichtonderzoek terug op te nemen en te actualiseren. In 2020 werd, na het uitvoeren van de eerste onderzoeksopdrachten – meer in het bijzonder de verzameling en analyse van het open bronnenmateriaal – beslist om dit onderzoek te fusioneren met het toezichtonderzoek naar de operatie Rubicon (cf. I.14.6). In 2021 vonden tussen het Vast Comité I en beide inlichtingendiensten hieromtrent ontmoetingen en bevragingen plaats. Ook werden er vragen voorgelegd aan het Belgische Centrum voor Cybersecurity (CCB). Ook in deze liep de redactie van het toezichtrapport vertraging op omwille van meer urgent onderzoek, te weten de zaak-Conings (cf. I.9.). De resultaten worden verwacht voor begin 2022.

160 VAST COMITÉ I, *Activiteitenverslag 2016*, 52 e.v. Voluit 'Toezichtonderzoek over de aandacht die de Belgische inlichtingendiensten (al dan niet) besteden aan de mogelijke dreigingen voor het Belgische WEP uitgaande van op grote schaal door buitenlandse grootmachten en/of inlichtingendiensten gehanteerde elektronische bewakingsprogramma's op communicatie – en informatiesystemen'.

I.14.5. SPIONAGE VIA GEMANIPULEERDE CODEERAPPARATRUUR: DE OPERATIE RUBICON

De 'Operatie Rubicon'[161] of de inlichtingenoperatie waarbij Amerikaanse en Duitse inlichtingendiensten met het Zwitserse bedrijf Crypto AG als dekmantel meerdere decennia meeluisterden met versleutelde communicatie van overheden in tientallen landen, geraakte halfweg februari 2020 in de openbaarheid.[162] Onder andere Nederland, Frankrijk, Zweden en Denemarken (de 'Maximator-landen') waren zgn. '*cognescenti*': ingewijden in de cryptologische details van bepaalde apparaten. Onder meer België, "*waardevol voor de verheldering die zijn rapporten bood over diplomatieke gebeurtenissen*" en vooral interessant als diplomatiek centrum van de NATO en de (toenmalige) Europese Economische Gemeenschap, zou zijn afgeluisterd.

Het Comité besloot een toezichtonderzoek te openen, waarmee een antwoord werd gezocht naar vragen als[163]: in welke mate waren de Belgische inlichtingendiensten op de hoogte waren (of in welke mate dienden ze er – gezien hun wettelijke opdrachten – van op de hoogte te zijn van deze operatie? Werden hierover inlichtingen verzameld of werd dit niet wenselijk geacht? Maar belangrijker nog: bieden de diensten op dit ogenblik voldoende bescherming ter zake? Zijn er risico-analyses voorhanden? Als crypto-materiaal wordt gebruikt, welke voorzorgsmaatregelen worden er dan genomen? Hoe wordt heden ten dage omgegaan met deze crypto-problematiek… Eind september 2020 werd beslist om dit onderzoek samen te voegen met het opvolgonderzoek PRISM/WEP (cf. I.14.4).

I.14.6. (BIJKOMENDE) INLICHTINGENCAPACITEITEN IN HET BUITENLAND VOOR DE BELGISCHE INLICHTINGENDIENSTEN?

Gelet op de door de wetgever omschreven inlichtingenopdracht bevindt de voor de inlichtingendiensten relevante informatie zich zowel in het binnen- als in het

---

161 Het tijdschrift *Intelligence and National Security* (Volume 35, August 2020, Issue 5) wijdde hieraan een themanummer. Zie daarin onder meer R. ALDRICH et al., 'Operation Rubicon: sixty years of German-American success in signals intelligence'; M.J. DOBSON, 'Operation Rubicon: Germany as an intelligence 'Great Power" en B. JACOBS, 'Maximator: Europan signals intelligence cooperation from a Dutch perspective'.

162 Er werd ruchtbaarheid gegeven aan evaluatierapporten van de Amerikaanse en Duitse inlichtingendiensten door de Duitse televisiezender ZDF en de Washington Post. Het Nederlandse onderzoeksplatform Argos kreeg inzage in de rapporten, dewelke onder meer door De Tijd werden overgenomen (L. BOVÉ, *De Tijd*, 13 februari 2020, ('Geheime documenten onthullen spionage van België door CIA en Duitse BND')).

163 Maar bijvoorbeeld ook: wat is de betekenis/waarde van de notie 'bevriende Staat' in de context van inlichtingendiensten en in welke mate bepaalt die notie de houding van de eigen inlichtingendiensten?

buitenland. In september 2020 werd daarom een toezichtonderzoek geopend 'naar de behoefte voor (bijkomende) inlichtingencapaciteiten voor de Belgische inlichtingendiensten in het buitenland'. De doelstelling van het onderzoek is divers:

- Nagaan of de VSSE/ADIV actueel enige operationele informatiegaring in het buitenland verrichten, en zoja, onder welke vorm en via welke concrete inlichtingenactiviteiten;
- Toetsen van deze buitenlandse activiteiten aan het bestaand regelgevend kader;
- Nagaan of de diensten nood hebben aan bijkomende bevoegdheden waaronder juridische mogelijkheden (m.a.w. onderzoeksbevoegdheden) om in het buitenland informatie te kunnen inwinnen.

In 2021 werden, op basis van een analyse van het betreffende juridische kader, de VSSE en de ADIV bevraagd over de eventuele inlichtingenactiviteiten die zij uitvoeren in het buitenland. Omwille van andere prioriteiten en gezien de impact van de gezondheidscrisis op de effectieven van het Comité, werd de analyse van deze antwoorden onderbroken. Het onderzoek zal worden afgesloten in de loop van 2022.

I.14.7. CONTROLE OP DE SPECIALE FONDSEN: OPVOLGONDERZOEK

Zoals elke overheidsdienst, krijgen ook de inlichtingendiensten overheidsgeld toegekend voor de uitoefening van hun wettelijke opdrachten. De normale regel bij de besteding van die gelden is dat er volledige transparantie en controle moet zijn. Maar aangezien bepaalde taken van de VSSE en de ADIV onvoorzienbaar zijn of geheim moeten blijven, ontsnapt een deel van hun budget aan die 'normale regel'. Dat deel is beter gekend als de 'speciale fondsen'. Hoewel het bedrag van die fondsen deel uitmaakt van het budget dat aan de diensten wordt toegewezen, gelden er bijzondere regels voor het beheer, het gebruik en de controle ervan. Het Comité onderzocht in 2015[164] onder meer welke de 'speciale fondsen' zijn, om welke bedragen het gaat en hoe ze worden verdeeld. Het controleerde ook de wijze waarop de middelen werden aangewend en hoe de wisselwerking verloopt tussen deze 'speciale fondsen' en de 'normale' budgetten. Ook werd het reglementaire kader bestudeerd en onderzocht welke controlemechanismen er bestaan, en dit zowel intern (binnen de diensten) als extern (Rekenhof, Vast Comité I...). Diverse aanbevelingen werden geformuleerd.

164 VAST COMITE I, *Activiteitenverslag 2015*, 12-15 ('Het beheer, het gebruik en de controle van de speciale fondsen').

Sinds 2018 (VSSE) en 2020 (ADIV) uitte het Rekenhof het voornemen om eveneens een periodieke controle te doen van deze fondsen.[165] Daarbij kon het Rekenhof beroep doen op de technische ondersteuning zoals voorgeteld door het Vast Comité I.[166] Het Comité op zijn beurt kon dan weer "*exercer sa mission avec plus d'attention sur l'utilisation de ces dits fonds*". In 2020 werd een opvolgonderzoek opgestart naar het beheer, het gebruik en de controle van de speciale fondsen. Onderbroken omwille van andere, meer prioritaire dossiers in 2021, worden de onderzoeksactiviteiten hernomen in 2022.

I.14.8. ONDERZOEK NAAR DE OPVOLGING DOOR DE INLICHTINGENDIENSTEN VAN 'DES MOUVEMENTS SECTAIRES À OBÉDIENCE RELIGIEUSE AYANT DES VISÉES POLITIQUES'

In juli 2021 opende het Vast Comité I op verzoek van de Voorzitster van de Kamer van volksvertegenwoordigers een onderzoek naar "*la manière dont les services de renseignement s'intéressent aux activités des mouvements sectaires à obédience religieuse ayant des visées politiques (autres mouvements salafistes politiques, Opus Dei, mouvement Civitas, etc.)*".[167]

Dit was het derde onderzoek van een drieluik en volgde als dusdanig twee eerder door het Comité gerealiseerde onderzoeken op, te weten het onderzoek naar de wijze waarop de VSSE de regeringscommissaris Ihsane Haouach had opgevolgd[168] en het onderzoek naar de aandacht van de inlichtingendiensten voor de Moslimbroederschap.[169]

Eind 2021 en na enkele incoherenties te hebben verduidelijkt, werd in samenspraak het spectrum van het onderzoek geherdefineerd naar '*les organisations à obédience religieuse ayant des visées politiques*'.

---

165 Het Comité kreeg in 2020 kopie van de in 2019 door het Rekenhof uitgevoerde controle bij de VSSE voor het boekjaar 2018 COUR DES COMPTES, *Sûreté de l'Etat. Contrôle 2019 des fonds spéciaux. Rapport adressé au ministre de la Justice*, 20 mai 2020.

166 "*Ce contrôle sera périodique et comportera, outre un examen des processus et un contrôle de caisse, un contrôle formel réalisé par sondage et portant sur l'existence des pièces justificatives conformes aux instructions et approuvées par les fonctionnaires compétents. Le contrôle ne portera pas sur le bien-fondé ou la bonne gestion des opérations sous-jacentes et sera mis en œuvre, dans le respect des missions du SGRS, par des auditeurs disposant de l'habilitation de sécurité requise*".

167 Brief van 19 juli 2021 van de Voorzitster van de Kamer, E. TILLIEUX, aan de voorzitter van het Vast Comité I.

168 Zie 'I.11. De opvolging van een regeringscommissaris door de VSSE' (*supra*).

169 Zie 'I.12. Een vernieuwde aandacht voor de Moslimbroederschap' (*supra*).

HOOFDSTUK II.

DE CONTROLE OP DE BIJZONDERE EN BEPAALDE GEWONE INLICHTINGENMETHODEN

Het Vast Comité I is gehouden tot transparantie over de inzet van de zogenaamde 'bijzondere inlichtingenmethoden'(BIM) door de inlichtingendiensten: artikel 35 §1, 1° van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse (W.Toezicht) – zoals gewijzigd door artikel 25 BIM-Wet[170] vermeldt immers dat het Comité in zijn activiteitenverslag "*specifiek aandacht besteedt aan de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, zoals bedoeld in artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten […]*". En verder (art. 35 §2 W.Toezicht) dient het Comité jaarlijks verslag uit te brengen *"aan de Kamer van Volksvertegenwoordigers over de toepassing van artikel 16/2 en artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten […].*[171] *Het verslag bevat het aantal gegeven machtigingen, de duur van de uitzonderlijke methoden voor het verzamelen van gegevens, het aantal betrokken personen en, in voorkomend geval, de behaalde resultaten.*[172] *Het verslag vermeldt ook de activiteiten van het Vast Comité I.*"

Voorliggend hoofdstuk bevat dan ook cijfermateriaal over de inzet door enerzijds de Veiligheid van de Staat (VSSE) en anderzijds de Algemene Dienst Inlichting en Veiligheid (ADIV) van de specifieke en de uitzonderlijke methoden (gegroepeerd als de zgn. 'bijzondere inlichtingenmethoden') én van de gewone methoden waarin aan het Comité een bijzondere controleopdracht wordt toegekend (de zgn. 'gewone methoden plus').

---

170 Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, *BS* 10 maart 2010.

171 Een afschrift van dit jaarlijks verslag wordt eveneens bezorgd aan de ministers van Justitie en Landsverdediging alsook aan de Veiligheid van de Staat en de Algemene Dienst Inlichting en Veiligheid, die de mogelijkheid hebben de aandacht van het Vast Comité I te vestigen op hun opmerkingen (art. 35 §2 W.Toezicht).

172 Een specifiek verslag over de 'behaalde resultaten' is vooralsnog niet aan de orde. Het Comité is zich bewust van het gegeven dat hier een belangrijke opdracht ligt: *"there will be an important job for oversight bodies to measure the effectiveness of these new techniques while nonetheless providing public assurance that any new powers or resources are proportionate to the threat and not abused"*, in: I. LEIGH and N. WEGGE, *Intelligence oversight in the twenty-first century. Accountability in a changing world*, Routledge, 2020, 18.

Tevens wordt verslag gedaan over de wijze waarop het Vast Comité I zijn (jurisdictionele) controletaak op deze methoden heeft waargenomen. Destijds heeft het Comité de keuze gemaakt om zijn rechtspraak te publiceren in de jaarlijkse activiteitenverslagen. De beslissingen die soms geclassificeerde elementen bevatten, worden uiteraard niet *in extenso* gepubliceerd. Alleen de juridisch relevante elementen en de hoogstnodige feiten worden weergegeven. Dergelijke transparantie is (vrij) uniek. De afgelopen jaren hebben ondertussen echter bewezen dat dit kan zonder daardoor de werking van de inlichtingendiensten in het gedrang te brengen.

Merk ten slotte op dat het Comité ook kan gevat worden in zijn hoedanigheid van 'pre-judicieel adviesverlener' (art. 131*bis*, 189*quater* en 279*bis* Sv.).[173] In dat geval geeft het Comité een advies over de al dan niet rechtmatigheid van specifieke of uitzonderlijke methoden die inlichtingen hebben opgeleverd die in een strafzaak worden gebruikt. Tot op heden blijft dit evenwel een louter theoretisch concept; afgelopen decennium werd nog nooit van deze mogelijkheid gebruik gemaakt.[174]

II.1. CIJFERS MET BETREKKING TOT DE BIJZONDERE EN BEPAALDE GEWONE METHODEN

II.1.1. ALGEMENE TRENDS

II.1.1.1. Inzet van bijzondere inlichtingenmethoden door de VSSE en de ADIV

De wetgever opteerde er destijds voor om een duidelijke onderverdeling aan te brengen tussen de verschillende methoden van gegevensverzameling, in de wet geduid als gewone, specifieke of uitzonderlijke methoden. Deze zijn (of beter: zouden moeten zijn) in de zwaarte van de inbreuk op het privéleven oplopend en hebben ieder hun eigen toetsingskader en controlemechanisme, eveneens oplopend in

173 Hierover: VAST COMITE I, *Activiteitenverslag 2010*, 59.

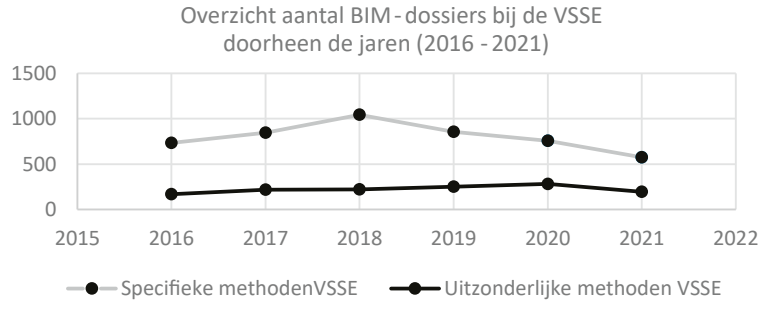
174 De beslissing om een advies te vragen berust bij de onderzoeksgerechten of de strafrechters. Over de beperkte toepassing ervan, zie: VANDERBORGHT, J., '*If you torture the data long enough, it will confess. Enkele cijfers over de inzet van bijzondere inlichtingenmethoden*', in VANDERBORGHT, J. (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers*, Intersentia, Antwerpen, 2020, 25.

'zwaarte'.[175] Hiermee werd beoogd te verhinderen dat de diensten niet meteen naar het zwaarste middel zouden grijpen.

Tussen 1 januari en 31 december 2021 werden door de twee inlichtingendiensten samen 1823 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 1570 door de VSSE (waarvan 1220 specifieke en 350 uitzonderlijke) en 253 door de ADIV (waarvan 166 specifieke en 87 uitzonderlijke).[176]

175 Deze opdeling blijkt voor sommige experten te theoretisch en houdt te weinig rekening met de realiteit. Zie bijv. W. VAN LAETHEM, 'Enkele reflecties over tien jaar BIM-controle door het Vast Comité I', in VANDERBORGHT, J. (ed.), *o.c.*, 70-72. Het Comité is eenzelfde mening toegedaan en haalde bij wijze van voorbeeld artikel 16/3 W.I&V (verzamelen en verwerken van passagiersgegevens) en 16/4 W.I&V (verzamelen en verwerken van politionele camerabeelden) aan. Hoewel beide onderzoeksbevoegdheden als gewone methoden worden gekwalificeerd, is de inmenging in de privacy en de gegevensbescherming bij deze methoden vaak groter dan bij specifieke en zelfs uitzonderlijke inlichtingenmethoden. Dit is zeker het geval bij het cameragebruik wanneer hierbij intelligente camera's of *software* worden gebruikt zoals ANPR. Zie VAST COMITÉ I, Advies nr. 001/VCI/2021 van 12 juli 2021 (Wijzigingen Inlichtingenwet), consulteerbaar op www.comiteri.be. De inlichtingendiensten op hun beurt wijzen in dit kader op de noodzaak tot instandhouding van het gelijkheidsbeginsel met de bijzondere opsporingsmethoden (BOM).

176 De inlichtingendiensten houden er een andere wijze van telling op na. Bij de VSSE wordt gerekend in 'BIM dossiers', waarbij één dossier meer dan één methode kan bevatten. Eenzelfde tendens blijft evenwel merkbaar:

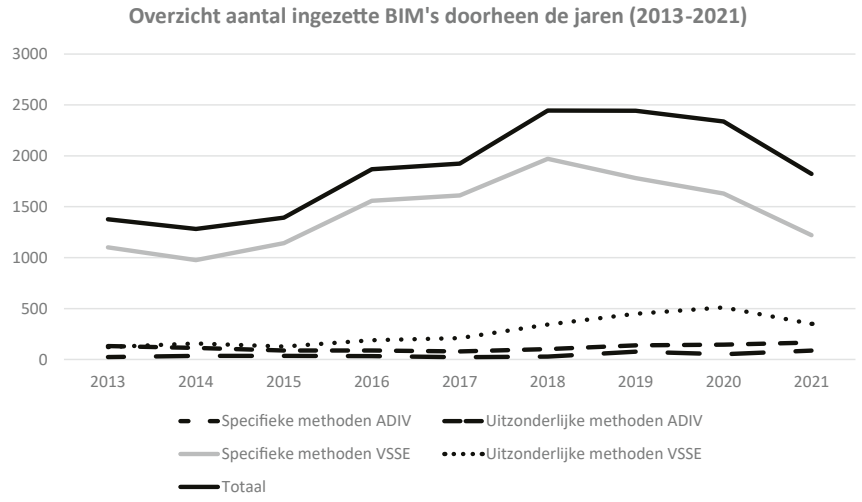


Ook de ADIV telt anders: de dienst telt de methoden per artikel, zonder een onderscheid te maken tussen de verschillende paragrafen, wat het Comité wel doet. De ADIV-cijfers omvatten ook het geheel van alle ingediende aanvragen (inclusief deze dewelke intern werden afgewezen). Ten slotte wordt door de ADIV een methode meegeteld in het jaar waarin de aanvraag werd ingediend, ongeacht wanneer de methode effectief werd toegelaten.

Onderstaande tabel maakt een vergelijking met de cijfers van de afgelopen jaren.

	ADIV		VSSE		TOTAAL
	Specifieke Methoden	Uitzonderlijke methoden	Specifieke Methoden	Uitzonderlijke methoden	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445
2019	138	76	1781	449	2444
2020	146	51	1629	511	2337
2021	166	87	1220	350	1823

Dit kan als volgt grafisch worden weergegeven:



Na een constante stijging van het aantal ingezette BIM's tot 2018 en een stagnatie in 2019-2020, diende in 2021 een significante daling te worden opgetekend.[177] Let wel, als de cijfers worden uitgesplitst naar de diensten, dient voor 2021 een aanzienlijke stijging te worden vastgesteld (circa 30%) van het aantal door de ADIV ingezette BIM's. Daartegenover staat een aanzienlijke daling (circa 28%) bij de VSSE (*infra*).

177 Per toegelaten methode kunnen wel meerdere targets (zoals personen, organisaties, plaatsen, voorwerpen, communicatiemiddelen…) worden geviseerd.

Niettegenstaande een kleine inhaalbeweging wordt vastgesteld, blijft de VSSE het leeuwendeel van de ingezette methoden voor zijn rekening te nemen (86%). Beide diensten kregen weliswaar dezelfde bevoegdheden, maar hun opdrachten zijn dermate verschillend (bijv. de grote 'buitenlandopdracht' van de ADIV) dat uit een vergelijking van de twee diensten wat dit betreft, weinig lering kan worden getrokken. Bijkomende reden voor deze verschillen door de diensten aangehaald, is bijvoorbeeld het gegeven dat de door het gemeenschappelijk contraterrorisme-platform (Platform CT) uitgevoerde BIM's inzake de dreiging 'terrorisme' voor rekening worden genomen van de VSSE.

Als deze cijfers worden uitgesplitst, kan worden vastgesteld dat bij de ADIV de vorig jaar ingezette stijging van specifieke methoden (van 146 naar 166) blijft voortduren. Het aantal ingezette uitzonderlijke methoden stijgt sterk (een toename van 51 in 2020 naar 87 in 2021).[178] Naar luid van de ADIV zijn de redenen hiertoe de interne herstructuring van de BIM-cel, wat een vlottere dienstverlening[179] impliceert en de aanwerving van bijkomende *case-managers*, met bijgevolg meer '*request for operations*'. Inhoudelijk had de zaak-Jurgen Conings (cf. *supra*) en de uitlopers van dit dossier (extreemrechts in het leger) een grote impact. Maar zelfs zonder de zaak-Conings, kon een aanzienlijke toename worden opgetekend van het aantal ingezette BIM's, aldus de ADIV.

De VSSE daarentegen laat het tegenovergestelde optekenen. Er wordt zowel een opmerkelijke daling vastgesteld van het aantal ingezette specifieke methoden (van 1629 in 2020 naar 1220 in 2021) als een daling van het aantal ingezette uitzonderlijke methoden (van 511 in 2020 naar 350 in 2021 of een daling van meer dan 30%). Daartoe zijn, aldus de VSSE, meerdere redenen: het aantal zgn. 'gewone methoden plus' nam toe (communicerende vaten); bij de dienst vond een grote rekrutering plaats met een arbeidsintensieve opleiding waardoor bijgevolg tijdelijk minder personeel bij de buitendiensten beschikbaar was voor onderzoeken; de voortdurende gevolgen van de COVID-maatregelen…

II.1.1.2. De inzet van gewone methoden plus, in het bijzonder artikel 16/2 W.I&V

De identificatie van de abonnee of de gewoonlijke gebruiker van telecommunicatiedienst of -middel (bijv. gsm-nummer of IP-adres[180]) wordt als een gewone methode beschouwd in de mate waarin dit gebeurt via een vordering aan telecomope-

178 Belangrijk in dit kader is dat de ADIV eveneens bijzondere bevoegdheden heeft tot het inwinnen van gegevens zoals geregeld in de artikelen 44 ev. W.I&V. Zie hieromtrent: 'Hoofdstuk III. Het toezicht op buitenlandse intercepties, beeldopnamen en IT-intrusies' (*infra*).

179 Toch blijft de procedure tot indienen van BIM's bij de ADIV merkelijk (administratief) omslachtiger dan bij de VSSE, wat volgens de ADIV aanleiding zou geven tot een vorm van 'zelfcensuur'.

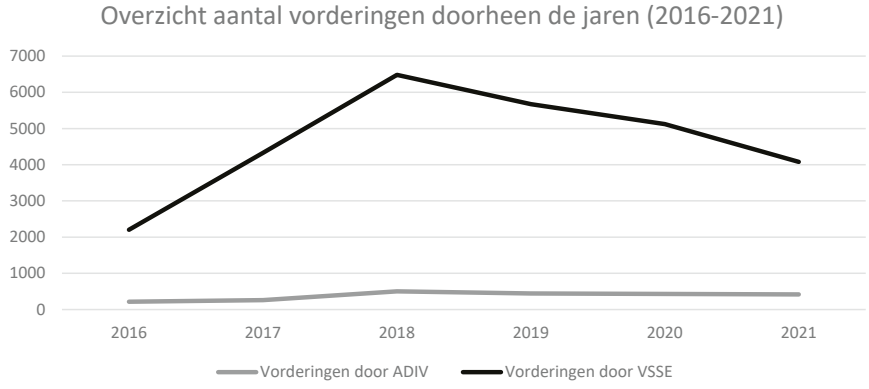
180 Vanaf 2022 wordt ook het aantal vorderingen opgesplitst in 'vorderingen IP' en 'vorderingen non-IP'.

ratoren of -providers of via een rechtstreekse toegang tot hun klantenbestanden.[181] De regeling voorziet in een verplichting voor de inlichtingendiensten om een register bij te houden van alle gevorderde identificaties en van alle via rechtstreekse toegang verkregen identificaties.[182] Er werd ook bepaald dat het Comité maandelijks een lijst van de gevorderde identificaties en van elke toegang moet ontvangen.

Wat betreft deze methode, blijft de ingezette daling van het aantal vorderingen voortduren (een tiental vorderingen minder bij de ADIV in vergelijking met 2020, tegenover meer dan 1000 vorderingen minder bij de VSSE).[183]

	Vorderingen door ADIV	Vorderingen door VSSE
2016	216	2203
2017	257	4327
2018	502	6482
2019	442	5674
2020	433	5123
2021	420	4080

In een grafiek weergegeven geeft dit volgend beeld:



181 Wanneer de identificatie met behulp van een technisch middel verloopt (en dus niet via de vordering aan een operator) blijft de collecte een specifieke methode (art. 18/7 § 1 W.I&V).

182 De in artikel 16/2, §1, laatste lid W.I&V gecreëerde mogelijkheid voor de inlichtingendiensten om dergelijke identificatiegegevens op te vragen via een rechtstreekse toegang tot de klantenbestanden van de telecomoperatoren en -providers kende tot op heden geen uitwerking.

183 Vanuit zijn algemene toezichtsbevoegdheid onderzocht het Comité de redenen hiertoe; de resultaten werden opgenomen in het in 2019 geopende *'toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten die recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld*' (cf. I.14.1. De toepassing van nieuwe (bijzondere) inlichtingenmethoden').

Een aantal belangrijke kanttekeningen zijn hier op zijn plaats. Uit bovenstaande tabel kan inderdaad worden afgeleid dat na de implementatie van de wetsaanpassingen in 2016 en 2017, het aantal vorderingen een piek kende in 2018. Niettegenstaande het aantal vorderingen een indicatie vormt voor de werklast, kan hieruit niets worden afgeleid wat betreft de toe- of afname van het aantal selectoren (telefoonnummers, namen, IP-adressen…). Daar waar bij bijv. de militaire inlichtingendienst een daling van het aantal vorderingen dient te worden vastgesteld (van 433 in 2020 naar 420 in 2021), steeg het aantal selectoren opmerkelijk: van 5334 in 2020 naar 6385 in 2021 (of een stijging van bijna 20%). Bij de VSSE bleef ondanks de daling van het aantal vorderingen, het aantal selectoren vrij stabiel (31.730[184] in 2021 tegenover 31.204 in 2020).

Verder wordt door beide diensten in de telling geen onderscheid gemaakt tussen artikel 16/2 §1 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (W.I&V) en artikel 16/2 §2 W.I&V[185] (identificatie van een pre-paid kaarthouder).

II.1.1.3. Gevolgen van de vernietiging van de Dataretentiewet?[186]

Met zijn arrest van 22 april 2021 vernietigde het Grondwettelijk Hof de zogenaamde Dataretentiewet.[187] Het Hof oordeelde dat de algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie het recht schendt op eerbiediging van het privéleven en op bescherming van persoonsgegevens. Dit arrest betekent een obstakel voor onder meer inlichtingenonderzoeken.

Het hoeft geen betoog dat identificatie-, verkeers- en locatiegegevens een belangrijke rol speelt in het inlichtingenwerk. Onder meer hiervoor werd destijds in art. 126 Wet electronische communicatie (WEC)[188] de dataretentieplicht in het leven geroepen. Aanbieders van openbare telefoniediensten en operatoren van openbare elektronische communicatienetwerken werden hierdoor verplicht om deze gegevens gedurende twaalf maanden bij te houden.[189]

---

184 Bij de VSSE bedroeg het aantal identificaties van IP-adressen 4925, terwijl het 'aantal identificaties anders dan IP' 26.805 bedroeg (in 2020 waas dat respectievelijk 3188 en 28.016).

185 Artikel 16/2 W.I&V vermeldt: '§ 2. *De inlichtingen- en veiligheidsdiensten kunnen, in het belang van de uitoefening van hun opdrachten, de medewerking vorderen van een bank of financiële instelling om over te gaan tot het identificeren van de eindgebruiker van de in artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie bedoelde voorafbetaalde kaart, op basis van de referentie van een elektronische banktransactie die verband houdt met de voorafbetaalde kaart en die voorafgaand meegedeeld is door een operator of verstrekker in toepassing van paragraaf 1.*'

186 Zie hierover 'Hoofdstuk VI.3. Advies over dataretentie'.

187 Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie, *BS* 18 juli 2016. Persbericht Grondwettelijk Hof, "*Het Grondwettelijk Hof vernietigt de verplichting tot algemene en ongedifferentieerde bewaring van gegevens met betrekking tot elektronische communicatie*", 22 april 2021.

188 Wet van 13 juni 2005 betreffende de elektronische communicatie, *BS* 20 mei 2005, 28070.

189 De dataretentieplicht is niet alleen van toepassing op telefoonverkeer, maar ook op verscheidene soorten internetverkeer.

Concreet oordeelde het Grondwettelijk Hof dat het bewaren van gegevens voortaan de uitzondering moet worden; de gerichte bewaring van gegevens dient steeds evenredig te zijn met het nagestreefde doel.

Gevraagd naar de implicaties op de werking van beide inlichtingendiensten in 2021, lieten zowel de ADIV als de VSSE optekenen dat deze eerder verwaarloosbaar zijn en er vooralsnog geen ingrijpende gevolgen te noteren vielen.

Ondertussen heeft de regering een wetsontwerp neergelegd[190] dat er voornamelijk op gericht is weer een juridisch kader in te stellen dat voldoet aan de rechtspraak inzake bewaring van de 'metagegevens' of 'verkeers- en locatiegegevens' door operatoren. De regering uitte de wens dat deze reparatiewet voor de zomer van 2022 in voege zou treden. Het nieuwe voorstel zou in het voorjaar 2022 aan de Ministerraad worden voorgelegd.[191]

II.1.2. METHODEN AANGEWEND DOOR DE ADIV

II.1.2.1. Gewone methoden 'plus'

De identificatie van de abonnee of de gewoonlijke gebruiker van telecommunicatiedienst of -middel

De ingezette daling van het aantal vorderingen blijft voortduren (een tiental vorderingen minder bij de ADIV in vergelijking met 2020) (*supra*).

Toegang tot PNR-gegevens

Naast de identificatie van de abonnee of de gewoonlijke gebruiker van telecommunicatie als gewone methoden 'plus' (*supra*), werd begin 2017[192] de mogelijkheid ingebouwd voor de inlichtingendiensten om toegang te krijgen tot informatie die berust bij de Passagiersinformatie-eenheid (BELPIU) en dit bij wijze van gerichte opzoekingen (art. 16/3 W.I&V en art. 27 van de Wet van 25 december 2016 betreffende de verwerking van passagiersgegevens (PNR-Wet).[193] Het Comité wordt

190 Wetsontwerp van 17 maart 2022 betreffende het verzamelen en het bewaren van de identificatiegegevens en van metagegevens in de sector van de elektronische communicatie en de verstrekking ervan aan de autoriteiten. *Parl. St.* Kamer 2021-22, 55K2575/001.

191 Vraag van E. GILISSEN aan de minister van Telecommunicatie over 'de wet op de bewaring van gegevens' (*Hand.* Kamer 2021-22, 9 maart 2022, CRIV55COM715, 11).

192 Wet van 25 december 2016 (*BS* 25 januari 2017).

193 De BIM-cel van de ADIV heeft in deze geen functie; alles verloopt via de bij BELPIU gedetacheerde ADIV-medewerker.

in kennis gesteld van de aanwending van deze methode en kan ze desgevallend verbieden.[194]

De PNR-regeling laat ook toe een zgn. 'voorafgaande beoordeling' te doen waarbij ingevoerde PNR-gegevens automatisch afgetoetst worden aan namenlijsten of bestanden van de inlichtingendiensten en waarbij informatie op basis van gevalideerde hits wordt doorgezonden (art. 24 PNR-Wet). Het aantal gerichte opzoekingen in PNR-gegevens bleef in 2021 stabiel (28 in 2020, 29 in 2021). Voor meer dan de helft betrof dit dossiers gelieerd aan de dreiging 'spionage'.

Gebruik van politionele camerabeelden

Bij Wet van 21 maart 2018 (*BS* 16 april 2018) werd de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten aangepast om de inlichtingendiensten toe te laten gebruik te maken van politionele camerabeelden. Daartoe werd er een nieuwe gewone methode ingevoerd (art. 16/4, §2 W.I&V).[195] [196] Er werd door de ADIV in 2021 (voor het eerst) vijftien maal van deze methode gebruik gemaakt. Drie van de vijftien aanvragen betroffen aanvragen voor een periode van minder dan één maand.

De cijfers

Gewone methoden plus (ADIV)	Aantal toelatingen 2020	Aantal toelatingen 2021
Identificatie van de 'abonnee of de gewoonlijke gebruiker' van telecommunicatie	433	420
Gerichte opzoekingen PNR-gegevens	28	29
Gebruik van politionele camerabeelden[197]	Niet in werking	15

194 Anders dan voor de methoden opgenomen in artikel 16/2 W.I&V werd niet voorzien in een verplichte verslaggeving aan het Parlement; artikel 35 § 2 W.Toezicht werd immers niet aangepast. Op suggestie van de Begeleidingscommissie besliste het Comité om deze cijfers mee op te nemen in zijn jaarlijkse verslaggeving en niet te wachten op een eventuele wetswijziging. Pas in 2020 werden de eerste twee stopzettingen bevolen.

195 Bij dezelfde wet werd de bestaande specifieke en uitzonderlijke observatiemogelijkheid uitgebreid (artt. 18/4 § 3 en 18/11 § 3 W.I&V).

196 Begin 2019 keurde de Ministerraad een ontwerp van koninklijk besluit goed ter uitvoering van artikel 16/4 W.I&V. Het werd aan het advies van het Vast Comité I voorgelegd. Dit advies 002/VCI-BTA/2019 van 9 april 2019 is te consulteren op de website van het Comité (www.comiteri.be).

197 Het toepassingsgebied van artikel 16/4 W.I&V (bijv. met betrekking tot de bevragingen van de Directie van de politionele informatie en de ICT-middelen (DRI) van de Federale politie) maakt het voorwerp uit van een juridische analyse (2021).

II.1.2.2. De specifieke methoden

Onderstaande tabel geeft de cijfers weer over de toepassing van de specifieke methoden door de ADIV. Er worden daarbij zeven specifieke methoden onderscheiden.

Specifieke methoden (ADIV)	Aantal toelatingen 2020	Aantal toelatingen 2021
Observeren in publiek toegankelijke plaatsen met een technisch middel of al dan niet met behulp van een technisch middel observeren in een niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is (art. 18/4 W.I&V)[198]	6	12
Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (art. 18/5 W.I&V)	0	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	0	0
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	2	0
Identificatie met behulp van een technisch middel, van de elektronische communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt (art. 18/7 §1, 1° W.I&V)	2	6
Vordering van de operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst tot het bekomen van de gegevens betreffende de betalingswijze, de identificatie van het betalingsmiddel en het tijdstip van betaling voor het abonnement of voor het gebruik van de elektronische communicatiedienst (art. 18/7 §1, 2° W.I&V)	0	0
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8, §1, 1° W.I&V)	69	75
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator (art. 18/8, §1, 2° W.I&V)	67	73
TOTAAL	**146**	**166**

198 Bij Wet van 21 maart 2018 (*BS* 16 april 2018) werd een nieuwe paragraaf toegevoegd aan art. 18/4 W.I&V om de inlichtingendiensten toe te laten gebruik te maken van politionele camerabeelden om *real time*-observaties uit te voeren. Deze methode, die een rechtstreekse toegang vereist tot de bedoelde informatie, werd nog niet geoperationaliseerd.

Wat betreft de inzet van specifieke methoden, spannen het 'opsporen van lokalisatiegegevens van elektronische communicatiemiddelen' (art. 18/8, §1, 1° W.I&V) en het kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer (art. 18/8, §1, 2° W.I&V), beiden met het vorderen van de medewerking van een telecomoperator of -provider, duidelijk de kroon (148 van de 166 ingezette specifieke methoden). Er vonden dubbel zoveel observaties plaats in publiek toegankelijke plaatsen met een technisch middel dan in 2020 (van 6 naar 12 in 2021).

Volgens de ADIV werd een aantal methoden niet ingezet wegens gebrek aan personeel. Daarnaast kwam men bij de ADIV tot de vaststelling dat een aantal specifieke methoden te weinig ingeburgerd zijn bij de medewerkers en bijgevolg te weinig worden ingezet. Om aan dit euvel te verhelpen, werden begin 2022 interne briefings georganiseerd.

II.1.2.3. De uitzonderlijke methoden

De ADIV kan in het kader van zijn opdrachten bedoeld in de artikelen 11, § 1, 1° tot 3° en 5°, en § 2 W.I&V diverse uitzonderlijke methoden machtigen:

Uitzonderlijke methoden (ADIV)	Aantal toelatingen 2020	Aantal toelatingen 2021
Al dan niet met behulp van technische middelen, observeren in niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en betreden van al dan niet aan het zicht onttrokken niet voor het publiek toegankelijke plaatsen om te observeren, een technisch middel te installeren, een voorwerp te openen of mee te nemen (art. 18/11 W.I&V) [199]	2	3
Al dan niet met behulp van technische middelen niet voor het publiek toegankelijke plaatsen doorzoeken, evenals al dan niet vergrendelde voorwerpen die zich daar bevinden (art. 18/12 W.I&V)	0	2
Een rechtspersoon als bedoeld in art. 13/3 § 1 W.I&V inzetten om gegevens te verzamelen (art. 18/13 W.I&V)	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	0	2
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	6	8

[199] Bij Wet van 21 maart 2018 (*BS* 16 april 2018) werd een nieuwe paragraaf toegevoegd aan art. 18/11 W.I&V om de inlichtingendiensten toe te laten gebruik te maken van politionele camerabeelden om real time-observaties uit te voeren. Deze methode, die een rechtstreekse toegang vereist tot de bedoelde informatie, werd nog niet geoperationaliseerd.

Uitzonderlijke methoden (ADIV)	Aantal toelatingen 2020	Aantal toelatingen 2021
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	4	14
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	39	60
TOTAAL	**51**	**89**

Er wordt een sterke stijging van het aantal ingezette uitzonderlijke methoden vastgesteld. De procentueel sterke stijging (bijna verdubbeling) van het aantal door de ADIV ingezette uitzonderlijke methoden, situeert zich voornamelijk in het kader van het binnendringen in een informaticasysteem (art. 18/16 W.I&V) (van 4 in 2020 naar 14 in 2021) en voor wat betreft het afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V) (van 39 in 2020 naar 60 in 2021). Het 'inzetten van een fictieve rechtspersoon om gegevens te verzamelen (art. 18/13 W.I&V)' als uitzonderlijke methode werd door de ADIV sinds de invoegetreding van de Wet van 2010 nog nooit toegepast. Al in 2016 werd dezelfde vaststelling gedaan en toen verklaard door het feit dat "*de procedure voor de oprichting te omslachtig is om die voor een enkel dossier in gang te zetten*".[200]

Het Comité wees de ADIV eerder[201] op de verplichting om de BIM-Commissie tweewekelijks in te lichten over de uitvoering van deze uitzonderlijke methoden (art. 18/10 §1, derde lid W.I&V en art. 9 KB 12 oktober 2010). Daarop werd een tweewekelijks overleg in het leven geroepen. De sanitaire maatregelen opgelegd in het kader van het coronavirus, maakten dat deze vergaderingen niet meer konden plaatsvinden. Ze werden in het voorjaar van 2022 opnieuw opgestart.

II.1.2.4. De opdrachten en de dreigingen die de inzet van (de gewone en) bijzondere methoden rechtvaardigen[202]

De ADIV mag de specifieke en uitzonderlijke methoden aanwenden in het kader van vier opdrachten[203] daarbij rekening houdend met verschillende dreigingen.

---

200 Memorie van toelichting bij het wetsontwerp tot wijziging van de wet van 30 november 1998, *Parl. St.* Kamer, 2015-16, 54K2043/001, 11.

201 VAST COMITÉ I, *Activiteitenverslag 2017*, 109 ('XII.II.3.3. Informatieplicht in het kader van uitzonderlijke methoden').

202 Per toelating kunnen meerdere opdrachten en dreigingen aan de orde zijn.

203 Deze methoden kunnen dus niet ingezet worden in het kader van veiligheidsonderzoeken of andere door of krachtens bijzondere wetten aan de ADIV toevertrouwde opdrachten (bijv. het verrichten van veiligheidsverificaties voor kandidaat-militairen).

1. **De inlichtingenopdracht (art. 11, 1° W.I&V)**
   Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de factoren die de nationale en internationale veiligheid beïnvloeden of kunnen beïnvloeden in die mate dat de Krijgsmacht betrokken is of zou kunnen worden om inlichtingensteun te bieden aan hun lopende of eventuele komende operaties. Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op elke activiteit die volgende belangen bedreigt of zou kunnen bedreigen:
   - de onschendbaarheid van het nationaal grondgebied of het voortbestaan van de gehele of een deel van de bevolking;
   - de militaire defensieplannen;
   - het wetenschappelijk en economisch potentieel op vlak van defensie;
   - de vervulling van de opdrachten van de strijdkrachten;
   - de veiligheid van de Belgische onderdanen in het buitenland.
2. **De zorg voor het behoud van de militaire veiligheid (art. 11, 2° W.I&V)**
   - de militaire veiligheid van het personeel dat onder de minister van Landsverdediging ressorteert;
   - de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen;
   - in het kader van de cyberaanvallen op militaire informatica- en verbindingssystemen of systemen die de minister van Landsverdediging beheert, de aanval neutraliseren en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het recht van de gewapende conflicten.
3. **De bescherming van geheimen (art. 11, 3° W.I&V)**
   Het beschermen van het geheim dat, krachtens de internationale verbintenissen van België of teneinde de onschendbaarheid van het nationaal grondgebied en de vervulling van de opdrachten van de strijdkrachten te verzekeren, verbonden is met de militaire installaties, wapens, munitie, uitrusting, met de plannen, geschriften, documenten of andere militaire voorwerpen, met de militaire inlichtingen en verbindingen, alsook met de militaire informatica- en verbindingssystemen of die systemen die de minister van Landsverdediging beheert.
4. **Het inwinnen, analyseren en verwerken van inlichtingen die betrekking hebben op de activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied (art. 11, 5° W.I&V).**

De inzet van bijzondere methoden is sinds de inwerkingtreding van de Wet van 30 maart 2017 niet meer beperkt tot het Belgische grondgebied (art. 18/1, 2° W.I&V). Door de ADIV werd meegedeeld dat er in 2021 geen BIM's werden

ingezet in het buitenland.[204] Deze bevoegdheid, dewelke nog nooit werd toegepast, werd nochtans in de memorie van toelichting van de Wet van 30 maart 2017 voorgesteld als zijnde een noodzakelijkheid om de ADIV toe te laten zijn buitenlandse opdrachten (in het bijzonder deze in het kader van de operaties met een mandaat van de Veiligheidsraad van de Verenigde Naties) naar behoren uit te kunnen voeren.[205] Nader onderzoek moet uitwijzen of de ADIV daadwerkelijk geen BIM-methoden heeft aangewend in het buitenland – wat dan wel een negatie zou betekenen van de argumentatie in de memorie van toelichting om het territoriale toepassingsgebied van de BIM-methoden te wijzigen – of als de situatie bestaat dat de ADIV wel BIM's in het buitenland aanwendt zonder evenwel gebruik te maken van de verplicht toe te passen BIM-procedure. Het Comité zal in 2022 nagaan of de ADIV (verkeerdelijk?) exclusief gebruik maakt van de INT-regeling beschreven in artikel 44 W.I&V.[206]

Er werden ook geen bijzondere inlichtingenmethoden ingezet op vraag van buitenlandse partnerdiensten.[207] Wel kan, aldus de ADIV, informatie verkregen van buitenlandse diensten de directe aanleiding vormen tot het opstarten van een bijzondere inlichtingenmethode.

De praktijk wijst uit dat per toelating verschillende dreigingen aan de orde kunnen zijn. Er kan een lichte daling worden opgetekend voor wat betreft de inzet van BIM's in het kader van de dreigingen 'spionage' en 'terrorisme'. Opmerkelijk is de sterke stijging van het aantal uitzonderlijke methoden ingezet in het kader van de dreiging 'extremisme' (van 20 in 2020 naar 82 in 2021). Het zal niet verbazen dat deze steile opgang te wijten is aan de zaak-Jurgen Conings[208] en de bijzondere aandacht voor extreemrechts binnen de Krijgsmacht als gevolg hiervan. Voor het eerst komen ook 'criminele organisaties' als dreiging aan de bod (29 ingezette methoden).[209]

---

204 Wel werd beroep gedaan op de mogelijkheden geboden door art. 44 W.I&V (zie hierover Hoofdstuk III. Het toezicht op buitenlandse intercepties, beeldopnamen en IT-intrusies).

205 MvT, *Parl. St.* Kamer 2015-16, 54K2043/001.

206 Dit initiatief schrijft zich in in de filosofie van de memorie van toelichting van de wet van 2017 waarin wordt gesteld dat *"Binnen vijf jaar wordt de situatie opnieuw geëvalueerd om na te gaan of de voorrechten van de ADIV in het buitenland uitvoerbaar zijn en of zij de mandaten van de Verenigde Naties voldoende dekken*".

207 Dit bleek soms wel het geval voor de inzet van 'gewone methoden plus' (maar enkel indien er ook een aanwijsbaar nut is voor de ADIV zelf).

208 Zie 'Hoofdstuk I.9. Het opsporen en opvolgen van de radicalisering van een militair: de zaak-Jürgen Conings'.

209 Hiervoor bleken twee specifieke dossiers voor verantwoordelijk; één met betrekking tot wapenhandel/*organised crime* en een ander tot drugshandel (initieel opgestart in het kader van de opvolging van extreemrechts).

AARD DREIGING	AANTAL 2020	AANTAL 2021
Spionage	139	120
Inmenging	19	16
Extremisme - radicalisme	20	82
Terrorisme	19	9
Criminele organisatie	-	26
Andere	-	0
Totaal	**197**	**253**

Anders dan voor de inzet van bijzondere methoden, beschikt het Comité niet over de cijfers met betrekking tot de geviseerde dreiging en de te verdedigen belangen wat betreft de in dit hoofdstuk bedoelde gewone methoden. In zijn vorig activiteitenverslag beveelde het Comité de diensten aan ook deze gegevens te registreren en ter beschikking te stellen.[210] Dit gebeurde vooralsnog niet; het Comité herhaalt in dat kader dan ook zijn eerder geformuleerde aanbeveling.

II.1.3. METHODEN AANGEWEND DOOR DE VSSE

II.1.3.1. De gewone methoden 'plus'

Gewone methoden plus (VSSE)	Aantal toelatingen 2020	Aantal toelatingen 2021
Identificatie van de 'abonnee of de gewoonlijke gebruiker' van telecommunicatie	5123	4080
Gerichte opzoekingen PNR-gegevens[211]	30	98[212]
Gebruik van politionele camerabeelden	Niet in werking	46

Wat betreft de zogenaamde 'gewone methoden plus' is voor het derde jaar op rij een sterk daling (+/- 1000 aangevraagde identificaties) merkbaar van het aantal 'identificaties van de abonnee of gewoonlijke gebruiker van telecommunicatie'.[213] De inzet van methoden op basis van artt. 16/3 en 16/4 W.I&V kent daarentegen een gestage opgang. Het aantal toelatingen voor gerichte opzoekingen in de passagiers-

210 VAST COMITÉ I, *Activiteitenverslag 2017*, 43.

211 Met *profiling* wordt (nog) niet gewerkt

212 Het jaarrapport van BELPIU stelt dat "*de VSSE heeft […] 133 gerichte opzoekingen gerealiseerd*". Zie: Nationaal Crisiscentrum, *Jaarrapport BELPIU 2021*, 14.

213 In de praktijk wordt eerst het '*commun reference database centre*' (CRDC) geconsulteerd. Deze gegevensbank verstrekt uitsluitend informatie over de operator die het opgevraagde nummer uitbaat zonder vermelding of dit nummer werd toegekend aan een eindgebruiker. Er worden in deze 'gegevensbank voor nummerlocatie toegankelijk voor het publiek' geen persoonlijke gegevens opgeslagen.

gegevens (PNR) (art. 16/3 W.I&V) werd meer dan verdrievoudigd (van 30 naar 98). Het nut van deze methode neemt ook gestaag toe, nu het aantal aangesloten luchtvaartmaatschappijen ook exponentieel is toegenomen.[214] Vanaf 2021 kon ook een beroep worden gedaan op art. 16/4 §2 W.I&V dat de retroactieve opvraging regelt van politionele camerabeelden door de inlichtingendiensten.[215] De procedurele vereisten zijn zowel van toepassing op de gerichte opvragingen van politionele camerabeelden via een rechtstreekse (online) toegang tot de betrokken politionele gegevensbanken (actueel nog niet mogelijk) alsook op de gerichte opvragingen via een schriftelijke bevraging van de bevoegde politiediensten[216] (*in casu* de Directie van de politonele informatie en de ICT-middelen bij de Federale Politie (DRI)). De methode werd 46[217] keer ingezet.

De identificatie van prepaid-kaarthouders als methode wordt niet apart geregistreerd.

II.1.3.2. De specifieke methoden

Specifieke methoden (VSSE)	Aantal toelatingen 2020	Aantal toelatingen 2021
Observeren in publiek toegankelijke plaatsen met een technisch middel of al dan niet met behulp van een technisch middel observeren in een niet voor het publiek toegankelijke plaats die niet aan het zicht onttrokken is (art. 18/4 W.I&V)	245	195
Doorzoeken van publiek toegankelijke plaatsen met een technisch middel, de inhoud van vergrendelde voorwerpen doorzoeken of deze voorwerpen meenemen (art. 18/5 W.I&V)	0	0

214 "*Het aantal verwerkte passagiersgegevens lag in 2021 lager dan in 2019. Er werden daarentegen wel meer gegevens verwerkt dan in 2020 omdat de eenheid de passagiersgegevens van meer luchtvaartmaatschappijen verwerkt. Op dit moment worden de gegevens van* 94% van het internationaal luchtverkeer *verwerkt. Binnen de BelPIU wordt bovendien gerichter gewerkt met de passagiersgegevens en zijn er meer samenwerkingen met andere Europese Passagiers Informatie Eenheden (PIU's)*", in: Nationaal Crisiscentrum, *Jaarrapport BELPIU 2021*, 14.

215 Begin 2022 formuleerde het Vast Comité I in zijn hoedanigheid van Bevoegde Toezichthoudende Autoriteit hierover een beslissing: VAST COMITÉ I, DPA-beslissing n° VCI-DPA/2022/2 – Verwerkingsinstructie m.b.t. de door de inlichtingendiensten ingestelde retroactieve opvragingen van politionele camerabeelden gegrond op artikel 16/4, §2 W.I&V.

216 Vanaf de inwerkingtreding van de Camerawet van 21 maart 2018 moet artikel 16/4, §2 W.I&V gehanteerd worden als rechtsgrond voor het schriftelijk opvragen van politionele camerabeelden en kunnen de inlichtingendiensten hiervoor niet langer gebruik maken van artikel 14, tweede lid W.I&V. Zie hierover DPA-beslissing n° VCI-DPA/2022/2 (*supra*).

217 In 2021 werd enkel melding gemaakt van methoden dewelke één maand overstegen. In zijn DPA-beslissing n° VCI-DPA/2022/2 benadrukte het Comité dat '*schriftelijke DRI-bevragingen slechts kunnen plaatsvinden met respect van beide vernoemde procedurele vereisten (schriftelijke bevestiging én kennisgeving), en dit ongeacht of de toegang tot de politionele camerabeelden plaatsvindt tijdens of na de eerste bewaarmaand*'.

Specifieke methoden (VSSE)	Aantal toelatingen 2020	Aantal toelatingen 2021
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator (art. 18/6 W.I&V)	1	0
Vervoers- en reisgegevens vorderen van private vervoers- en reisdiensten (art. 18/6/1 W.I&V)	70	33
Identificatie met behulp van een technisch middel, van de elektronische communicatiediensten en -middelen waarop een bepaald persoon is geabonneerd of die door een bepaald persoon gewoonlijk worden gebruikt (art. 18/7 §1, 1° W.I&V)	46	22
Vordering van de operator van een elektronisch communicatienetwerk of van een verstrekker van een elektronische communicatiedienst tot het bekomen van de gegevens betreffende de betalingswijze, de identificatie van het betalingsmiddel en het tijdstip van betaling voor het abonnement of voor het gebruik van de elektronische communicatiedienst (art. 18/7 §1, 2° W.I&V)	0	2
Opsporen van verkeersgegevens van elektronische communicatiemiddelen en het vorderen van de medewerking van een operator (art. 18/8, §1, 1° W.I&V)	650	491
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator (art. 18/8, §1, 2° W.I&V)	617	477
TOTAAL	**1629**	**1220**

Opnieuw nam de inzet van het aantal specifieke methoden duidelijk af (van 1629 naar 1220). Deze daling doet zich voor bij zowat alle specifieke methoden. Naar luid van de VSSE zijn hiervoor naast de supra vermelde algemene redenen (personeelsuitbreiding, coronamaatregelen) een aantal redenen aan te halen. Zo blijkt de inzet van de specifieke methode op basis van art. 18/6/1 W.I&V (het vorderen van vervoers- en reisgegevens) gelinkt aan de PNR-opvraging; gezien de stijging van het aantal gerichte opzoekingen van PNR-gegevens, nam de inzet van deze specifieke methode af (communicerende vaten).[218] Wat het doorzoeken van publiek toegankelijke plaatsen (art. 18/5 W.I&V) en kennisnemen van identificatiegegevens van postverkeer (art. 18/6 W.I&V)[219] betreft, verkiest de VSSE net zoals in 2020 de inzet van een uitzonderlijke methoden om met zekerheid binnen het wettelijk kader te opereren.

218 Voor data van vliegtuigmaatschappijen dewelke (nog) niet zijn opgenomen in BELPIU, gebeuren de aanvragen vooralsnog via art. 18/6/1 W.I&V. Het is de uitdrukkelijke wens van de VSSE om in de toekomst ook de deeleconomie (Uber, deelsteps DOTT) in dit kader te kunnen bevragen.

219 Gezien de ontvangen informatie met betrekking tot het postverkeer, is het meer aangewezen een uitzonderlijke methode aan te vragen.

II.1.3.3. De uitzonderlijke methoden

Uitzonderlijke methoden (VSSE)	Aantal toelatingen 2020	Aantal toelatingen 2021
Al dan niet met behulp van technische middelen, observeren in niet voor het publiek toegankelijke plaatsen die aan het zicht onttrokken zijn en betreden van al dan niet aan het zicht onttrokken niet voor het publiek toegankelijke plaatsen om te observeren, een technisch middel te installeren, een voorwerp te openen of mee te nemen (art. 18/11 W.I&V)	9	13
Al dan niet met behulp van technische middelen niet voor het publiek toegankelijke plaatsen doorzoeken, evenals al dan niet vergrendelde voorwerpen die zich daar bevinden (art. 18/12 W.I&V)	8	11
Een rechtspersoon als bedoeld in art. 13/3 § 1 W.I&V inzetten om gegevens te verzamelen (art. 18/13 W.I&V)	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post (art. 18/14 W.I&V)	11	13
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen (art. 18/15 W.I&V)	186	73
Binnendringen in een informaticasysteem (art. 18/16 W.I&V)	74	61
Afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V)	223	192
TOTAAL	**511**	**363**

Net als de inzet van specifieke methoden, nam ook het aantal door de VSSE ingezette uitzonderlijke methoden af (van 511 in 2020 naar 363 in 2021). Deze sterke daling is bijna volledig te wijten aan een halvering van de inzet van de methoden tot 'verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen' (art. 18/15 W.I&V) (van 186 in 2020 naar 73 in 2021).

De inzet van deze methode (het verwerken financiële gegevens) blijkt bijzonder arbeidsintensief te zijn.[220] Daarnaast valt een zij het lichtere daling van het aantal ingezette methoden inzake het afluisteren, kennisnemen en opnemen van communicaties (art. 18/17 W.I&V) (van 223 in 2020 naar 192 in 2021) op te tekenen. Ook voor de VSSE blijkt het inzetten van een rechtspersoon (art. 18/13 W.I&V) te veel middelen vragen.

II.1.3.4. De opdrachten en de dreigingen die de inzet van (de gewone en) bijzondere methoden rechtvaardigen

De volgende tabel toont in het kader van welke (potentiële) dreigingen de VSSE specifieke en uitzonderlijke methoden toepasten. Uiteraard kan één methode gericht zijn tegen meerdere dreigingen. De VSSE kan de specifieke methoden aanwenden in het kader van alle dreigingen die tot haar bevoegdheid behoren (art. 8 W.I&V).

In acht genomen dat per toelating verschillende dreigingen aan de orde kunnen zijn, kunnen volgende cijfers worden opgetekend:

AARD DREIGING	AANTAL 2020	AANTAL 2021
Spionage	816	478
Inmenging	27	121
Extremisme - radicalisme	296	279
Proliferatie	3	2
Schadelijke sektarische organisaties	0	0
Terrorisme	998	690
Criminele organisaties	0	0
Activiteiten buitenlandse diensten in België opvolgen	(inbegrepen in bovenstaande cijfers)	(inbegrepen in bovenstaande cijfers)
TOTAAL	**2140**	**1570**

Bovenstaande tabel toont aan dat wat betreft de inzet van BIM-methoden in 2021 de dreiging 'terrorisme' weliswaar afneemt (van 998 naar 690), maar toch de absolute prioriteit blijft voor de VSSE en dit gevolgd door spionage. Waar in 2020

[220] Het voorontwerp van wet tot wijziging van de Inlichtingenwet, waarover het Comité in 2021 een advies formuleerde, stelt in dit kader voor een nieuwe gewone methode in te voeren Deze creëert een medewerkingsverplichting voor financiële instellingen in de meeste ruime zin van het woord om over te gaan tot de identificatie van financiële producten of diensten waarover een persoon beschikt of, omgekeerd, om te identificeren welke persoon kan gelinkt worden aan bepaalde financiële producten of diensten. In de memorie van toelichting wordt deze keuze verantwoord door te stellen dat '*de intrusiviteit van een dergelijke methode […] gering tot zeer gering is*'. Het Comité is het hier niet mee eens. In zijn advies beveelt het Comité aan deze methode te kwalificeren als een specifieke methode (Advies nr. 001/VCI/2021 van 12 juli 2021 – Wijzigingen Inlichtingenwet).

nog sprake was van een sterke afname van het aantal 'inmengingsdossiers', kan opnieuw een sterke stijging worden vastgesteld (van 27 in 2020 naar 121 in 2021). Het is in de praktijk evenwel niet altijd evident om een duidelijk onderscheid te maken tussen spionage (het clandestien gegevens ophalen) en inmenging (beïnvloeden van beslissingsprocessen). De dreiging 'extremisme-radicalisme' bleef stabiel (279 dossiers). Gezien schadelijke sektarische alsook criminele organisaties sinds 2015 niet meer het voorwerp uitmaken van actieve opvolging[221], hoeft het niet te verbazen dat deze dreigingen niet voorkomen in de cijfergegevens.

Op vlak van territorialiteit, is de VSSE bevoegd om BIM's in te zetten 'op en vanaf Belgisch grondgebied' (art. 18/1, 1 W.I&V). Net zoals bij de ADIV, werden door de VSSE geen bijzondere inlichtingenmethoden ingezet in het buitenland. Ook de inzet van dergelijke methoden in België op vraag van buitenlandse partnerdiensten, is verwaarloosbaar. Wel werd op basis van informatie ontvangen van partnerdiensten beslist om bijzondere inlichtingenmethoden toe te passen.

De bevoegdheid van de VSSE wordt niet alleen bepaald door de aard van de dreiging. De dienst mag slechts optreden ter vrijwaring van welbepaalde belangen:

1. De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde zijnde,
   a) de veiligheid van de instellingen van de Staat en het vrijwaren van de continuïteit van de regelmatige werking van de rechtsstaat, de democratische instellingen, de elementaire beginselen die eigen zijn aan iedere rechtsstaat, alsook de mensenrechten en de fundamentele vrijheden;
   b) de veiligheid en de fysieke en morele vrijwaring van personen en de veiligheid en de vrijwaring van goederen
2. De uitwendige veiligheid van de Staat en de internationale betrekkingen: het vrijwaren van de onschendbaarheid van het nationaal grondgebied, van de soevereiniteit en de onafhankelijkheid van de Staat, van de belangen van de landen waarmee België gemeenschappelijke doeleinden nastreeft, alsook van de internationale en andere betrekkingen die België met vreemde Staten en internationale of supranationale instellingen onderhoudt;
3. De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

Net als bij de ADIV, worden door de VSSE verschillende belangen gecombineerd. Wel kan worden vermeld dat de 'vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel' weinig voorkwam.

Zoals gezegd, beschikt het Comité niet over de cijfers met betrekking tot de geviseerde dreiging en de te verdedigen belangen wat betreft de in dit hoofdstuk bedoelde gewone methoden.

---

221 Zie hierover 'I.5. De opvolging van schadelijke sektarische organisaties en criminele organisaties' (*supra*).

II.2. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS (JURISDICTIONEEL) CONTROLEORGAAN EN ALS PREJUDICIEEL ADVIESVERLENER

II.2.1. CONTROLE OP BEPAALDE GEWONE METHODEN

II.2.1.1. Algemeen

De controle op bepaalde gewone methoden is voor elk van die methoden anders geregeld.

Wat betreft de identificatie van de gebruiker van telecommunicatie (en daarmee verbonden, de identificatie van de gebruiker van een prepaid-kaart), voerde de wet geen specifieke controle in. In artikel 16/2 §4 W.I&V werd alleen bepaald dat het Comité maandelijks in het bezit wordt gesteld van de lijst van de gevorderde identificaties en van de rechtstreekse toegang. Zoals hoger gesteld, ontvangt het Comité in dit kader alleen het aantal vorderingen. Het Comité nam zich echter voor om jaarlijks steekproefsgewijs een aantal vorderingen te controleren.[222]

Wat betreft de toegang tot PNR-gegevens die berusten bij de Passagiersinformatie-eenheid, bepaalt artikel 16/3 W.I&V dat die toegang alleen kan na beslissing van het diensthoofd en '*mits afdoende motivering*'. Het Comité moet hiervan in kennis worden gesteld en '*verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen*'. In 2021 werd door het Comité vier dergelijke verboden uitgesproken. Zowel drie beslissingen van de VSSE als een beslissing van de ADIV voldeden niet afdoende aan de wettelijk opgelegde motiveringsplicht. Beide diensten werd verboden de in het kader van deze dossiers verzamelde informatie te exploiteren.

Ten slotte werden aan het Comité bijzondere controlemodaliteiten toegekend in het kader van de mogelijkheid voor de inlichtingendiensten om toegang te

222 VAST COMITÉ I, *Activiteitenverslag 2017*, 25 voetnoot 40. Hiermee werd een aanvang genomen in 2020. Het Comité besliste deze thematiek mee op te nemen in zijn in 2019 geopende *'toezichtonderzoek naar de toepassing en de interne controle door de inlichtingendiensten naar de methoden en instrumenten die recent door de wetgever zijn ingevoerd of aangepast en waarbij het Vast Comité I een bijzondere toezichtsrol werd toebedeeld.'*

krijgen tot informatie afkomstig van politionele camerabeelden (artikel 16/4 W.I&V): een *a priori*-controle[223] en een *a posteriori*-controle.[224]

II.2.2. CONTROLE OP BIJZONDERE METHODEN

II.2.2.1. De cijfers

In dit onderdeel wordt ingegaan op de activiteiten van het Vast Comité I met betrekking tot de specifieke en uitzonderlijke inlichtingenmethoden. Daarbij wordt uitsluitend aandacht besteed aan de ter zake genomen jurisdictionele beslissingen en niet aan de operationele gegevens. Vooraf dient evenwel te worden onderlijnd dat het Comité *alle* toelatingen tot de inzet van bijzondere methoden aan een *prima facie*-onderzoek onderwerpt, en dit met het oog op de al dan niet vatting. Tot vóór de coronamaatregelen, woonde een commissaris-auditor van de Dienst Enquêtes de (tweewekelijkse) vergaderingen bij waarop de betrokken inlichtingendienst de BIM-Commissie inlicht over de uitvoering van de uitzonderlijke methoden. Omwille van de voor de hand liggende redenen werden deze vergaderingen opgeschort. Zoals eerder vermeldt, wordt dit initiatief opnieuw opgenomen in het voorjaar van 2022.

Artikel 43/4 W.I&V stelt dat het Vast Comité I op vijf manieren kan worden gevat:

1. Op eigen initiatief;
2. Op verzoek van de Gegevensbeschermingsautoriteit (GBA);
3. Op klacht van een burger;
4. Van rechtswege als de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden;
5. Van rechtswege als de bevoegde minister een toelating heeft verleend op basis van artikel 18/10 § 3 W.I&V.

---

223 '*De beoordelingscriteria bedoeld in het eerste lid, 2°, worden voorafgaandelijk aan het Vast Comité I voorgeleg*d.'

224 *'De beslissing van het diensthoofd of zijn gedelegeerde wordt met de motivering van deze beslissing zo spoedig mogelijk aan het Vast Comité I betekend. De beslissing kan betrekking hebben op een geheel van gegevens die betrekking hebben op een specifiek inlichtingenonderzoek. In dit geval wordt een lijst van de gerichte toegangen eenmaal per maand aan het Vast Comité I doorgegeven. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.*' en '*Elke lijst aan de hand waarvan de correlatie bedoeld in het eerste lid, 1°, wordt uitgevoerd, wordt zo spoedig mogelijk doorgegeven aan het Vast Comité I. Het Vast Comité I verbiedt de inlichtingen- en veiligheidsdiensten om gebruik te maken van de gegevens die verzameld werden in omstandigheden die niet aan de wettelijke voorwaarden voldoen.*'

Daarnaast kan het Comité ook gevat worden in zijn hoedanigheid van 'prejudicieel adviesverlener' (art. 131*bis*, 189*quater* en 279*bis* Sv.). In dat geval geeft het Comité een advies over de al dan niet rechtmatigheid de specifieke of uitzonderlijke methoden die inlichtingen hebben opgeleverd die in een strafzaak worden gebruikt. De beslissing om een advies te vragen berust bij de onderzoeksgerechten of de strafrechters. Strikt genomen treedt het Comité alsdan niet op als jurisdictioneel orgaan.

WIJZE VAN VATTING	2013	2014	2015	2016	2017	2018	2019	2020	2021
1. Op eigen initiatief	16	12	16	3	1	1	4	2	1
2. Gegevensbeschermingsautoriteit	0	0	0	0	0	0	0	0	0
3. Klacht	0	0	0	1	0	0	0	0	0
4. Exploitatieverbod door BIM-Commissie[225]	5	5	11	19	15	10	12	9	8
5. Toelating minister	2	1	0	0	0	0	0	0	0
6. Prejudicieel adviesverlener	0	0	0	0	0	0	0	0	0
TOTAAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**	**9**

Het aantal door het Comité genomen beslissingen blijft dalen (van 11 in 2020 naar 9 in 2021). Bovendien zijn – één uitzondering niet te na gesproken – alle vattingen het gevolg van een schorsing door de BIM-Commissie. Het Comité werd in deze nog nooit gevat door de Gegevensbeschermingsautoriteit noch door een klacht.

Eens gevat, kan het Comité verschillende soorten (tussen)beslissingen nemen.

1. Nietigheid van de klacht wegens vormgebrek of afwezigheid van een persoonlijk en rechtmatig belang (art. 43/4, eerste lid, W.I&V);
2. Beslissing om geen gevolg te geven aan een klacht die kennelijk niet gegrond is (art. 43/4, eerste lid, W.I&V);
3. Schorsing van de betwiste methode in afwachting van een definitieve beslissing (art. 43/4, laatste lid, W.I&V);

[225] Ze vloeien voort uit opnameproblemen of bij de verwijdering van apparatuur.

4. Vordering tot bijkomende informatie ten aanzien van de BIM-Commissie (43/5 § 1, eerste tot derde lid, W.I&V);
5. Vordering tot bijkomende informatie ten aanzien van de betrokken inlichtingendienst (43/5 § 1, derde lid, W.I&V);
6. Onderzoeksopdracht voor de Dienst Enquêtes I (art. 43/5 § 2 W.I&V). In deze rubriek wordt zowel verwezen naar de veelvuldige bijkomende informatie die door de Dienst Enquêtes I op eerder informele wijze wordt ingewonnen vóór de eigenlijke vatting als naar informatie die op verzoek van het Comité wordt ingewonnen na de vatting;
7. Horen van de BIM-Commissieleden (art. 43/5 § 4, eerste lid, W.I&V);
8. Horen van het diensthoofd of de leden van de betrokken inlichtingendienst (art. 43/5 § 4, eerste lid, W.I&V);
9. Beslissing over geheimen die betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek waarvan de leden van de inlichtingendiensten drager zijn, na overleg met de bevoegde magistraat (art. 43/5 § 4, tweede lid, W.I&V);
10. Uitspraak door de voorzitter van het Vast Comité I, na het diensthoofd te hebben gehoord, indien het lid van de inlichtingendienst meent het geheim waarvan hij drager is te moeten bewaren omdat de onthulling ervan nadelig is voor de bescherming van de bronnen, de bescherming van de persoonlijke levenssfeer van derden of de vervulling van de opdrachten van de inlichtingendienst (art. 43/5 § 4, derde lid, W.I&V);
11. Stopzetting van een methode indien ze nog steeds in uitvoering is of indien zij werd geschorst door de BIM-Commissie en bevel dat de gegevens die met deze methode werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd (art. 43/6 § 1, eerste lid, W.I&V);
12. Gedeeltelijke stopzetting van een toegelaten methode. Hier wordt de situatie bedoeld waarbij bijvoorbeeld één methode in tijd wordt beperkt, niet de situatie waarbij in één toelating van een diensthoofd meerdere methoden worden gemachtigd en het Comité slechts één ervan stopzet;
13. Gehele of gedeeltelijke opheffing van de schorsing en het verbod die door de BIM-Commissie was uitgesproken (art. 43/6 § 1, eerste lid, W.I&V). Dit houdt in dat de door het diensthoofd toegelaten methode door het Comité wel (gedeeltelijk) wettelijk, proportioneel en subsidiair werd bevonden;
14. Onbevoegdheid van het Vast Comité I;
15. Ongegrondheid van de aanhangige zaak en geen stopzetting van de methode;
16. Advies als prejudicieel adviesverlener (artt. 131*bis*, 189*quater* en 279*bis* Sv.).

AARD VAN DE BESLISSING	2014	2015	2016	2017	2018	2019	2020	2021
Beslissingen voorafgaand aan de vatting								
1. Nietige klacht	0	0	0	0	0	0	0	0
2. Kennelijk ongegronde klacht	0	0	0	0	0	0	0	0
Tussenbeslissingen								
3. Schorsing methode	3	2	1	0	0	0	1	0
4. Bijkomende informatie van BIM-Commissie	0	0	0	0	0	0	0	0
5. Bijkomende informatie van inlichtingendienst	1	1	4	0	0	0	1	1
6. Onderzoeksopdracht Dienst Enquêtes[226]	54	48	60	35	52	52	24	33
7. Horen BIM-Commissieleden	0	2	0	0	0	0	0	0
8. Horen leden inlichtingendiensten	0	2	0	0	0	1	1	0
9. Beslissing m.b.t. geheim van onderzoek	0	0	0	0	0	0	0	0
10. Gevoelige informatie tijdens verhoor	0	0	0	0	0	0	0	0

[226] Het Comité verzoekt de Dienst Enquêtes I om een bijkomende onderzoeksopdracht uit te voeren en/of mondeling de betrokken inlichtingendienst of de BIM-Commissie te contacteren.

AARD VAN DE BESLISSING	2014	2015	2016	2017	2018	2019	2020	2021
Eindbeslissingen								
11. Stopzetting methode	3	3	6	9	4	11	10	5
12. Gedeeltelijke stopzetting methode	10	13	4	6	6	4	0	3
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	0	4	11	0	0	0	0	0
14. Onbevoegd	0	0	0	0	0	0	0	0
15. Wettige toelating / Geen stopzetting methode / Ongegrond	4	6	2	1	1	0	0	1
Prejudicieel advies								
16. Prejudicieel advies	0	0	0	0	0	0		0

II.2.2.2. De rechtspraak

Hieronder wordt de essentie weergegeven van de eindbeslissingen die het Vast Comité I in 2021 nam binnen zijn jurisdictionele controle op de aanwending van de bijzondere inlichtingenmethoden.[227] De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk worden opgenomen.
De beslissingen werden gegroepeerd onder volgende rubrieken:
– De wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode;
– De wettigheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van de dreiging;
– De wettigheid van de uitvoering van een wettige methode.

[227] In sommige dossiers werd het Comité gevat in 2020, maar werd een eindbeslissing genomen in 2021.

De wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode

SUBSIDIARITEIT, PROPORTIONALITEIT EN DREIGINGSORIËNTATIE

Krachtens artikel 18/3, §1, eerste lid W.I&V kan een specifieke methode slechts door een inlichtingendienst worden aangewend ingeval er een tot de bevoegdheid van de betrokken dienst behorende potentiële dreiging voor de fundamentele belangen van het land aanwezig is. Daarnaast kan een dergelijke BIM-methode slechts worden ingezet indien de gewone methoden voor het verzamelen van gegevens ontoereikend worden geacht om de informatie te verzamelen die nodig is om de inlichtingenopdracht te volbrengen (de subsidiariteitseis). Tot slot eist vernoemde wetsbepaling dat een specifieke methode moet worden gekozen in functie van de graad van ernst van de potentiële dreiging waarvoor ze wordt aangewend (de proportionaliteitseis).

In dossier 2021/10548 wenste een inlichtingendienst de verkeers- en lokalisatiegegevens te bekomen die verliepen via een welbepaald telefoonnummer.[228] De inzet ervan kaderde binnen een door de inlichtingendienst gestarte operatie om na te gaan of een bepaalde ambtenaar betrokken was, bewust dan wel onbewust, bij spionageactiviteiten van een vreemde mogendheid. De medewerker was immers gedurende vele jaren in het betrokken land tewerkgesteld en aantal specifieke gedragingen van deze medewerker deden bij de inlichtingendienst de vraag rijzen of er door een inlichtingendienst van deze vreemde mogendheid ten aanzien van betrokkene gebruik werd gemaakt van de zogenaamde '*honey trap*'. Hierbij trachten buitenlandse inlichtingendiensten door middel van manipulatieve, amoureuze en seksuele avances informatie te bekomen van een persoon. Het profiel van deze medewerker sloot, *dixit* betrokken Belgische inlichtingendienst, aan bij het profiel dat door buitenlandse inlichtingendiensten als interessant beschouwd wordt voor de inzet van een dergelijke werkwijze. Via het vorderen van de verkeers- en lokalisatiegegevens wou de Belgische inlichtingendienst de sociale en professionele contacten van de betrokken medewerker in kaart brengen. Vervolgens kon dan nagegaan worden of deze contacten geoorloofd waren in het kader van de uitoefening van zijn functie, dan wel of het ging om onofficiële, ongepaste en/of niet-geoorloofde contacten waarvan een eventuele dreiging uitging.

De BIM-Commissie besloot de uitvoering van deze specifieke methode te schorsen. Ze was van oordeel dat de door de inlichtingendienst aangehaalde argumenten en feitelijke gegevens niet aantoonden dat er ernstige en op feiten beruste gronden bestonden om aan te nemen dat er tegen betrokkene aanwijzingen bestonden dat hij zich zou inlaten met clandestiene inlichtingenactiviteiten voor een buitenlandse inlichtingendienst. De Commissie stelde dat de door de inlichtingendienst ingeroepen gedragingen onvoldoende waren om hieruit te kunnen

[228] *Cf.* artikel 18/8, §1, eerste lid, 1° en 2° W.I&V.

concluderen dat deze mogelijks het voorwerp was geweest van een *Honey Trap*. Tevens was de Commissie van oordeel dat de inlichtingendienst onvoldoende omstandig motiveerde dat de gevraagde methode in verhouding stonden met de ernst van de dreiging (proportionaliteit) en dat het door de methoden na te streven doel, in acht genomen de stand van het inlichtingenonderzoek, niet op minder ingrijpende wijze kon worden bereikt (subsidiariteit). Wat dit laatste aspect betreft, was de Commissie van oordeel dat nog heel wat informatie kon bekomen worden via gewone methoden (bv. een persoonlijkheidsonderzoek van target).

Krachtens artikel 43/4 W.I&V is het Vast Comité I van rechtswege gevat telkens wanneer de Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden. In tegenstelling tot de Commissie was het Comité echter van oordeel dat de door de inlichtingendienst ingeroepen gedragingen wél afdoende waren om het bestaan van een potentiële dreiging aan te tonen, althans in combinatie met de specifieke functie van betrokkene, de gevoelige positie die hiermee gepaard ging alsook het specifieke (privé-)profiel van betrokkene. Ook oordeelde het Comité dat de vereisten inzake subsidiariteit en proportionaliteit door de inlichtingendienst waren gerespecteerd.

BIJZONDERE TOELATINGSPROCEDURE BIJ BESCHERMDE BEROEPSCATEGORIEËN

In zijn *Activiteitenverslag 2020* deelde het Vast Comité I mee dat het in dat jaar voor het eerst sinds de inwerkingtreding van de BIM-Wet van 4 februari 2010, een prejudiciële vraag gesteld had aan het Grondwettelijk Hof aangaande de BIM-wetgeving (dossier 2020/9606).[229] De aanleiding was een beslissing van een inlichtingendienst om de in artikel 18/8, §1, 1° en 2° W.I&V bedoelde specifieke methoden aan te wenden tegen een door een arts gebruikte telefoonnummer. Via een gewone methode bleek het geviseerde telefoonnummer enkel op naam van betrokkene in België te zijn geregistreerd. Hoewel de inlichtingendienst wist dat het om een arts ging, volgde ze de gewone toelatingsprocedure voor specifieke methoden.[230] De BIM-Commissie was het hiermee niet eens en schorste de lopende methoden. Gelet op de hoedanigheid van de geviseerde persoon, zijnde arts, moest volgens de Commissie gebruik gemaakt worden van de bijzondere toelatingsprocedure voor beschermde beroepscategorieën voorzien in artikel 18/3, §5 W.I&V: *'(d)e specifieke methoden kunnen slechts worden aangewend ten opzichte van een advocaat, een arts of een journalist, of van communicatiemiddelen die ze voor beroepsdoeleinden gebruiken, op voorwaarde dat de inlichtingen- en veiligheidsdienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief*

229 VAST COMITÉ I, *Activiteitenverslag 2020*, 94-97.

230 Meteen nadat de inlichtingendienst zijn fout had ingezien, werd een nieuwe aanvraag ingediend, rekening houdende met het gegeven van de beschermde beroepscategorie.

meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële dreiging en nadat de commissie, overeenkomstig artikel 18/10 een eensluidend advies uitgebracht heeft op het ontwerp van beslissing van het diensthoofd'. Deze bijzondere procedure komt er dus op neer dat wanneer een inlichtingendienst een specifieke methode wenst aan te wenden jegens artsen, advocaten of journalisten de toelatingsprocedure voor uitzonderlijke methoden dient gevolgd te worden. Op deze wijze wordt elke methode vóór zijn aanwending onderworpen aan een voorafgaande controle van de BIM-Commissie. Naast de schorsing van de betrokken methode, legde de BIM-Commissie een exploitatieverbod op voor de, desgevallend, reeds verkregen gegevens.

Het schorsingsbevel van de BIM-Commissie zorgde voor de ambtshalve vatting van het Vast Comité I. Gelet op het belang van het bijzondere beschermingsregime van vernoemde beroepscategorieën en vanuit zijn hoedanigheid van rechtsprekend orgaan[231] binnen het toezicht op de specifieke en uitzonderlijke methoden, besloot het Comité om volgende prejudiciële vraag te stellen aan het Grondwettelijk Hof: *'Schendt artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten de artikelen 10 en 11 van de Grondwet, alleen gelezen of in samenhang met artikel 22 van de Grondwet en/of al dan niet gecombineerd met artikel 8 van het Europees Verdrag tot Bescherming van de Rechten van de Mens en de Fundamentele Vrijheden, ondertekend te Rome op 4 november 1950 en goedgekeurd bij wet van 13 mei 1955, in zoverre het een advocaat, arts of journalist geen bijzondere bescherming biedt bij communicatiemiddelen die hij voor andere dan beroepsdoeleinden gebruikt?'*.[232] Het Comité merkte immers op dat artikel 18/2, §3, eerste en tweede lid W.I&V de aan advocaten, artsen en journalisten verleende bescherming beperkt tot de communicatiemiddelen die zij voor beroepsdoeleinden gebruiken. Uit de huidige tekst van vernoemde bepaling volgt dat communicatiemiddelen die zij voor andere dan beroepsdoeleinden gebruiken niet onder de wettelijke bescherming (lijkt te) vallen.

In april 2021 deed het Grondwettelijk Hof uitspraak: *'Onder voorbehoud van de in B.15.2 vermelde interpretatie schendt artikel 18/2, § 3, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten niet de artikelen 10, 11 en 22 van de Grondwet, in samenhang gelezen met artikel 8 van het Europees Verdrag voor de rechten van de mens'*.[233] Overweging B.15.2 stelt: *'Gelet op de bijzondere bescherming die voor alle medische gegevens moet gelden, met name krachtens de rechtspraak van het Europees Hof voor de Rechten van de Mens en het Belgische strafrecht, moet artikel 18/2, § 3, van de wet van 30 november 1998 in die zin worden geïnterpreteerd dat het de inlichtingen- en veiligheidsdiensten verplicht om de door de wetgever geboden bescherming voor de communicatiemiddelen die voor beroepsdoeleinden worden gebruikt, toe te passen wanneer het niet vaststaat*

231 GwH 22 september 2011, nr. 145/2011, overw. B.38.1.
232 Vrije vertaling.
233 GwH 22 april 2021, nr. 64/2021.

dat het door een arts gebruikte communicatiemiddel uitsluitend werd aangewend om andere doeleinden dan beroepsdoeleinden.'.

Volgend op het arrest van het Grondwettelijk Hof neemt het Vast Comité I een eindbeslissing in voorliggend BIM-dossier: *'Gelet op de hoedanigheid van [persoon X] als arts en indachtig het arrest n° 64/2021 van 22 april 2021 van het Grondwettelijk Hof, is de [betrokken inlichtingendienst] in voorliggend dossier verplicht om aan te tonen dat betrokken communicatiemiddel door [persoon X] uitsluitend wordt aangewend om andere doeleinden dan beroepsdoeleinden, opdat [betrokken inlichtingendienst] op rechtmatige wijze de gewone procedure voor specifieke methoden mag aanwenden. Het Comité stelt vast dat de motivering van de [betrokken inlichtingendienst] in de bestreden beslissing zich beperkt tot de mededeling dat « de selector XXX de enige bleek te zijn die in België op zijn naam geregistreerd stond ». Deze vaststelling is niet afdoende om aan te tonen dat betrokken communicatiemiddel door [persoon X] uitsluitend wordt aangewend om andere doeleinden dan beroepsdoeleinden. Ten gevolge hiervan heeft de [betrokken inlichtingendienst] op onregelmatige wijze gebruik gemaakt van de gewone procedure voor specifieke methoden.'.*[234]

NIET-TIJDIGE NOTIFICATIE AAN DE BIM-COMMISSIE

Een inlichtingendienst wenste over te gaan tot de verlenging van een specifieke methode, meer bepaald een observatie met technische hulpmiddelen van een voor het publiek toegankelijke plaats (dossier 2021/10346). Krachtens artikel 18/3, §4 W.I&V kan een verlenging (of hernieuwing)[235] van een specifieke methode slechts plaatsvinden na een nieuwe beslissing van het diensthoofd én na een kennisgeving hiervan aan de BIM-Commissie. De toegelaten uitvoeringsperiode van de eerste specifieke methode liep af de 25e van de maand om 24h. De beslissing van het diensthoofd tot verlenging van de observatie, hoewel genomen op de 25e van de maand, werd echter pas op de 26e van de maand om 9h45 aan de BIM-Commissie genotificeerd. Het Comité instrueerde, in navolging van het door de BIM-Commissie uitgesproken exploitatieverbod, dat de gegevens verkregen gedurende de niet gedekte periode niet mochten worden geëxploiteerd en moesten worden vernietigd.

234 Vrije vertaling.

235 Hoewel artikel 18/3, §4 W.I&V geen onderscheid maakt tussen een 'verlenging' van een specifieke methode en een 'hernieuwing' wat betreft de na te leven formele voorwaarden (*i.c.* beslissing van het diensthoofd én notificatie aan de BIM-Commissie) dient een inlichtingendienst in het beheer van betrokken methode een grotere aandacht aan de dag te leggen bij een verlenging. Zo niet bestaat het gevaar dat er periodes zijn waarin een lopende specifieke methode niet gedekt wordt door een genotificeerde beslissing waardoor er op onrechtmatige wijze gegevens ingewonnen worden. Zie ook: VAST COMITÉ I, *Activiteitenverslag 2020*, 98.

GEEN MONDELING EENSLUIDEND ADVIES VAN DE VOORZITTER VAN DE BIM-COMMISSIE

Krachtens artikel 18/10, §4, eerste lid W.I&V kan, in geval van hoogdringendheid, een uitzonderlijke methode door het diensthoofd van een inlichtingendienst mondeling gemachtigd worden doch slechts na een mondeling eensluidend advies van de voorzitter van de BIM-Commissie. In dossier 2021/10612 werd door een inlichtingendienst, per vergissing en binnen een context van hoogdringendheid, een afluistering (*ex* art. 18/17, §§ 1 en 3 W.I&V) zonder eensluidend advies van de voorzitter van de Commissie opgestart. De betrokken inlichtingendienst stelde deze vergissing zelf vast, waarschuwde daaropvolgend onmiddellijk de BIM-Commissie en zette de onrechtmatig verkregen gegevens reeds in quarantaine. Zoals wettelijk voorzien, verbood de Commissie de exploitatie van de betrokken gegevens en verwittigde ze het Vast Comité I, waarop deze het bevel gaf om de onrechtmatig verkregen gegevens te vernietigen.

De wettigheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van de dreiging

VERKEERD VOORWERP VAN DE METHODE

In dossier 2020/10180 bleek de inlichtingendienst in zijn toelating per vergissing een telefoonnummer te hebben vermeld dat niet geviseerd werd door de betrokken specifieke methode (*i.c.* het opvragen van de verkeers- en lokalisatiegegevens inzake elektronische communicatie bedoeld in artikel 18/8, §1, eerste lid, 1° en 2° W.I&V). Ook in de daaropvolgende vordering aan de telecomoperator werd dit verkeerd oproepnummer vermeld. De dienst merkte dit zelf op, evenwel nadat de gevorderde gegevens reeds van de telecomoperator werden verkregen. De inlichtingendienst plaatste eigenmachtig de verkregen gegevens in elektronische quarantaine en bracht de BIM-Commissie van de vergissing op de hoogte. De Commissie verbood de exploitatie van de onrechtmatig verkregen gegevens, verwittigde het Vast Comité I, waarop laatstgenoemde het bevel gaf om de onwettelijk bekomen gegevens te vernietigen.

DUUR VAN DE METHODE

Krachtens artikel 18/10, §2 W.I&V moet het ontwerp van machtiging aangaande de aanwending van een uitzonderlijke methode op straffe van onwettigheid de periode vermelden waarin de methode kan worden aangewend. De wettelijke toelatingsprocedure voor uitzonderlijke methoden vereist vervolgens een eensluidend advies van de BIM-Commissie. Voorafgaand aan dit advies gaat de Commissie de

wettigheid, de subsidiariteit en de proportionaliteit na. Eén van de door de Commissie te controleren aspecten vormt de voorgestelde uitvoeringsperiode.

In dossier 2021/10428 had een inlichtingendienst een verlenging aangevraagd voor een afluistering zoals bedoeld in artikel 18/17, §§ 1 en 2 W.I&V. In het ontwerp van machtiging werden evenwel twee verschillende uitvoeringsperioden vooropgesteld (nl. één maand vs. twee maanden). De Commissie leverde een eensluidend advies op dit ontwerp van machtiging en verleende haar akkoord voor een uitvoeringsperiode van twee maanden. Van belang is dat de Commissie in zijn eensluidend advies evenwel niet nader ingaat op het feit dat het ontwerp van machtiging twee verschillende uitvoeringsperiodes vermeldde. Het was bijgevolg niet duidelijk of een doelbewuste keuze werd gemaakt tussen de twee door de betrokken dienst voorgestelde periodes. Het Vast Comité I vatte zich in dit dossier ambtshalve. Het stelde *'dat de vermelding van deze verschillende data (1 maand, respectievelijk 2 maanden) in het ontwerp van machtiging waarschijnlijk op een materiële vergissing berust.'*. Aangezien echter het Comité van oordeel was *'dat, zelfs bij een materiële vergissing, met het oog op het streven naar duidelijkheid en rechtszekerheid, een uitzonderlijke methode enkel kan worden toegestaan voor de kortste periode vermeld in het ontwerp van machtiging.'*. Het Comité besloot dat de uitzonderlijke methode wettig was voor een periode van één maand vanaf de machtiging van het diensthoofd.

De wettigheid van de uitvoering van een wettige methode

VERKEERDE ONTVANGEN GEGEVENS

In drie afzonderlijke dossiers (2021/10533, 2021/10550 en 2021/10982) had de betrokken inlichtingendienst op wettige wijze beslist tot het opsporen van elektronische communicatie[236] en tot het lokaliseren van de oorsprong of de bestemming van elektronische communicatie.[237] Maar er stelde zich een probleem bij de overmaking van de gevorderde gegevens in de zin dat de door de dienst NTSU-CTIF[238] overgemaakte gegevens geen betrekking hadden op de gevorderde gegevens. *In casu* werd telkenmale door een foutieve manipulatie bij de dienst NTSU-CTIF in plaats van een lokalisatie een afluistering[239] opgestart. Het betrof dus een onwettigheid buiten de wil van de inlichtingendienst om. In alle drie de gevallen werd dit door de betrokken inlichtingendienst zelf vastgesteld. De BIM-Commissie en de dienst NTSU-CTIF werd telkenmale na de vaststelling onmiddellijk in kennis

236 *Cf.* artikel 18/8, §1, eerste lid, 1° W.I&V (specifieke methode).
237 *Cf.* artikel 18/8, §1, eerste lid, 2° W.I&V (specifieke methode).
238 De dienst NTSU-CTIF (*National Technical & Tactical Support Unit – Central Technical Interception Facility*) is de Centrale Technische Interceptiefaciliteit van de geïntegreerde politie. Zie : Koninklijk besluit van 9 januari 2003 houdende modaliteiten voor de wettelijke medewerkingsplicht bij gerechtelijke vorderingen met betrekking tot elektronische communicatie.
239 *Cf.* artikel 18/17 W.I&V (uitzonderlijke methode).

gesteld. In alle drie de gevallen besliste de betrokken inlichtingendienst ook uit eigen beweging om de onregelmatig verkregen gegevens ontoegankelijk te maken. De BIM-Commissie sprak telkenmale een exploitatieverbod uit, gevolgd door een vernietigingsbevel van het Vast Comité I.

II.3. ALGEMENE VASTSTELLINGEN

Het Vast Comité I formuleert volgende algemene vaststellingen:

- Tussen 1 januari en 31 december 2021 werden door de twee inlichtingendiensten samen 1823 toelatingen verleend tot het aanwenden van bijzondere inlichtingenmethoden: 1570 door de VSSE (waarvan 1220 specifieke en 350 uitzonderlijke) en 253 door de ADIV (waarvan 166 specifieke en 87 uitzonderlijke). Na een constante stijging van het totale aantal ingezette BIM's de afgelopen jaren en een stagnatie in 2019-2020, dient een significante daling te worden opgetekend.
- De VSSE blijft het leeuwendeel van de ingezette methoden voor zijn rekening nemen (86 %). Afgelopen jaar kon een lichte inhaalbeweging door de ADIV worden vastgesteld.
- Als de globale cijfers worden uitgesplitst, dient voor 2021 een aanzienlijke stijging (ca. 30%) bij de ADIV worden opgetekend van de inzet van zowel specifieke (van 146 naar 166) als uitzonderlijke methoden (van 51 in 2020 naar 87 in 2021). De VSSE laat een opmerkelijke daling optekenen (circa 28%) van het aantal ingezette specifieke (van 1629 naar 1220 in 2021) alsook uitzonderlijke methoden (van 511 naar 350) ten overstaan van 2020.
- Wat betreft de gewone methoden van vorderingen gericht aan operatoren om bepaalde communicatiemiddelen te identificeren betreft, wordt opnieuw – en dit voor zowel de ADIV als de VSSE – een daling opgetekend. Desalniettemin steeg het aantal selectoren bij de ADIV met bijna 20%. Voor de Veiligheid van de Staat bleef het aantal selectoren eerder stabiel.
- Er werd door beide inlichtingendiensten voor het eerst de gewone methode plus 'gebruik van politionele camerabeelden' ingezet. Het aantal gerichte opzoekingen van PNR-gegevens nam voor beide diensten gestaag toe.
- Er konden nog voorlopig geen gevolgen van de door het Grondwettelijk Hof vernietigde Dataretentiewet worden vastgesteld.
- Verder kan voor de VSSE worden genoteerd dat het aantal ingezette BIM's voor wat betreft de dreigingen 'terrorisme' en 'spionage' in belangrijkheid afnamen, maar nog steeds de belangrijkste dreigingen vormen. Er werd opnieuw een stijging vastgesteld van het aantal inmengingsdossiers; de dreiging 'extremisme-radicalisme' bleef stabiel.
- Bij de ADIV was een opmerkelijke stijging zichtbaar bij de inzet van BIM-methoden voor de dreiging 'extremisme-radicalisme', te wijten aan het dossier

Jurgen Conings en de bijzondere aandacht voor extreemrechts binnen de Krijgsmacht als gevolg hiervan. De dreiging 'spionage' was evenwel het meeste aan de orde.

- De ADIV heeft (nog) geen BIM's in het buitenland ingezet. Een meer diepgaand onderzoek moet toelaten vast te stellen of de militaire inlichtingendienst effectief nog geen BIM's heeft ingezet in het buitenland dan wel of er (verkeerdelijk) beroep wordt gedaan op de mogelijkheden geboden in artikel 44 W.I&V. Een dergelijk onderzoek schrijft zich in in de filosofie van de memorie van toelichting van de Wet van 30 maart 2017 dat stelt dat *"binnen vijf jaar wordt de situatie opnieuw geëvalueerd om na te gaan of de voorrechten van de ADIV in het buitenland uitvoerbaar zijn en of zij de mandaten van de Verenigde Naties voldoende dekken"*.
- Het Comité werd gevat in negen dossiers, waarvan één vatting op eigen initiatief en acht van rechtswege nadat de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid had geschorst (art. 43/4 W.I&V). Onwettigheden betroffen onder meer problemen met de duur en het voorwerp van de methoden, verkeerde ontvangen gegevens of nog, de niet-tijdige verwittiging van de BIM-Commissie.
- Het Vast Comité I heeft in 2020 voor het eerst sinds de inwerkingtreding van de BIM-wet een prejudiciële vraag gesteld aan het Grondwettelijk Hof aangaande de BIM-wetgeving. In april 2021 deed het Hof hierover uitspraak.

De keuze van de BIM-wetgever in 2010 om in de Inlichtingenwet een logische structuur in te stellen voor wat betreft de (onderzoeks)bevoegdheden van de inlichtingendiensten (o.m. een onderscheid in uitzonderlijke, specifieke en gewone methoden naargelang de graad van privacy inmenging) werd door de wetswijzigingen van de laatste jaren grotendeels verlaten. De recente voorstellen tot wijziging van de Inlichtingenwet[240] brengen op dat vlak weinig verbetering. Het Comité betreurt dat de regelgeving hierdoor als maar complexer en meer onsamenhangend wordt. Een wetgevend initiatief, waartoe het Vast Comité I steeds bereid kan worden gevonden om hieraan zijn bijdrage te leveren, dringt zich op. Dit kan, voor zowel de burger als de inlichtingendiensten, een grotere rechtszekerheid bieden.

[240] Hierover 'Hoofdstuk VI.4. Advies betreffende het voorontwerp van wet tot wijziging van de Inlichtingenwet'.

HOOFDSTUK III.

HET TOEZICHT OP BUITENLANDSE INTERCEPTIES, BEELDOPNAMEN EN IT-INTRUSIES

III.1. DE BEVOEGDHEDEN VAN DE ADIV EN DE CONTROLETAAK VAN HET VAST COMITE I[241]

Al in 2017 werd de bevoegdheid van de Algemene Dienst Inlichting en Veiligheid (ADIV) in het kader van de veiligheidsintercepties uitgebreid.[242] De intercepties konden sindsdien voor communicaties '*uitgezonden of ontvangen in het buitenland*'. Deze mogelijkheid geldt voor *quasi* alle opdrachten van de ADIV. Daarbij is het niet onbelangrijk te vermelden dat de opdrachtomschrijvingen zelf, ook werden verruimd. Tegelijkertijd voerde de wetgever twee andere methoden in, te weten de 'intrusie in een informaticasysteem' (art. 44/1 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (W.I&V)) en de 'opname van bewegende beelden' (art. 44/2 W.I&V). En ook de wijze waarop het Comité deze methoden kan controleren, werd gewijzigd.

De controle *voorafgaand* aan de intercepties, intrusies of beeldopnames gebeurt op basis van jaarlijks opgestelde lijsten.[243] Dit betekent dat er naast een jaarlijks interceptieplan, ook een intrusie- en beeldplan dient te worden opgesteld door de ADIV.[244] De ADIV moet die lijsten in de maand december voor toelating aan de minister van Defensie zenden. Deze heeft tien werkdagen om zijn beslissing mee te

241 Zie artt. 44 t.e.m. 44/5 W.I&V.

242 Over de opeenvolgende wetswijzigingen inzake de interceptiebevoegdheid van de ADIV, zie VAST COMITÉ I, *Activiteitenverslag 2018*, 61 e.v.

243 Dit impliceert niet dat het Vast Comité I de bevoegdheid heeft om de door de minister goedgekeurde lijst al dan niet goed te keuren.

244 In deze plannen stelt de ADIV een lijst op van '*organisaties of instellingen die het voorwerp zullen uitmaken van interceptie van hun communicaties, intrusies in hun informaticasystemen of opnames van vaste of bewegende beelden tijdens het komende jaar. Deze lijsten verantwoorden voor iedere organisatie of instelling de reden waarom zij het voorwerp is van een interceptie, intrusie of opname van vaste of bewegende beelden in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°, en vermelden de voorziene duur*' (art. 44/3 W.I&V).

delen aan de ADIV[245] die op zijn beurt de lijsten, voorzien van de toelating van de minister, overzendt aan het Vast Comité I.[246]

Het toezicht *tijdens* de interceptie, intrusie of opname gebeurt '*op elk ogenblik door middel van bezoeken aan de installaties waar de Algemene Dienst Inlichting en Veiligheid deze intercepties, intrusies en opnames van vaste of bewegende beelden uitvoert*'.

Het toezicht *na* de uitvoering van de methode gebeurt '*aan de hand van maandelijkse lijsten van landen of van organisaties of instellingen die effectief het onderwerp hebben uitgemaakt van een afluistering, intrusie of opname van beelden gedurende de voorafgaande maand*' en die '*de reden verantwoorden waarom de interceptie, intrusie of opname van beelden werd uitgevoerd in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°*'. Deze lijsten moeten ter kennis van het Vast Comité I worden gebracht. De *ex post*-controle gebeurt ook aan de hand van '*het nazicht van logboeken die permanent op de plaats van de interceptie, de intrusie of de opname van vaste of bewegende beelden door de Algemene Dienst Inlichting en Veiligheid worden bijgehouden*'. Deze logboeken moeten steeds toegankelijk zijn voor het Vast Comité I.

Wat kan het Vast Comité I nu ondernemen indien het een onregelmatigheid vaststelt? Artikel 44/4 W.I&V bepaalt dat het Comité, '*[o]ngeacht de andere bevoegdheden aan dit Comité toegekend op basis van de wet van 18 juli 1991, het recht [heeft] de aan de gang zijnde intercepties, intrusies of beeldopnames te doen stopzetten wanneer blijkt dat ze de wettelijke bepalingen of de [ministeriële] toelating niet respecteren. Het beveelt dat de gegevens die onwettig werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd, volgens de door de Koning te bepalen nadere regels*.' Ondanks de dringende aanbeveling van het Comité[247], werd evenwel nog steeds geen dergelijk interceptie-KB getroffen.[248] Het Comité beveelt dan ook opnieuw aan om dit zo spoedig mogelijk te doen.

---

245 Indien de minister geen beslissing heeft genomen of deze niet heeft meegedeeld aan de ADIV vóór 1 januari, mogen de voorziene intercepties, intrusies en opnames aanvangen, onverminderd iedere latere beslissing van de minister.

246 Voor intercepties, intrusies of opnames die niet opgenomen zijn in de jaarlijkse lijsten, maar die *'onontbeerlijk en dringend blijken te zijn'*, wordt de minister zo spoedig mogelijk en uiterlijk op de eerste werkdag die volgt op de aanvang van de methode ingelicht. Indien de minister niet akkoord gaat, kan hij deze methode laten stopzetten. Deze beslissing wordt door de ADIV zo spoedig mogelijk meegedeeld aan het Vast Comité I.

247 VAST COMITÉ I, *Activiteitenverslag 2018*, 129.

248 Het Comité moet zijn beslissing alleszins omstandig motiveren en meedelen aan de minister en aan de ADIV.

III.2. HET IN 2021 VERRICHTE TOEZICHT

III.2.1. HET TOEZICHT VOORAFGAAND AAN DE INTERCEPTIE, INTRUSIE OF OPNAME

Het Vast Comité I ontving alle plannen aangaande intercepties, intrusies en beeldopnamen midden januari 2021.

Voorafgaand aan het toezenden van deze documenten, organiseerde de ADIV een werkvergadering hierover met het Comité. Tijdens deze vergadering werden er door het Comité een aantal opmerkingen geformuleerd aangaande de na te leven wettelijke vereisten. Bij de ontvangst van de plannen op het Comité kon worden vastgesteld dat, conform zijn aanbevelingen, de drie plannen (het interceptie-, beeldopname- en intrusieplan) werden gebundeld in één document. Op deze wijze trachtte de ADIV op korte termijn het geheel van plannen dat de dienst realiseert in uitvoering van artikel 44 W.I&V, te uniformiseren. Het Comité kon vaststellen dat, met inbegrip van de geformuleerde opmerkingen waarmee rekening werd gehouden, de plannen voldeden aan alle wettelijke vereisten.

III.2.2. HET TOEZICHT TIJDENS DE INTERCEPTIE, INTRUSIE OF OPNAME

In de loop van 2021 heeft het Comité de installaties van waaruit de intercepties gebeuren, bezocht. Tijdens het bezoek werd, onder meer, nagegaan of het logboek in overeenstemming was met de desbetreffende wetten en richtlijnen. Het Vast Comité I diende kleine gebreken vast te stellen, dewelke meteen werden rechtgezet door de verantwoordelijke ter plaatse.

Het Comité realiseerde tevens, en voor het eerst, een controle op de site van de dienst van ADIV belast met de uitvoering van het intrusieplan. Bij deze gelegenheid kon het Comité vaststellen dat de dienst geleidelijk aan zijn volledige operationele capaciteit bereikt. Ook hier werd aan de toepasselijke wettelijke vereisten herinnerd (en meer bepaald aan de verplichting tot het bijhouden van een *logbook*) en werd de dienst verzocht deze na te leven. Dit element zal zeker de aandacht krijgen van het Comité bij de eerstvolgende bezoeken.

Wat betreft het beeldopnameplan kon het Vast Comité I in 2021 geen controle uitvoeren van de installaties. Deze controle zal prioritair worden uitgevoerd in 2022.

III.2.3. HET TOEZICHT NA DE UITVOERING VAN DE METHODE

Het Comité ontving twaalf '*maandelijkse lijsten van landen of van organisaties of instellingen die effectief het onderwerp hebben uitgemaakt van een afluistering, intrusies of opname van beelden gedurende de voorafgaande maand*' en die '*de reden verantwoorden waarom de interceptie, intrusie of opname van beelden werd uitgevoerd in verband met de opdrachten bedoeld in artikel 11, § 1, 1° tot 3° en 5°*'.

Het Vast Comité I ontving dus het geheel van de lijsten zoals wettelijk voorzien. De vorm en de inhoud van deze lijsten zullen, in samenspraak met de ADIV, het voorwerp uitmaken van een evaluatie in 2022.

HOOFDSTUK IV.

HET VAST COMITÉ I ALS BEVOEGDE TOEZICHTHOUDENDE AUTORITEIT IN HET KADER VAN DE VERWERKING VAN PERSOONSGEGEVENS

IV.1. INLEIDING

De Algemene Verordening Gegevensbescherming 2016/679 (AVG)[249] en de Richtlijn 2016/680 (Richtlijn)[250] regelen de wijze waarop publieke en private actoren dienen te handelen wanneer zij persoonsgegevens verzamelen, opslaan, bewaren en doorgeven. Beide Europese instrumenten gaven aanleiding tot enkele belangrijke wetswijzigingen op nationaal vlak: in december 2017 werd de Gegevensbeschermingsautoriteit (GBA)[251] – de opvolger van de Privacycommissie – opgericht en in juli 2018 werd een nieuwe Gegevensbeschermingswet (GBW) gestemd.[252] Deze wet wijzigde op zijn beurt de Toezichtwet van 18 juli 1991. Het Vast Comité I werd immers als gegevensbeschermingsautoriteit aangeduid voor verwerkingen van persoonsgegevens die kaderen binnen het domein van de 'nationale veiligheid'.

De rol van het Comité in deze staat omschreven in de Wet tot oprichting van de Gegevensbeschermingsautoriteit (GBA-Wet), in de Gegevensbeschermingswet (GBW) en in de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse (W.Toezicht).[253]

---

249 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (AVG), PB L 2 mei 2016.

250 Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en het vrije verkeer van die gegevens en tot intrekking van het Kaderbesluit 2008/977/JBZ van de Raad, PB L 4 mei 2016, afl. 119/89.

251 Wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (GBA-Wet), *BS* 10 januari 2018.

252 Volledige benaming: Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens (GBW), *BS* 5 september 2018.

253 Hierover uitvoerig: VAST COMITÉ I, *Activiteitenverslag 2018*, 75-86.

Artikel 35 §3 W.Toezicht stelt dat het Vast Comité I '*jaarlijks verslag uit[brengt] bij de Kamer van volksvertegenwoordigers omtrent de gegeven adviezen in zijn hoedanigheid van gegevensbeschermingsautoriteit, omtrent de onderzoeken die werden uitgevoerd en de maatregelen die werden genomen in dezelfde hoedanigheid alsook omtrent haar samenwerking met de andere gegevensbeschermingsautoriteiten*'.

In dit hoofdstuk wordt aan die verplichting gevolg gegeven. Achtereenvolgens worden volgende thema's besproken:

- de verificaties die het Comité – alleen of samen met het Controleorgaan voor politionele informatie (COC) of het Vast Comité P – verricht op verzoek van individuele burgers die gebruik wensen te maken van hun recht op onrechtstreekse toegang tot hun 'dossier' bij een van de door het Comité te controleren diensten;
- de juridische adviesverlening van het Comité in het kader van gegevensbescherming;
- de melding in het kader van een mogelijke *data breach*;
- de werkzaamheden in het kader van de evaluatie van de Gegevensbeschermingswet.

IV.2. DE BEHANDELING VAN INDIVIDUELE VERZOEKEN

Het Vast Comité I behandelt eveneens individuele verzoeken met betrekking tot de verwerkingen van persoonsgegevens door de hogervermelde personen en diensten en hun verwerkers (art. 34 W.Toezicht en artt. 79, 113, 145 en 173 GBW). De verzoeker heeft het recht om onjuiste persoonsgegevens die op hem betrekking hebben te laten verbeteren of verwijderen. Hij mag vragen om te laten verifiëren of de toepasselijke regels inzake gegevensbescherming werden nageleefd. Hij mag ook een klacht indienen wegens de eventuele niet-naleving van de regels inzake gegevensbescherming door een verwerkingsverantwoordelijke voor wie het Comité bevoegd is.

Om ontvankelijk te zijn, moet het verzoek geschreven, gedateerd, ondertekend en met redenen omkleed zijn (art 51/2 W.Toezicht).[254] Indien het verzoek kennelijk niet gegrond is, kan het Comité besluiten geen gevolg te geven aan het verzoek. Deze beslissing moet worden gemotiveerd en schriftelijk ter kennis gebracht van de verzoeker.[255]

---

254 Deze bepaling stelt ook dat het verzoek '*de identiteit van de betrokkene [moet] rechtvaardigen*.' Het is niet meteen duidelijk wat hiermee wordt bedoeld. Waarschijnlijk wordt bedoeld dat hij zijn identiteit moet bewijzen. Die verplichting is namelijk opgenomen in de betrokken bepalingen van de Gegevensbeschermingswet (zie artt. 80, 114, 146 en 174 GBW).

255 Deze verificaties gebeuren kosteloos (zie artt. 80, 114, 146 en 174 GBW).

De onderstaande tabel bevat een overzicht van de in 2021 behandelde dossiers (open en/of afgesloten). De kolommen van de tabel verdelen de verzoeken naargelang het Vast Comité I exclusief bevoegd is dan wel samen met andere toezichthoudende autoriteiten (TA).[256]

[256] In de tabel zijn dus niet de hypothesen opgenomen waarin er kon worden samengewerkt met een andere toezichthoudende autoriteiten (bijv. het COC) wanneer de bevoegdheden van elke TA duidelijk zijn onderscheiden.

Tabel 1. Behandeling van individuele verzoeken[257]

2021	Vast Comité I		Vaste Comités I en P	Vaste Comités I en P en het COC	Totaal
1. Dossiers geopend in 2021	14		2	0	16
2. Onontvankelijke verzoeken 2021	3		0	0	3
3. Ontvankelijke verzoeken 2021	8		0	0	8
	t. ADIV	2			
	t. VSSE	6			
	t. VSSE&ADIV	-			
4. Hangende verzoeken in 2021	3		0	0	0
5. Lopende dossiers in 2021	10[258]		1	2[259]	13
6. Afgesloten dossiers in 2021[260]	10[261]		2[262]	1[263]	13
7. Corrigerende maatregelen	3		0	1	4
8. Totaal behandelde verzoeken	20		3	3	26

In 85% van de verzoeken beweren de betrokkenen[264] dat er sprake is van concrete inmenging in hun rechten en vrijheden als gevolg van, of in ieder geval in verband met, een verwerking van gegevens door een verwerkingsverantwoordelijke

257 De eerste regel geeft aan hoeveel dossiers er in 2021 werden geopend. Regels 2 en 3 verdelen de dossiers naargelang de beslissing tot ontvankelijkheid of ontontvankelijkheid. Voor wat betreft de dossiers dewelke alleen door het Vast Comité I worden behandeld, preciseert regel 3 nog de verdeling tussen de betrokken diensten voor wat betreft de ontvankelijke dossiers. Regel 4 betreft dossiers waarbij de ontvankelijkheidsbeslissing nog hangende is. De regels 5 en 6 tonen de vooruitgang in de dssiers aan (nog lopende of reeds afgesloten). Regel 7 ten slotte geeft het aantal dossiers aan waarin door het Comité corrigerende maatregelen werden opgelegd.

258 Waarvan één dossier geopend in 2020.

259 Waarvan twee dossiers geopend in 2020.

260 Volledig afgesloten. Wanneer corrigerende maatregelen werden opgelegd, sluit het Vast Comité I het dossier af wanneer kon worden vastgesteld dat de maatregelen werden uitgevoerd.

261 Waarvan vijf dossiers geopend in 2020.

262 Waarvan één dossier geopend in 2020.

263 Waarvan één dossier geopend in 2020.

264 Op te merken valt dat, in meerdere dossiers, dergelijke gevallen van inmenging niet alleen worden gemeld door de betrokkenen, maar door hen ook worden gestaafd en bewezen (bv. door analysenota's te bezorgen waarover de betrokkenen beschikken in het kader van de procedures waarin deze nota's worden gebruikt door de publieke autoriteiten). In andere gevallen zijn die beweringen vermoedens die min of meer of helemaal niet worden gestaafd.

die onder de bevoegdheid van het Vast Comité I valt. Van een dergelijke inmenging zou bijvoorbeeld sprake zijn in het kader van een procedure van nationaliteitsverklaring waarbij een inlichtingendienst informatie verstrekt aan het Openbaar Ministerie, wanneer de betrokkene beweert dat hij regelmatig door de politie wordt gecontroleerd, wanneer hij vaststelt dat hem de toegang tot een grondgebied is geweigerd, wanneer gegevens van een inlichtingendienst zijn gebruikt in strafrechtelijke procedures, enz.

In 2021 diende het Comité verschillende verzoeken te behandelen die waren ingediend in het kader van de aanvraag tot verkrijging van de nationaliteit of een verblijfstitel. Geconfronteerd met een negatief besluit op basis van door de Veiligheid van de Staat (VSSE), de Algemene Dienst Inlichting en Veiligheid (ADIV) en/of het Coördinatieorgaan voor de dreigingsanalyse (OCAD) verstrekte informatie, wenden verzoekers zich (onder meer) tot het Vast Comité I voor een controle van de verwerking van hun persoonsgegevens.

Een in 2020 ingediend verzoek heeft ook geleid tot de opening van een informatiedossier in 2021. Tijdens de behandeling van het verzoek kon het Vast Comité I immers praktijken vaststellen die niet in overeenstemming waren met de wettelijke voorschriften. Op basis van dat individuele verzoek, heeft het Comité de algemene verwerking van persoonsgegevens door de inlichtingendiensten in een specifieke context aan een onderzoek onderworpen.

De resterende 15% aan verzoeken bestaat uit aanvragen tot indirecte uitoefening van rechten, zonder bijzondere precisering of concrete grief. Doorgaans vraagt de betrokkene zich af of gegevens over hem of haar worden verwerkt en of de verwerking in overeenstemming is met de toepasselijke regelgeving (indirecte toegang).

Die onevenwicht (85-15%) hoeft niet te verbazen, daar het antwoord dat wordt gegeven aan de betrokkene die zijn rechten uitoefent geen informatie bevat over hoe het staat met de (eventuele) verwerking van zijn persoonsgegevens door de diensten waarvoor het Comité bevoegd is. Alleen wanneer de betrokkene het bestaan vermoedt of concreet de gevolgen ondergaat van een dergelijke gegevensverwerking, heeft hij of zij er belang bij zich tot het Vast Comité I te wenden opdat het de nodige verificaties zou verrichten, in de hoop een verbetering van de situatie te verkrijgen.

IV.3. ADVIESVERLENING

Het Comité kan in twee gevallen een advies uitbrengen '*over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin beleidslijnen van de bevoegde ministers worden geformuleerd*': wanneer de wet zijn advies vereist of op verzoek van de Kamer van volksvertegenwoordigers of van de bevoegde minister (artikel 33, lid 8 W. Toezicht). Dergelijk advies heeft specifiek betrek-

king op de problematiek van de gegevensverwerking en moet dus onderscheiden worden van de algemene adviesbevoegdheid die bijvoorbeeld ook betrekking kan hebben op de efficiëntie en de coördinatie (cf. Hoofdstuk VI. Adviezen). Deze algemene adviesbevoegdheid is in die zin ruimer, maar ze is ook enger aangezien ze beperkt is tot de werking van de inlichtingendiensten en het OCAD.

Het Comité heeft in 2021 in totaal drie adviezen verleend in deze hoedanigheid, waarvan twee wat betreft de uitwisseling van geclassificeerde informatie[265] en één aangaande een voorontwerp van wet tot wijziging van de W.OCAD als gezamenlijk bevoegde toezichthoudende autoriteit (met het Vast Comité P)[266]:

- Advies 005/VCI/2021 van 1 december 2021 aangaande een vraag tot advies van de voorzitter van de Nationale Veiligheidsoverheid met betrekking tot het '*Wetsontwerp houdende instemming met de Overeenkomst tussen het Koninkrijk België en het Koninkrijk der Nederlanden inzake de uitwisseling en wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 5 november 2019*';
- Advies 006/VCI/2021 van 1 december 2021 aangaande een vraag tot advies van de voorzitter van de Nationale Veiligheidsoverheid met betrekking tot het '*Wetsontwerp houdende instemming met de Overeenkomst tussen het Koninkrijk België en het Verenigd Koninkrijk en Noord-Ierland inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 1december 2020*'.
- Gezamenlijk advies VCI-VCP 001/2021 van 8 oktober 2021 over '*het voorontwerp van wet tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging*'.

IV.4. DE MELDING VAN EEN MOGELIJKE DATA BREACH

De door het Vast Comité I gecontroleerde diensten moeten een hele reeks gegevens ter beschikking houden of stellen van het Comité.[267] Zo moet de verwerkingsverantwoordelijke binnen de kortste termijn en indien mogelijk binnen de 72 uur nadat hij er kennis van heeft gekregen, melding maken van eender welke inbreuk op de beveiliging die aanleiding kan geven tot een hoog risico voor de rechten en vrijheden van natuurlijke personen (artt. 89, 122, 155 en 180 GBW).

---

265 In 2019 en 2020 werden in die zin al adviezen verleend over de uitwisseling van geclassificeerde informatie met de Republiek Cyprus, Hongarije, de Republiek Finland, het Koninkrijk Spanje, de Franse Republiek en de Italiaanse Republiek.

266 Zie *in extenso* op de website van het Vast Comité I.

267 Niet elke dienst moet alle hier vermelde gegevens bijhouden of ter beschikking stellen. Dit geldt bijvoorbeeld zeker wat betreft de BIM-Commissie die geen informatie moet meedelen aan het Vast Comité I.

In 2021 werd in de pers gewag gemaakt van een *hacking* van het computernetwerk van de FOD Binnenlandse Zaken.[268] Daarop meldde de directeur van Belgische Passagiersinformatie-eenheid (BELPIU) spontaan dat het afgescheiden Passenger Name Record (PNR) IT-systeem niet was gecompromitteerd. Dit bleek uit een door het Centrum voor Cybersecurity België (CCB) uitgevoerde scanning.

IV.5. EVALUATIE VAN DE GEGEVENSBESCHERMINGSWET

Artikel 286 GBW bepaalt dat de Gegevensbeschermingswet in het derde jaar na de inwerkingtreding ervan moet worden onderworpen aan een gezamenlijke evaluatie door de bevoegde ministers. In deze context richtte staatsecretaris Mathieu Michel een schrijven tot het Comité met de vraag zijn medewerking te verlenen aan het door hem opgerichte oriëntatiecomité. Het Vast Comité I bezorgde daarop verschillende documenten met daarin zowel meer algemene als zeer specifieke, technisch-juridische voorstellen ter versterking van de dataprotectie.[269]

[268] H. DECREM en L. BELGHMIDI, www.vrt.be, 26 mei 2021 ("Twee jaar lang 'doelbewuste cyberaanval op overheidsdienst Binnenlandse Zaken: 'Dit is spionage").

[269] Zie hiervoor: VAST COMITÉ I, *Activiteitenverslag 2020*, 119-125 ('V.7. Evaluatie van de gegevensbeschermingswet').

HOOFDSTUK V.

DE CONTROLE VAN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN

In 2016 werd door de ministers van Binnenlandse Zaken en Justitie de gemeenschappelijke gegevensbank '*foreign terrorist fighters*' opgericht. Deze gemeenschappelijke gegevensbank (GGB) werd in 2018 omgevormd: ze heet voortaan gemeenschappelijke gegevensbank '*terrorist fighters*' (GGB TF) en omvat naast de algemene categorie van de *'foreign terrorist fighters'* tevens een categorie van '*homegrown terrorist fighters*'. Daarnaast werd in 2018 ook een aparte gemeenschappelijke gegevensbank opgericht voor '*haatpropagandisten*' (GGB HP). Bij koninklijk besluit van eind 2019 werden nog twee bijkomende categoriën van personen in de GGB TF opgenomen, zijnde de 'potentieel gewelddadige extremisten' (PGE) en 'terrorisme-veroordeelden' (TV).

Artikel 44/11/3*quinquies*/2 WPA vertrouwt het toezicht op de verwerking van de in de GGB vervatte informatie en persoonsgegevens toe aan het Controleorgaan op de politionele informatie (COC) en aan het Vast Comité I (verder 'de toezichthoudende autoriteiten'). Dit resulteerde in een gemeenschappelijk verslag dat begin oktober 2021 werd besproken in de schoot van de parlementaire Begleidingscommissie.[270]

V.1. DE CONTROLEOPDRACHT EN HET VOORWERP VAN CONTROLE

Voor wat betreft 2020/2021 beslisten het Vast Comité I en het COC om de gezamenlijke controle te focussen op, enerzijds, de verificatie van de rechtstreekse toegang toegekend aan de Nationale Veiligheidsoverheid (NVO) en, anderzijds, op de opvolging van bepaalde aanbevelingen die in de rapporten van de afgelopen jaren werden geformuleerd.

---

270 COC en VAST COMITÉ I, *Verslag betreffende de gezamenlijke controle van de gemeenschappelijke gegevensbanken terrorist fighters en haatpropagandisten door het Vast Comité I en het Controleorgaan op de politionele informatie*, 2020, 34 p. (Beperkte verspreiding (K.B. 20 maart 2000). Het verslag werd door de toezichthoudende autoriteiten goedgekeurd op 12 augustus 2021.

Daarnaast werd eveneens de coördinatie van de gegevensverwerking van informatie in de GGB TF en HP aan een grondig onderzoek onderworpen, onder meer met aandacht voor de rol van de *data protection officer* (DPO). Het stijgend aantal diensten dat een toegang heeft tot de GGB TF en HP werd daarbij eveneens in rekening genomen.

Vanuit methodologisch oogpunt werd, met de sanitaire crisis in het achterhoofd en om de diensten voldoende tijd te geven om de aanbevelingen uit het verslag over de in 2019 uitgevoerde controle uit te kunnen voeren, besloten om de nieuwe bevraging pas in het vierde kwartaal van 2020 te laten plaatsvinden. Verschillende diensten werden bevraagd, waaronder de NVO, het OCAD (operationeel beheerder van de gemeenschappelijke gegevensbanken), de Federale Politie (technisch beheerder) en de *data protection officers* (DPO). Het onderzoek werd afgesloten met een vergadering met de waarnemend directeur van OCAD en de DPO van de gemeenschappelijke gegevensbanken.

V.2. ONDERZOEKSVASTSTELLINGEN

V.2.1. HET GEBREK AAN TOEGANG VAN DE NVO

Ten tijde van de controle hebben het COC en het Vast Comité I vastgesteld dat de NVO niet verbonden was met de GGB en daartoe ook niet de minste actie had ondernomen.

Het COC en het Vast Comité I waren van mening dat de NVO blijk gaf van kennelijke en onverantwoorde nonchalance. Haar gebrek aan handelen, dat in strijd was met de toepasselijke regelgeving deed veiligheidsrisico's ontstaan, niet alleen wat betreft de stelselmatige raadpleging van de GGB maar ook wat betreft de gegevensinvoer in de GGB. De Federale Politie verklaarde dat ze geen gegevens invoerde in de GGB in het kader van de veiligheidsverificaties (en evenmin van de veiligheidsmachtigingen). Niets wees erop dat dergelijke invoer op stelselmatige wijze werd verricht door de inlichtingendiensten wat betreft de veiligheidsmachtigingen. Bijgevolg konden mogelijkerwijs diverse interessante of zelfs cruciale inlichtingen ontsnappen aan de aandacht van de diensten.

Anderzijds, rekening gehouden met het feit dat de NVO geen exclusieve bevoegdheid geniet als veiligheidsoverheid, en teneinde garanties te bieden voor de volledigheid van de GGB, bevolen het COC en het Vast Comité I aan de verschillende veiligheidsautoriteiten zoals bedoeld in de artikelen 15, lid 2 en 22*ter*, lid 2 van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheids-adviezen (W.C.&VM) en 9, lid 1,

9° van de Wet van 28 februari 2007[271] aan zich te vergewissen van de effectieve raadpleging van de GGB in de verschillende processen waarvoor ze bevoegd zijn en om hun beslissingen in te voeren in de GGB, hetzij op basis van hun rechtstreekse toegang tot de GGB of door daartoe contact op te nemen met een basisdienst (in het geval waarin ze geen rechtstreekse toegang hebben).

Het COC en het Vast Comité I kondigden aan deze verschillende aspecten te verifiëren in het kader van latere controles.

V.2.2. DE OPVOLGING VAN DE VROEGERE AANBEVELINGEN

V.2.2.1. Aanbevelingen waaraan gevolg werd gegeven

Beschikbaarheid en onafhankelijkheid van de DPO

De controle wees uit dat de DPO van de GGB over de vereiste juridische kennis beschikte om de functie te bekleden. Het geleverde werk schonk voldoening, des te meer daar de omstandigheden (pandemie) niet bevorderlijk waren voor de uitvoering van alle opdrachten. Eerder werd het probleem van de werklast en de beschikbaarheid van de DPO aangekaart.[272] In het kader van de controle kon worden vastgesteld dat deze laatste ondertussen om een '*aanpassing van de werktijd*' had gevraagd. De vraag werd geanalyseerd door de dienst HR van het OCAD. Het COC en het Vast Comité I legden de nadruk op het feit dat de DPO alle mogelijke vrijheid moet genieten nu zijn opdracht delicaat en complex is als gevolg van het grote aantal gebruikers en de techniciteit van de materie. De vaststelling of goedkeuring van de prioriteiten (opgenomen in een opdrachtbrief) door de verwerkingsverantwoordelijken was eveneens een kritische succesfactor. Wat betreft het risico van belangenconflict bleek uit de verrichte controle dat dit risico kon worden geweerd: verschillende adviezen van de DPO van de GGB gaven aan dat hij over de vereiste onafhankelijkheid beschikt.

---

271 Wet van 28 februari 2007 tot vaststelling van het statuut van de militairen en kandidaat-militairen van het actief kader van de Krijgsmacht, ingevoegd door de wet van 31 juli 2013 tot wijziging van voornoemde wet, *B.S.*, 20 september 2013.

272 Hierover: VAST COMITÉ I, *Activiteitenverslag 2019*, 131 (XI.2.4.1. Evaluatie van de belangenconflicten en de tijdsbesteding van de functionaris van de gegevensbescherming').

V.2.2.2. Aanbevelingen waaraan geen gevolg werd gegeven

Melding van de veiligheidsincidenten

Het COC en het Vast Comité I herhaalden, ter attentie van de Federale Politie, hun aanbeveling om hen formeel kennis te geven van veiligheidsincidenten. De verrichte controle bracht een veiligheidsincident aan het licht dat niet onmiddellijk werd gesignaleerd. Deze melding behoort tot de verantwoordelijkheid van de Federale Politie, in haar hoedanigheid van technisch beheerder van de GGB. Bovendien vestigden de toezichthoudende autoriteiten de aandacht van de Federale Politie op het feit dat het begrip '*veiligheidsincident*' niet enkel betrekking heeft op de vertrouwelijkheid, maar ook op de beschikbaarheid en de integriteit van de GGB.

Wat betreft de opvolging van de tweede aanbeveling (passende informatie van de gebruikende diensten wat betreft de rapportering van vastgestelde incidenten), stelden het COC en het Vast Comité I vast dat er in 2020 geen significante vooruitgang werd geboekt. Ook deze aanbeveling werd herhaald.

V.2.2.3. Aanbevelingen waaraan deels gevolg werd gegeven

Uitvoering van IT-ontwikkelingen

Het COC en het Vast Comité I stelden vast dat er gevolg leek te worden gegeven aan hun aanbeveling met betrekking tot de uitvoering van IT-ontwikkelingen om de opvolging te verzekeren van de termijnen voor bewaring van de gegevens in de GGB. De Federale Politie kondigde een opvolging aan in het begin van het tweede semester van 2021. Ze drongen erop aan dat dit aspect, dat sinds het begin van de gezamenlijke controles regelmatig in herinnering werd gebracht, definitief zou worden geregeld binnen de door de Federale Politie aangekondigde termijn. In dit verband kon een latere controle worden uitgevoerd.

Controle van de loggings

Anderzijds stelden het COC en het Vast Comité I vast dat hun aanbeveling wat betreft de controle van loggings werd uitgevoerd. De Federale Politie nam een initiatief dat tot doel had de controle van de loggings door de politiediensten aan te moedigen. Het COC en het Vast Comité I wensten dat de DPO van de GGB erover zou waken – in het kader van zijn opdracht van stimuleren van de informatiebeveiliging – dat dit initiatief werd uitgebreid tot alle (DPO's van de) gebruikers, des te meer daar sommige van hen het niet gewoon zijn om gevoelige informatie te verwerken. Tijdens de controle werd meegedeeld dat de functionaliteit van controle van de loggings werd opgenomen in versie '3.0' van de GGB. Het COC en het Vast

Comité I drongen erop aan dat, bij een volgende controle, alle diensten bij machte zouden zijn aan te tonen dat ze een controle van de loggings hebben uitgevoerd.

De uitzondering op de verplichting van politionele informatie op te nemen in de GGB

Uit eerdere controles is gebeleken dat politionele informatie afkomstig van 'RIR, code 01 of 00' niet werd opgenomen in de GGB.[273] De toezichthoudende autoriteiten hadden de politie gevraagd de regelgeving betreffende de gegevensinvoer in de GGB op grondige wijze te analyseren. Het COC en het Vast Comité I waren van mening dat de analyse van de Politie slechts deels bevredigend was. Er werd een meer grondige analyse ingewacht, waarbij ook de gerechtelijke overheden moesten worden geraadpleegd.

Doorgifte van de lijsten

Het COC en het Vast Comité I stelden vast dat er initiatieven waren genomen om, enerzijds, (gedeeltelijk) een einde te maken aan de doorgifte van lijsten die niet beantwoordde aan de regelgeving en, anderzijds, duidelijke principes te definiëren en protocolakkoorden op te stellen betreffende de doeleinden, de modaliteiten en de veiligheidsaspecten van dergelijke doorgifte. Ze hadden waardering voor de bijzondere initiatieven die de DPO van de GGB nam. Gelet op de actuele regelgeving (en onder voorbehoud van een wijziging daarvan als gevolg van de door het OCAD gevoerde enquête), is het afsluiten van protocollen vereist voor alle diensten die geen rechtstreekse toegang tot de GGB hebben; daarbij dient voorrang te worden gegeven aan de diensten die geen enkele toegang hebben. Het COC en het Vast Comité I bevolen aan om de voorstellen van protocolakkoorden van de DPO te analyseren en vervolgens snel ten uitvoer te leggen.

Raadpleging van het openbaar ministerie door het OCAD m.b.t. de gerechtelijke maatregelen

Gezien het onafhankelijk statuut van het Openbaar Ministerie, bestaat er voor die partnerdienst geen verplichting (maar wel een mogelijkheid) om de GGB TF en HP te voeden, ook al heeft ze een rechtstreekse toegang tot de gegevensbank. De wetgever heeft geoordeeld dat de gerechtelijke gegevens voornamelijk afkomstig zijn van de politiediensten. In die zin is de verplichting voor de politiediensten om de gemeenschappelijke gegevensbank te voeden, voldoende opdat de pertinente

[273] Een 'RIR 01' heeft betrekking oppoliotnele informatie die enkel mag wworden gebruikt voor zover de opsteller daarmee akkoord gaat. Een 'RIR 00' heeft betrekking op politionele informatie die in geen geval mag worden gebruikt.

gegevens van de gerechtelijke politie worden geregistreerd.[274] Om zich ervan te vergewissen dat de voeding van de gegegevensbank goed wordt uitgevoerd, hebben de gerechtelijke overheden instructies verstuurd. Er bleek echter niet dat het OCAD de beginselen toepaste zoals die waren opgenomen in de COL 18/2020. Het COC en het Vast Comité I bevolen het OCAD aan om de beginselen toe te passen die zijn opgenomen in deze COL, om te komen tot een stelselmatige gegevensinvoer en actualisering van de GGB.

Bovendien en onverminderd het beginsel van de scheiding der machten en de autonomie van de gerechtelijke overheden nodigden het COC en het Vast Comité I de minister van Justitie uit om aan het College van procureurs-generaal de opdracht te geven om de omzendbrief COL 18/2020 aan te passen wat betreft de mededeling van de gerechtelijke maatregelen ten aanzien van de potentieel gewelddadige extremisten (PGE).

V.2.3. NIEUWE AANBEVELINGEN

Als gevolg van een veiligheidsincident - de dienst Erediensten en Vrijzinnigheid van de FOD Justitie beschikte over een toegang tot de GGB HP die ruimer was dan de toegang waarin het KB HP voorziet - interpelleerden het COC en het Vast Comité I de verwerkingsverantwoordelijken. Er werd de verwerkingsverantwoordelijken verzocht een einde te stellen aan de gevallen van onregelmatige toegang. De toezichthoudende autoriteiten bevolen de Federale Politie aan om de technische oplossingen te ontwikkelen die nodig zijn om de toegang door deze dienst in overeenstemming te brengen met de geldende wetgeving (i.e. enkel onrechtstreekse toegang tot de GGB HP). Het COC en het Vast Comité I wensten hierover grondig te worden geïnformeerd.

Voorts bevolen ze de verwerkingsverantwoordelijken aan om op juridisch en operationeel vlak na te gaan of de regelgeving betreffende de toegang van de dienst Erediensten en Vrijzinnigheid al dan niet moest worden herzien.

V.3. DE ADVIESOPDRACHT

De Wet op het politieambt (WPA) voorziet verder ook in de verplichting om een gemeenschappelijk advies van het Vast Comité I het COC in te winnen en dit naargelang verschillende hypotheses.

Zo moeten de ministers van Binnenlandse Zaken en Justitie, voorafgaand aan de oprichting van een gemeenschappelijke gegevensbank alsook van de verwer-

[274] Het COC en het Vast Comité I hebben evenwel opgemerkt dat deze redenering niet geldt voor vonnissen en arresten waarvan politiediensten geen kennis hebben.

kingsmodaliteiten, waaronder deze met betrekking tot de registratie van de gegevens en van de verschillende categorieën en types van persoonsgegevens en informatie die verwerkt worden, hiervan aangifte doen bij het Vast Comité I en het COC. Deze dienen op hun beurt een gezamenlijk een advies uit te brengen (art.44/11/3*bis* §3 WPA). Daarnaast bepaalt, na advies van bovenvernoemde controleorganen, voor elke gemeenschappelijke gegevensbank een koninklijk besluit vastgesteld na overleg in de Ministerraad, de types van verwerkte persoonsgegevens, de regels op het gebied van de verantwoordelijkheden op het vlak van de bescherming van de persoonlijke levenssfeer van de organen, diensten, overheden en organismen die gegevens verwerken, de regels op het gebied van de veiligheid van de verwerkingen, de regels van het gebruik, de bewaring en de uitwissing van de gegevens (art.44/11/3*bis* §4 WPA). Verder kunnen bijkomende beheersregels van de gemeenschappelijke gegevensbanken worden bepaald door een koninklijk besluit vastgesteld na overleg in de Ministerraad, evenwel ook hier na advies van het Comité en het COC (art.44/11/3*bis* §8 WPA). Ten slotte strekt de adviesfunctie zich tevens uit tot elk ontwerp van koninklijk besluit tot instelling of wijziging van de toegang tot de gemeenschappelijke gegevensbanken (art.44/11/3*ter* §§2 tot 4 WPA).

Het Vast Comité I en het COC werden in 2021 niet om een dergelijk advies verzocht.

HOOFDSTUK VI.
ADVIEZEN

Artikel 33 van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse (W.Toezicht) bepaalt dat het Comité '*enkel op verzoek van de Kamer van volksvertegenwoordigers of van de bevoegde minister advies [mag] uitbrengen over een ontwerp van wet, van koninklijk besluit, van circulaire of over enig ander document waarin de beleidslijnen van de bevoegde ministers worden geformuleerd*.'

In 2021 werd het Comité zes maal om advies verzocht.[275] De Commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken vroeg het Comité twee maal om advies (over de oprichting van een federaal inlichtingenagentschap (VI.1.) enerzijds en over de strafbaarstellingen ter bevordering van de democratische weerbaarheid (V.5) anderzijds). Ook de Kamer van volksvertegenwoordigers diende een verzoek tot advies bij het Vast Comité I in over de notificatieplicht (VI.2). De minister van Justitie op zijn beurt verzocht het Comité tweemaal om advies (over de dataretentie (VI.3) en over de wijzigingen van de Inlichtingenwet (VI.4)). Ten slotte vroeg de minister van Binnenlandse Zaken de Vaste Comités I en P om een gemeenschappelijk advies aangaande de wijzigingen van de OCAD-Wet (VI.6).[276] Alle adviezen, die hieronder werden opgenomen in chronologische volgorde, zijn intregraal consulteerbaar op de website van het Comité.[277]

Daarnaast dient het Comité ook advies te verlenen als Bevoegde Toezichthoudende Autoriteit (BTA) in het kader van de verwerking van persoonsgegevens alsook bij de wettelijke regeling in verband met gemeenschappelijke databanken, maar dan samen met het Controleorgaan op de politionele informatie (COC). Deze laatste twee adviesbevoegdheden worden respectievelijk behandeld in Hoofdstuk IV en Hoofdstuk V.

---

275 Het Comité wordt steeds meer om advies gevraagd op basis van artikel 33 W.Toezicht; de hieraan geïnvesteerde tijd is bijgevolg dan ook opmerkelijk gestegen.

276 De Vaste Comités I en P formuleerden dit advies als gemeenschappelijke toezichthouder ten aanzien van het OCAD zoals voorzien in de W.Toezicht en in hun hoedanigheid van gegevensbeschermingsautoriteiten ten overstaan van de verwerking van persoonsgegevens door het OCAD.

277 www.comiteri.be

VI.1. ADVIES OVER DE OPRICHTING VAN EEN FEDERAAL INLICHTINGENAGENTSCHAP

In december 2020 werd het Vast Comité I door de Commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken van de Kamer van Volksvertegenwoordigers om advies gevraagd in het kader van het onderzoek van het voorstel van resolutie over de oprichting van een federaal inlichtingenagentschap.[278]

Het voorstel van resolutie had voor ogen om de federale regering te vragen:

- om een audit uit te voeren van zowel de inlichtingendiensten als van de Federale Politie (OA3) voor wat betreft de informatiestroom binnen en tussen die diensten;
- om, op basis van deze audit, een federaal inlichtingenagentschap te creëren waarin alle inlichtingendiensten worden samengebracht onder de bevoegdheid van de Premier;
- de nodige menselijke en technische middelen ter beschikking te stellen van dit agentschap voor de uitvoering van zijn opdrachten.

In zijn advies stelde het Vast Comité I zich (in samenwerking met het Vast Comité P en het Controleorgaan op de politionele informatie) ter beschikking van de Kamer van volksvertegenwoordigers met het oog op zijn deelname aan een audit, waarvan de reikwijdte echter nog beter moest worden bepaald. Gezien de pluraliteit van de hierboven vermelde actoren en partners achtte het Vast Comité I het voorbarig om een conclusie te trekken over de noodzaak om een nieuwe instelling op te richten die één enkele federale inlichtingendienst en één enkele federale politiedienst verenigt (en de middelen die aan deze instellingen ter beschikking moeten worden gesteld) zonder dat de resultaten van de gevraagde audit beschikbaar zijn.

VI.2. ADVIES OVER HET INSTELLEN VAN EEN ACTIEVE KENNISGEVINGSPLICHT VOOR DE INLICHTINGENDIENSTEN

Eind januari 2021 werd een wetsvoorstel neergelegd tot wijziging van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (W.I&V), met het oog op het invoeren van een actieve kennisgevingsplicht met betrekking tot bepaalde specifieke methoden voor het verzamelen van gege-

[278] Dit voorstel van resolutie werd in september 2019 neergelegd in de Kamer. In april 2022 was het nog steeds hangende (*Parl. St.* Kamer 2019-20, 55K0287).

vens.[279] Het wetsvoorstel wenste, enerzijds en in hoofdorde een 'actieve kennisgevingsplicht' en anderzijds een 'passieve kennisgevingsplicht' in te voeren in hoofde van de Belgische inlichtingendiensten.

Een *actieve kennisgevingsplicht*, ook wel gekend als de '(actieve) notificatieplicht', houdt in dat de inlichtingendiensten onder bepaalde voorwaarden uit eigen beweging een geviseerde persoon op de hoogte moeten brengen dat hij of zij het voorwerp van onderzoek is geweest, meer in het bijzonder dat in het verleden een bepaalde inlichtingenmethode op hem of haar werd toegepast.

De *passieve notificatieplicht* impliceert dan weer dat de betrokken inlichtingendienst op verzoek van iedere persoon die een persoonlijk en legitiem belang heeft en onder de Belgische rechtsmacht valt, hem onder bepaalde voorwaarden en volgens bepaalde procedures meedeelt dat op hem een van de inlichtingenmethoden is toegepast.

VI.2.1. DE ACTIEVE NOTIFICATIE

De vraag of een Europees land de verplichting heeft om een actieve notificatieplicht in te voeren, vindt een antwoord in het Europees Verdrag voor de Rechten van de Mens (EVRM), de toepasselijke rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM), het Verdrag nr. 108 van de Raad van Europa tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (bijgewerkt tot Verdrag 108+[280]) alsook, desgevallend, in een betrokken Grondwet en de toepasselijke rechtspraak van een betrokken Grondwettelijk Hof.

Het Comité kon in zijn advies vaststellen dat het EVRM noch de betrokken EHRM-rechtspraak een expliciete verplichting in hoofde van de verdragspartijen bevat om te allen tijde een dergelijke *actieve* kennisgevingsplicht in te voeren. Het gewicht van zo'n plicht moet volgens het Hof wel worden afgezet tegen het geheel van de aanwezige rechtswaarborgen. Daarom moeten alle relevante regels van het nationale recht, met inbegrip van de regels inzake transparantie ten aanzien van de betrokkene, worden beoordeeld.

---

279 *Parl. St.*, Kamer 2020-21, 55K1763/001. Het Comité mocht het verzoek tot advies van de Kamer van volksvertegenwoordigers ontvangen op 6 mei 2021 en bracht advies uit op 31 mei 2021. De voorzitter van het Vast Comité I gaf op 2 juni 2021 toelichting bij het advies in de Kamercommissie Justitie. In april 2022 was het wetsvoorstel nog steeds hangende in de Kamer.

280 Verdrag van de Raad van Europa van 28 januari 1981 tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens (Verdrag 108), gewijzigd door het Protocol nr. 223 van 18 mei 2018 (Verdrag 108+). Het Verdrag 108+ trad nog niet in voege in België (reden waarom de « + » verder tussen haakjes wordt weergegeven). Zie https://www.coe.int/fr/web/data-protection/convention108-and-protocol).

Zich baserende op de twee arresten van het Grondwettelijk Hof[281] en op de rechtspraak van het Europees Hof, stelde de toelichting van het wetsvoorstel dat er nog steeds een plicht tot herinvoering van de actieve notificatieplicht bestaat. Het Comité was evenwel van oordeel dat deze stelling nuancering behoefde aangezien de wetgever nieuwe procedurele waarborgen[282] had ingebouwd sinds de wetten van 2010 en 2017.[283]

De rechtsbescherming van de burger, en dan in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, het recht op bescherming van persoonsgegevens én het recht op een effectief rechtsmiddel, werd sinds de Wet van 30 maart 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van gegevens (de Gegevensbeschermingswet, afgekort: GBW) omstandig gewijzigd. Niet enkel heeft de wetgever met deze wet het regelgevend kader t.a.v. de inlichtingendiensten uitgebreid en verduidelijkt (artt. 72 tot 104 GBW[284]), er werd ook een versterkt corrigerend toezichtmechanisme in het leven geroepen. Meer bepaald werd het Vast Comité I aangewezen als de bevoegde gegevensbeschermingsautoriteit (DPA) binnen het 'nationale veiligheid'-domein.[285] Sinds de GBW staat m.a.w. elke daad van informatiegaring, -behandeling, -analyse en -doorgifte alsook elke gegevensbewaring onder het corrigerend toezicht van het Comité ingeval er sprake is van een persoonsgegevensverwerking.[286] Betekenisvol in het licht van het recht op een effectief rechtsmiddel is dat – in tegenstelling tot bij de uitoefening van het (reeds gedurende de arresten van het Grondwettelijk Hof

281 De notificatieverplichting werd al in 2010 en 2017 ingevoerd door de wetgever in art. 263 W.I&V. Het Grondwettelijk Hof vernietigde evenwel tweemaal dit artikel aangezien zij de bestaande procedurele rechtswaarborgen onvoldoende achtte om het ontbreken van een actieve kennisgevingsplicht in hoofde van de inlichtingendiensten te rechtvaardigen.

282 Het Comité wenste op te merken dat de memorie van toelichting van de Wet van 30 maart 2017 noch het Grondwettelijk Hof gewag maken van de procedurele waarborgen voorzien in de Wet van 11 april 1994 betreffende de openbaarheid van bestuur (WOB). Nochtans kan de problematiek van de actieve notificatie eveneens gesitueerd worden binnen het recht op toegang tot bestuursdocumenten en informatie van de inlichtingendiensten, aangezien deze wetgeving, tot op zekere hoogte, kennisgeving aan de betrokkene toelaat. Zowel de Raad van State als de Commissie Openbaarheid van Bestuur hebben immers al herhaaldelijke malen bevestigd dat de WOB van toepassing is op de VSSE en de ADIV

283 De Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (*B.S.* 10 maart 2010) en de Wet van 30 maart 2017 tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst en van artikel 259*bis* van het Strafwetboek, *B.S.* 28 april 2017.

284 Ondertitel 1 van titel 3 (artt. 72 tot 104 GBW) regelt de verwerking van persoonsgegevens door de VSSE en de ADIV in het kader van de uitvoering van haar opdrachten, met uitzondering van de persoonsgegevensverwerkingen in het kader van de Classificatiewet van 11 december 1998. Laatstgenoemde aangelegenheid wordt geregeld in ondertitel 3 van titel 3 van de GBW (artt. 106 tot 137 GBW).

285 VAST COMITÉ I, *Activiteitenverslag 2019*, 75-80.

286 Gelet op de ruime verdragsrechtelijke invulling van het begrip 'verwerking van persoonsgegevens' (*cf.* artikel 8 EVRM *i.o.* Verdrag nr. 108(+)) staan zodoende alle persoons-gegevensverwerkingen verricht door de inlichtingendiensten onder het DPA-toezicht van het Comité. In zijn rol van gegevensbeschermingsautoriteit treedt het Vast Comité I ofwel op uit eigen beweging, ofwel op verzoek van een andere gegevensbeschermingsautoriteit, ofwel op verzoek van elke betrokkene.

bestaande) BIM-klachtenrecht[287] waarbij een klacht de grieven dient te vermelden van de verzoeker die tevens een persoonlijk en rechtmatig belang moet kunnen aantonen – er bij de uitoefening van het verzoek bedoeld in artikel 51/2 W.Toezicht geen dergelijke formele voorwaarden vereist worden: *"Om ontvankelijk te zijn, is het verzoek geschreven, gedateerd, ondertekend en met redenen omkleed en rechtvaardigt het de identiteit van de betrokkene*". In de praktijk heeft het Comité een zeer soepele houding aangenomen wat betreft de motiveringsplicht. In tegenstelling tot de situatie van voor de Gegevensbeschermingswet, is het recht op toegang tot een effectief rechtsmiddel gevoelig verbeterd.

Volgens het Comité zal de versterking van zijn bevoegdheden na de goedkeuring van de GBW in 2018, in combinatie met de invoering van een systeem van passieve kennisgeving[288] waarin dit voorstel voorziet, voldoen aan de transparantievereiste uit hoofde van het internationaal recht. In het licht van deze vaststelling was het Comité van oordeel dat er geen verdragsrechtelijke verplichting bestaat in hoofde van de federale wetgever om een actieve kennisgevingsplicht in te voeren, op voorwaarde dat enerzijds in het voorstel een verplichting tot passieve kennisgeving wordt opgenomen daarbij rekening houdend met de opmerkingen van het Comité (*infra*).

Niettemin wenste het Comité hier wel onmiddellijk aan toe te voegen en te benadrukken dat het de federale wetgever in België steeds vrijstaat om een dergelijke regeling desondanks in te voeren.[289] In de eventualiteit dat de wetgever hiervoor zou kiezen, formuleerde het Comité een aantal opmerkingen op de verschillende artikels over de verplichting tot actieve notificatie. Deze gingen onder meer over:

- de (niet toegelichte) keuze om de werkingssfeer van de vooropgestelde bepalingen tot slechts enkele methoden te beperken;
- het vastgestelde verschil met de bestaande actieve notificatieverplichting in de strafrechtsprocedure (art. 90novies Sv.);
- de uitzonderingsgronden die bij voorkeur moeten worden afgestemd op deze uit bestaande regelgeving (WPA, W.C&HS, W.I&V, W.Beroepsorgaan);
- de te notificeren personen;
- de notificatietermijnen;
- de toezichthoudende instantie, waarbij het Comité van oordeel was dat één toezichtsorgaan afdoende is.

---

287 Bedoeld in artikel 43/4, eerste lid, derde streepje W.I&V.

288 Rekening houdend met de opmerkingen in dit advies.

289 Een beslissing tot invoering van (een of andere vorm van) actieve kennisgevingsplicht werd zodoende genomen in 6 van 47 lidstaten van de Raad van Europa.

VI.2.2. DE PASSIEVE NOTIFICATIE

Weliswaar ingenomen met het voorstel om de passieve kennisgeving te herintroduceren, wees het Comité erop dat er reeds verschillende systemen, bevoegdheden en procedures bestaan inzake de transparantie van informatie waarover inlichtingendiensten beschikken. In dit verband merkte het Comité op dat de mogelijkheden om actie te ondernemen voor de burger ingewikkeld zijn en moeilijk uitvoerbaar en dat de keuze van een procedure gevolgen zal hebben voor zijn of haar mogelijkheden om (al dan niet) toegang te krijgen tot informatie. Een harmonisatie van de procedures voor toegang tot informatie en de uitzonderingen van mededeling van informatie – en dus een harmonisatie van de uitkomst van de verschillende procedures – is wenselijk.

Het Comité vestigt er dan ook de aandacht van de wetgever op dat in de memorie van toelichting van het passieve kennisgevingssysteem moeten worden toegelicht en gepreciseerd, alsook de manier waarop het zal worden gekoppeld aan de bestaande procedures.

VI.3. ADVIES OVER DATARETENTIE

Door de minister van Justitie werd bij het Vast Comité I een adviesaanvraag ingediend met betrekking tot het voorontwerp van wet 'betreffende het verzamelen en het bewaren van de identificatie-, verkeer- en localisatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten' (hierna: het wetsontwerp).[290] [291] Ten gevolge de annulatie door het Grondwettelijk Hof van de artikelen 2, b), 3 tot 11 en 14 van de Wet van 29 mei 2016 betreffende het verzamelen en het bewaren van de gegevens in de sector van de elektronische communicatie[292], had het voorstel tot doel om een systeem van bewaring van communicatiegegevens in te voeren dat voldeed aan de vereisten zoals opgelegd door het Hof van Justitie van de Europese Unie (HvJEU). Om dit te bewerkstelligen drongen er zich wijzigingen op aan onder meer de Wet van 13 juni 2005 betreffende de elektronische communicatie (Telecomwet, WEC) en aan de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (Inlichtingenwet, W.I&V).

---

290 Het Comité ontving de vraag op 7 mei 2021 en bracht op 15 juni 2021 zijn advies uit.

291 Het voorontwerp werd door de Ministerraad in december 2021 in tweede lezing goedgekeurd en neergelegd in de Kamer in maart 2022. Nog in maart 2022, werden 18 amendementen goedgekeurd op de Ministerraad (ten gevolge van het arrest van het Grondwettelijk hof nr. 158/2021 d.d. 18 november 2021). Er werd aan de Raad van State en de GBA om advies op deze amendementen gevraagd. De GBA gaf zijn advies op 1 april 2022 (Zie advies nr. 66/2022 van de GBA).

292 Deze wet werd geannuleerd omwille van tegenstrijdigheden met het Europees recht en de rechtspraak van het Hof van Justitie van de Europese Unie. (HvJEU).

Het Vast Comité I richtte zijn advies op de wijzigingen aan de Inlichtingenwet alsook op de wijzigingen relevant voor zijn bevoegdheid aan de Telecomwet.[293]

VI.3.1. WIJZIGINGEN AAN DE INLICHTINGENWET

VI.3.1.1. Gerichte bewaring van verkeers- en lokalisatiegegevens

De regering stelde voor om in het kader van het gericht bewaren van verkeers- en lokalisatiegegevens in de sector van de elektronische communicatie een nieuwe gewone methode in de Inlichtingenwet in te schrijven.

Het Comité stelde vast dat niet eenzelfde niveau van rechtsbescherming in het wetsontwerp wordt ingebouwd en was van oordeel dat er geen objectieve rechtvaardiging bestaat om de burger minder te beschermen in de inlichtingenprocedure dan in de strafprocedure.

Ook de als controlemechanisme voorgestelde procedure – m.n. een maandelijkse notificatie van de gedane methoden (dus na de uitvoering van meerdere methoden) – correspondeerde volgens het Comité geheel niet met de graad van inmenging die een dergelijke methode met zich meebrengt en beantwoordt niet aan de vereisten van het Hof van Justitie waarin werd gesteld dat een gerichte bewaring van verkeers- en lokalisatiegegeven een effectieve rechterlijke toetsing vereist.

Het Comité wees er tevens op dat de uitgewerkte delegatiebevoegdheid in het kader van deze nieuwe gewone methode met betrekking tot verkeers- en lokalisatiegegevens inzake elektronische communicatie niet voldeed. De regering stelde voor dat de betrokken vorderingsbevoegdheid uitgeoefend mag worden door *"het diensthoofd of zijn gedelegeerde"*. Net zoals het Grondwettelijk Hof en het EHRM is het Comité van oordeel dat dergelijke gegevens zeer intrusief zijn. Er kan bijgevolg geen rechtvaardiging gevonden worden om een bijkomende delegatiebevoegdheid te voorzien naast deze die al werd ingeschreven in de Inlichtingenwet. Bijgevolg werd de regering gevraagd deze keuze te motiveren.[294]

---

293 Het Comité sprak zich niet uit over de vraag of de door het wetsontwerp in de Telecomwet aangebrachte wijzigingen al dan niet voldoen aan de vereisten van de rechtspraak van het Hof van Justitie en het Belgische Grondwettelijk Hof. Daartoe wordt verwezen naar het advies van de Gegevensbeschermingsautoriteit over het wetsontwerp https://www.gegevensbeschermingsautoriteit.be/publications/advies-nr.-108-2021.pdf

294 Betekenisvol is dat de wettelijke definitie van het begrip diensthoofd reeds een delegatiebevoegdheid in zich draagt: *bij verhindering* van de administrateur-generaal van de VSSE of van de chef van de ADIV, hebben de respectievelijke hoofden de mogelijkheid om hun beslissingsbevoegdheid te delegeren naar de *dienstdoende* administrateur-generaal respectievelijk de *dienstdoende* chef. Een dergelijke delegatie beperkt zich niet tot de adjunct-administrateur-generaal van de VSSE en de adjunct-chef van de ADIV. Wanneer laatstgenoemden op hun beurt verhinderd zijn, kan opnieuw een delegatie toegekend worden aan een hiërarchisch lager niveau.

VI.3.1.2. Toegang tot verkeers- en lokalisatiegegevens

Het wetsontwerp beoogde het grotendeels door het Grondwettelijk Hof[295] vernietigde artikel 18/8 W.I&V te herstellen dat de toegang tot de verkeers- en lokalisatiegegevens met betrekking tot elektronische communicatie door de inlichtingendiensten regelde.

Het Comité bracht de regering in herinnering dat het Grondwettelijk Hof het gehele artikel 18/8 W.I&V had vernietigd. Stellen dat enkel de vernietiging van paragraaf 2 zich opdringt in het licht van de betrokken arresten van het Grondwettelijk Hof en het EHRM, was naar het oordeel van het Comité een voorbarige conclusie. Het is het geheel aan procedurele rechtswaarborgen dat in overweging genomen moet worden.

VI.3.1.3. Algemene en ongedifferentieerde bewaring van verkeers- en lokalisatiegegevens

Het wetsontwerp voorzag om in het kader van het bewaren van verkeers- en lokalisatiegegevens in de sector van de elektronische communicatie een nieuwe uitzonderlijke methode in de Inlichtingenwet in te schrijven in geval van een reële, actuele of voorzienbare ernstige bedreiging van de nationale veiligheid. In dat geval, voorzag het ontwerp dat de inlichtingendiensten de medewerking zouden (kunnen) vorderen van operatoren voor het algemeen en ongedifferentieerd bewaren van verkeers- en lokalisatiegegevens van elektronische communicatie die door hen wordt gegenereerd en verwerkt.

Het Comité onderschreef ten volle het voorstel van de regering om de aanwending van deze bevoegdheid te onderwerpen aan alle controlemechanismen eigen aan de uitzonderlijke methoden.

Het Comité beval aan om de band tussen het actuele artikel dat de toegang regelt en het ontworpen artikel dat de algemene bewaring regelt, te verstevigen. Momenteel is het mogelijk dat een welbepaalde dreiging (bijv. terrorisme) de rechtvaardiging kan vormen om een algemene en ongedifferentieerde bewaring op te leggen aan de telecomoperatoren, zonder dat vervolgens enige beperking van toepassing is en dat bijgevolg de toegang tot deze gegevens ook kan worden gebruikt voor andere doeleinden (bijv. binnen de bestrijding van andere dreigingen).

De memorie van toelichting stelde hieromtrent: *"De machtiging van het betrokken diensthoofd om deze uitzonderlijke methode toe te passen, wordt ter informatie aan de bevoegde minister overgemaakt. Het doel is de bevoegde minister in kennis te stellen van het feit dat een ongedifferentieerde bewaring gestart is."*[296] Het Comité

---

295 G.H., arrest nr. 57/2021 van 22 april 2021.

296 Voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie-, verkeer-, en localisatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten, pp. 111-112.

beval aan om de betrokken minister niet enkel in kennis te stellen van de uiteindelijke "machtiging" van het diensthoofd maar eerder ook al van het "ontwerp van machtiging". Zowel de notificatie van het ontwerp van machtiging als de notificatie van de machtiging worden actueel niet voorzien in de BIM-procedure bij uitzonderlijke methoden. Het Comité is echter van oordeel dat een bevel van de inlichtingendiensten aan de telecomoperatoren tot het algemeen en ongedifferentieerd[297] bewaren van verkeers- en lokalisatiegegevens een dusdanige grote impact heeft op vlak van de inmenging in de persoonlijke levenssfeer van de burgers en inwoners van België dat dergelijke afwijkende vormvereisten zeker te rechtvaardigen zijn.[298]

Het Comité kon tevens geen reden terugvinden waarom de bewaarperiode[299] en de periodiciteit van verslaggeving[300] afweken van de geldende aanwendingsduur bij uitzonderlijke methoden.

Het Comité beval ten slotte aan om te verduidelijken wat de verhouding is tussen het ontworpen artikel 18/17/1 W.I&V en de bijzondere beschermingsregeling voor advocaten, artsen en journalisten ingericht in de Inlichtingenwet.[301]

VI.3.1.4. Verplichte kennisgeving aan de operatoren

Het Comité beval tevens aan om een verplichting in hoofde van de inlichtingendiensten te creëren om de betrokken operatoren op de hoogte te brengen wanneer het Vast Comité I de stopzetting van een algemene en ongedifferentieerde bewaring of van een gerichte bewaring heeft bevolen.

---

297 In tegenstelling tot de andere uitzonderlijke methoden die doelgericht zijn (cf. art. 18/10, §2, 2° W.I&V).

298 Een kennisgeving van de machtiging dient hierbij, zoals de memorie van toelichting duidelijk verwoord, om de regering op de hoogte te brengen dat een algemene en ongedifferentieerde bewaring gestart is. Een kennisgeving van het ontwerp van machtiging aan de betrokken minister beoogt niet om de beslissingsbevoegdheid op ministerieel niveau te brengen, maar om de regering verplicht op de hoogte te brengen dat volgens de betrokken inlichtingendienst er een gevaar voor de nationale veiligheid aanwezig is van een dermate hoog niveau dat een dergelijke verregaande maatregel van algemene en ongedifferentieerde bewaring van betrokken communicatiegegevens gerechtvaardigd lijkt te zijn.

299 Er werd een bewaarperiode voorgesteld van zes maanden in plaats van twee maanden die verlengd kunnen worden.

300 Er werd gekozen voor een tweemaandelijkse periodiciteit, terwijl nu om de twee weken wordt gerapporteerd.

301 Krachtens artikel 18/9, §4 W.I&V kunnen uitzonderlijke methoden slechts aangewend worden tegen een van deze beschermde beroepen of, onder meer, van hun communicatiemiddelen die ze voor beroepsdoeleinden gebruikten op voorwaarde dat de inlichtingendienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van een ernstige potentiële dreiging. Desgevallend dient een bijzondere procedure gevolgd te worden.

VI.3.2. WIJZIGINGEN AAN DE TELECOMWET (WEC)

Het Comité formuleerde eveneens meerdere opmerkingen wat de betreft de voorgestelde wijzigingen aan de Telecomwet. De ontworpen bepaling stelde een gerichte gegevensbewaring voor in geval van ernstige, reële en actuele bedreiging voor de nationale veiligheid op grond van een geografisch criterium, zijnde voor alle zones waar het algemeen dreigingsniveau ten minste niveau 3 bedraagt en zolang niveau 3 blijft bestaan voor deze zones. Het Comité vroeg om het begrip "zones" in deze bepaling nader te verduidelijken.

Het ontwerp belastte de inlichtingendiensten met het jaarlijks opstellen van een lijst van "*de gebouwen bestemd voor rechtspersonen waarvan het economisch en wetenschappelijk potentieel beschermd moet worden*" en die op voorstel van de ministers van Justitie en Defensie dient goedgekeurd te worden door de Nationale Veiligheidsraad. Het Comité bracht de regering in herinnering van het bestaan van het Actieplan van de federale regering tot vrijwaring van het wetenschappelijk en economisch potentieel.[302] Ook dit actieplan bevat een lijst van entiteiten. Het Comité stelde vast dat deze lijst – gemaakt in 2007 – geen actualisering kende. In het licht van deze vaststelling stelde het Comité de vraag of een jaarlijkse actualisering van de lijst voorzien in het wetsontwerp realistisch is.

Het Comité stelde verder vast dat een verplichte kennisgeving ontbrak waarbij de gerichte geografische bewaring gebeurt op grond het algemene dreigingsniveau zoals bepaald door het Coördinatieorgaan voor de dreigingsanalyse (OCAD). Het Comité herinnerde er de regering aan dat het Vast Comité I en het Vast Comité P, gezamenlijk, de bevoegde gegevensbeschermingsautoriteiten zijn tegenover het OCAD. Het Comité beval aan om eenzelfde kennisgevingsplicht in te richten (minstens) aan het Vast Comité I en om hieromtrent eveneens het Vast Comité P te bevragen.

VI.4. ADVIES OVER HET VOORONTWERP VAN WET TOT WIJZIGING VAN DE INLICHTINGENWET

Op verzoek van de minister van Justitie gaf het Vast Comité I zijn advies over het voorontwerp van wet 'tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten'.[303] [304] Het wetsontwerp voorzag onder meer in een uitbreiding van de mogelijkheden voor de agenten van de

---

302 Op 16 maart 2007 goedgekeurd door het Ministerieel Comité voor inlichting en veiligheid (heden: de Nationale Veiligheidsraad), afgekort: het Plan WEP.

303 De minister verzocht het Comité om advies op 31 mei 2021; het Comité bracht zijn advies uit op 15 juni 2021. Het betrof het tweede advies van het Comité in deze context. Het Comité gaf al op 16 november 2018 een advies over een wetsontwerp waarin grotendeels dezelfde voorstellen werden geformuleerd.

304 In april 2022 werd dit voorstel in tweede lezing nog niet goedgekeurd door de Ministerraad.

inlichtingendiensten om misdrijven te plegen alsook in een bijzondere procedure voor de aanwending van een fictieve identiteit. Tevens werd de mogelijkheid gecreëerd opdat ook menselijke bronnen bepaalde misdrijven zouden kunnen plegen alsook om bijzondere inlichtingenmethoden in te zetten om de betrouwbaarheid van bronnen na te gaan. Er zou tevens een nieuwe bevoegdheid worden toegekend aan de Algemene Dienst Inlichting en Veiligheid (ADIV) in het kader van een nationale cybersecuritycrisis. Ten slotte werd ook een herschikking voorgesteld inzake de reeds bestaande methode van collecte bij de banken en financiële instellingen.

VI.4.1. EEN TE COMPLEXE REGELGEVING

Algemeen, stelde het Comité vast dat de voorgestelde wetswijzigingen de regelgeving van toepassing op de Veiligheid van de Staat (VSSE) en op de ADIV er een stuk complexer en onsamenhangender op maken. De keuzes van de BIM-wetgever in 2010 om in de Inlichtingenwet een logische structuur in te stellen voor wat betreft de (onderzoeks)bevoegdheden van de inlichtingendiensten (o.m. een onderscheid tussen uitzonderlijke, specifieke en gewone methoden naargelang de graad van privacy-inmenging) werd door de wetswijzigingen van de laatste jaren grotendeels verlaten. Het Comité betreurde dat het wetsontwerp zich inschakelde binnen deze evolutie.

Het Comité stelt vast dat bepaalde keuzes in voorliggend wetsontwerp nodeloos ingewikkeld en onvolledig zijn. Een gegeven dat volgens het Comité niet bevorderlijk is voor een goede toekomstige toepassing van betrokken regelgeving.

VI.4.2. CYBERSECURITY - OPDRACHT VAN DE ADIV

Het wetsontwerp gaf de ADIV een nieuwe opdracht, namelijk *"het neutraliseren, in het kader van een nationale cyber security crisis, van een cyberaanval op informatica- en verbindingssystemen niet beheerd door de Minister van Landsverdediging en er de daders van identificeren, onverminderd het recht onmiddellijk met een eigen cyberaanval te reageren overeenkomstig de bepalingen van het internationaal recht"*.

Deze nieuwe opdracht vormt een aanvulling op de bestaande cybersecurity-opdracht[305] door de ADIV de mogelijkheid te bieden op te treden tegen een cyberaanval op informatica- en verbindingssystemen die niet worden beheerd door de minister van Defensie. De materiële bevoegdheid van de ADIV in het kader van deze niet-militaire *cybersecurity*-opdracht wordt bepaald door het voorstel van

[305] Deze opdracht wordt bepaald in artikel 11, §1, 2° W.I&V en laat de ADIV toe te reageren op een cyberaanval op informatica- en communicatiesystemen dewelke worden beheerd door de minister van Defensie.

definitie van het begrip "nationale *cyber security* crisis" als "*elke cyber security gebeurtenis die wegens haar aard of gevolgen:*
- *de vitale belangen van het land of de essentiële behoeften van de bevolking bedreigt*
- *een dringende besluitvorming vereist*
- *en de gecoördineerde inzet van verscheidene departementen en organismen vergt.*[306]

Het Comité was van oordeel dat de door de ADIV te beschermen entiteiten in het kader van deze cybersecurity-opdracht te ruim omschreven werden. De woordengroep "*de vitale belangen van het land of de essentiële behoeften van de bevolking*" was te weinig afbakenend. Het Comité beval daarom aan in te zetten op de 'kritieke infrastructuren' als te beschermen entiteiten (*cf.* de Wet van 1 juli 2011 betreffende de beveiliging en de bescherming van de kritieke infrastructuren).

De ontworpen bepaling geeft de ADIV niet enkel de bevoegdheid om een cyberaanval te 'neutraliseren', maar tevens om hierop te reageren met 'een eigen cyberaanval'. Een dergelijk recht bestaat ook reeds in het bestaande artikel 11, §1, 2° W.I&V. Het Comité stelde zich de vraag wat het exacte wettelijke kader is dat bij de uitoefening van een dergelijke aanvalsbevoegdheid gerespecteerd moet worden. Het Comité vroeg daarom om te verduidelijken hoe het oorlogsrecht zich hier verhoudt ten aanzien van het strafrecht.[307]

VI.4.3. HET PLEGEN VAN ONDERSTEUNENDE MISDRIJVEN

VI.4.3.1. Algemeen

Het plegen van misdrijven wordt in het wetsontwerp toegelaten bij diverse soorten opdrachten van de VSSE en de ADIV. Het Comité beval aan om de mogelijkheid te schrappen om misdrijven te plegen in het kader van de ADIV-opdracht inzake het zorgen voor het behoud van de militaire veiligheid en deze inzake het beschermen van het geheim. Het Comité zag geenszins enige redenen waarom deze mogelijkheid zou moeten ingevoerd worden bij deze opdrachten.

Het ontwerp bevatte een lijst van misdrijven die niet door de agenten van beide inlichtingendiensten respectievelijk door menselijke bronnen (HUMINT) gepleegd mogen worden. Het Comité stelde vast dat betrokken lijst niet afdoende

306 De memorie van toelichting verduidelijkt dat deze definitie van 'crisis' werd overgenomen uit artikel 2 van het koninklijk besluit van 18 april 1988 tot oprichting van het Coördinatie- en Crisiscentrum van de Regering.

307 Een cyberaanval op Belgische IT-infrastructuren is namelijk een misdrijf. De vraag rijst bijgevolg of een dergelijke cyberaanval geen inmenging betekent in de gerechtelijke opdrachten. De situatie waarin een misdrijf plaatsvindt met louter een binnenlandse dimensie moet aangepakt wordt via het strafrecht.

exhaustief was en stelde voor om een aantal misdrijven en misdrijfcategorieën aan deze verbodslijst toe te voegen.

Het Comité betreurde het dat de BIM-Commissie geen overeenstemmende sanctiebevoegdheden in het wetsontwerp kreeg wanneer ondersteunende misdrijven onrechtmatig worden gepleegd gedurende de aanwending van gewone methoden. De Commissie heeft hier – i.t.t. bij BIM-methoden – geen actiemogelijkheid tegen onrechtmatig verkregen gegevens. Het Comité beval aan om de BIM-Commissie eenzelfde controle- en sanctiebevoegdheden toe te kennen die ze heeft bij de controle van uitzonderlijke methoden (*cf.* artikel 18/10, §6 W.I&V). Hierdoor zou het 'plegen van misdrijven' geen uitzonderlijke methode worden, maar zou de controle erop wel plaatsvinden *zoals bij uitzonderlijke methoden*. Er zou aldus eenzelfde niveau van rechtsbescherming plaatsvinden.

VI.4.3.2. Lacune binnen de strafprocedure

Het Comité bracht eveneens een lacune binnen de strafprocedure onder de aandacht. Binnen de strafprocedure is de kamer van inbeschuldigingstelling bevoegd voor het toezicht op de regelmatigheid van het gerechtelijk onderzoek (*cf.* art. 235*bis* e.v. Sv). Buiten een procedure met een beperkt toepassingsgebied[308], bestaat er geen vergelijkbare procedure waarbij er gedurende de strafprocedure een toezicht wordt ingericht op de regelmatigheid van het inlichtingenonderzoek. Dit is nochtans noodzakelijk gezien een strafdossier eveneens nota's van inlichtingendiensten kan bevatten.

In het licht van de door de regering voorgestelde 'plegen van misdrijven'-procedure beval het Comité daarom aan om de 'prejudiciële adviesprocedure in strafzaken' te veralgemenen. Hierbij dienen dan de strafgerechten de mogelijkheid te hebben om het Comité te vatten en bevragen rond de wettigheid van 'intelligence'-gegevens die zich in het strafdossier bevinden.

VI.4.3.3. Het plegen van misdrijven door agenten

Om de opvolging door de commissie van een misdrijf van een agent dat werd toegelaten door de BIM-Commissie te kunnen realiseren, beval het Comité aan dat

[308] De beperkte procedure vormt de zgn. 'prejudiciële adviesprocedure' (*cf.* artt. 131*bis*, 189*quater* en 279*bis* Sv.) waarbij een strafgerecht aan het Vast Comité I de regelmatigheid kan vragen van de BIM-methoden die aanleiding gaven tot het opstellen van een zogenaamd 'niet-geclassificeerd proces-verbaal' (*cf.* art. 19/1 W.I&V). Dit proces-verbaal wordt door de BIM-Commissie opgesteld wanneer er aanwijzingen van misdrijven naar boven kwamen via het gebruik van BIM-methoden.

in het ontwerp van machtiging de naam van de persoon verantwoordelijk om de aanwending van de maatregel op te volgen, zou worden opgenomen.[309]

In het licht van de bescherming van de agenten, beval het Comité aan dat het betrokken diensthoofd een jurisdictioneel beroep kan instellen bij het Vast Comité I tegen een negatieve beslissing van de Commissie, indien door onvoorziene omstandigheden de procedure niet kon worden gevolgd en er een strafbaar feit gepleegd is dat strikt noodzakelijk was ter verzekering van de eigen vrijheid of die van derden.

VI.4.3.4. Het plegen van misdrijven door informanten

Wat betreft het plegen van misdrijven door menselijke bronnen, beval het Comité aan te preciseren dat deze enkel zouden zijn toegelaten in het kader van een inlichtingenopdracht. Omdat er geen 'wettelijke' definitie van het begrip 'menselijke bronnen' bestaat, is het materiële toepassingsgebied van deze strafuitsluitingsgrond onvoldoende duidelijk.

Om een daadwerkelijke controle toe te laten, beval het Comité aan om in het ontwerp van machtiging de naam van de behandelende officier van de betrokken menselijke bron op te nemen. Het Comité was ook van oordeel dat alle betrokken toezichthoudende instanties de bevoegdheid moeten hebben om kennis te nemen van de identiteit van de informant.[310]

VI.4.3.5. Schade opgelopen of veroorzaakt door een menselijke bron

Het ontwerp creëert een schaderegeling voor schade aan een informant alsook voor schade veroorzaakt door een informant tijdens zijn opdracht. Het Comité onderlijnde het gebrek aan duidelijkheid inzake de beschrijving van de te volgen procedure.

VI.4.3.6. Onvoldoende rechtsbescherming voor de menselijke bron

Het Comité stelde vast dat het voor advies voorgelegde wetsontwerp een onvoldoende graad van rechtsbescherming bood voor de menselijke bron die een toelating verkreeg om bepaalde misdrijven te plegen. Het wetsontwerp geeft namelijk geen antwoord op de vraag hoe de betrokken gerechtelijke overheden met zekerheid kunnen weten dat een geverbaliseerd persoon over een toelating van de

---

309 Het Comité erkent dat het niet altijd mogelijk is om voorafgaand de naam te kennen van de agent die belast wordt met de uitvoering van een inlichtingenmethode of beschermings- en ondersteuningsmaatregel. Maar dit is niet het geval voor de verantwoordelijke voor de opvolging van de maatregel.

310 Het geven van een akkoord aan een informant (een privépersoon aldus) om misdrijven te plegen, zonder dat de BIM-Commissie weet aan wie dat ze deze toestemming geeft, maakt een effectieve controle onmogelijk.

BIM-Commissie beschikt om bepaalde misdrijven te plegen.[311] Het Comité deed diverse voorstellen om hieraan te verhelpen.[312]

VI.4.4. FICTIEVE IDENTITEIT EN HOEDANIGHEID: ALS ONDERSTEUNINGSMAATREGEL BIJ EEN INLICHTINGENMETHODE OF LOUTER OM VEILIGHEIDSREDENEN

Het wetsontwerp wijzigt de bestaande procedure voor de creatie en het gebruik van een fictieve identiteit (heden: artikel 13/2 W.I&V), alsook creëert het een nieuwe bevoegdheid inzake het gebruik van een fictieve identiteit voor redenen van informatiegaring.

Het Comité suggereerde om de BIM-Commissie toe te laten een controle uit te voeren in alle mogelijke gevallen waar zij de mening toegedaan is dat een fictieve identiteit wordt gebruikt voor de informatiegaring (en dit, zelfs als de betrokken dienst andere motieven vooropstelt om het beroep op een fictieve identiteit te rechtvaardigen). Het Comité nodigde de wetgever tevens uit om de begrippen 'fictieve identiteit' en 'fictieve hoedanigheid' in te wet te verduidelijken.[313]

VI.4.5. INFILTRATIE IN DE REËLE EN VIRTUELE WERELD

Het wetsontwerp kiest ervoor om de controle op de infiltratiebevoegdheid onrechtstreeks te organiseren via de controle op het plegen van misdrijven en/of op het gebruiken van een fictieve identiteit. De hieruit voortvloeiende procedure is nodeloos ingewikkeld, onvolledig en voldoet geenszins aan de noodzakelijke rechtswaarborgen die aanwezig moeten zijn bij een dergelijk verregaande onderzoeksbevoegdheid. Het Vast Comité I adviseerde dan ook negatief. Voor wat betreft het onderdeel rechtsbescherming is het Comité van oordeel dat voorliggend

311 Dit is problematisch gelet op het feit dat het parket, het onderzoeksgerecht of, in laatste instantie, het vonnisgerecht de bevoegde instanties zijn om te oordelen over het concreet bestaan van een strafuitsluitingsgrond in hoofde van de geverbaliseerde persoon.

312 Zoals bijv. de mogelijkheid voor de BIM-Commissie om, in sommige gevallen, een akte op te stellen waarin haar akkoord tot het plegen van bepaalde misdrijven beschreven wordt; het afsluiten van een protocolakkoord tussen de inlichtingen- en veiligheidsdiensten, de BIM-Commissie en het College van procureurs-generaal om een communicatiekanaal in te richten tussen alle actoren.

313 Het Comité stelt zich bijvoorbeeld de vraag of het doelbewust niet meedelen aan een gesprekspartner van de hoedanigheid van lid van een inlichtingendienst gedurende het inwinnen van gegevens reeds een gebruik van een fictieve hoedanigheid is

wetsontwerp niet voldoet aan de eisen gesteld door de parlementaire onderzoekscommissie.[314]

Het wetsontwerp geeft deze nieuwe bevoegdheid de kwalificatie van gewone methode. Rekening houdende met de wijze waarop infiltratie wordt geregeld in de strafprocedure, stelde het Comité voor om de 'infiltratie in de reële wereld' te kwalificeren als uitzonderlijke methode en de 'infiltratie in de virtuele wereld' als specifieke methode.

Bovendien stelde het Comité vast dat via de procedure vastgelegd aangaande het gebruik van een fictieve identiteit voor informatiegaring, de schijn wordt gewekt dat een procedure wordt ingericht vergelijkbaar met de BIM-toelatingsprocedure voor uitzonderlijke methoden. Het Comité stelt vast dat deze werkwijze er echter voor zorgt dat diverse controlemechanismen van toepassing bij uitzonderlijke methoden achterwege worden gelaten.

Een kwalificatie van de infiltratiebevoegdheid als BIM-methode heeft daarenboven als gevolg dat er een gestructureerde controle door de BIM-Commissie mogelijk wordt op de bekomen onderzoeksresultaten.[315]

VI.4.6. GEWONE METHODEN PLUS

In zijn advies onderlijnde het Comité dat de procedurele garanties voor de inzet van gewone methoden plus niet meer voldeden, en dat de controle er op onvoldoende juridische bescherming bood. Er werd bijgevolg dan ook aanbevolen om de controle op de gewone methoden plus (MPLUS-methoden) te versterken, en dit door alle MPLUS-methoden op eenzelfde wijze te behandelen en om zodoende in hoofde van de inlichtingendiensten een verplichting te creëren waarbij elke aanwending van een dergelijke methode voorafgaat door een schriftelijke en gemoti-

314 De memorie van toelichting verwijst terecht naar het Derde tussentijdse verslag van de parlementaire onderzoekscommissie Terroristische aanslagen waarin de aanbeveling wordt gedaan om een infiltratiebevoegdheid voor de inlichtingendiensten in te richten. De aanbeveling stelt echter eveneens dat *"(i)n de uit te werken wettelijke regeling (…) echter de nodige waarborgen (moeten) worden voorzien, zowel inzake de rechtsbescherming van de burgers als inzake de veiligheid van de agenten van de VSSE die met de infiltratie worden belast."* Zie *Parl. St.*, Kamer, 2016-17, 54K1752/008.

315 Vroeger was de toelatingsprocedure wellicht niet afdoende aangepast aan de uitoefening van een infiltratiebevoegdheid. De wetgever heeft evenwel de laatste jaren in de Inlichtingenwet een aantal instrumenten in het leven geroepen die deze vroegere belemmeringen remediëren.

veerde beslissing, die de betrokken dienst ambtshalve en zo spoedig mogelijk ter kennis brengt aan het Comité.[316]

VI.4.7. VORDEREN VAN FINANCIËLE GEGEVENS

Het ontwerp voert een nieuwe gewone methode in. Ze creëert een medewerkingsverplichting voor financiële instellingen in de meest ruime zin van het woord om over te gaan tot de identificatie van financiële producten of diensten waarover een persoon beschikt of, omgekeerd, om te identificeren welke persoon kan gelinkt worden aan bepaalde financiële producten of diensten. Actueel is dit een uitzonderlijke methode.

Het Comité beval aan om deze methode te kwalificeren als een specifieke methode. In de memorie van toelichting verantwoordt de regering de keuze voor een gewone methode door te stellen dat *'de intrusiviteit van een dergelijke methode (…) gering tot zeer gering is'*.

VI.4.8. PERSONELE EN FINANCIËLE MIDDELEN

Het Comité was van oordeel dat de tenuitvoerlegging van de diverse uitgewerkte maatregelen niet alleen een bijkomend beslag creëert op de capaciteit van de inlichtingendiensten, maar ook op deze van de betrokken toezichthoudende instanties. Het Comité beval zodoende aan dat een goedkeuring van het wetsontwerp gepaard zou gaan met een uitbreiding van het personeel van de BIM-Commissie en het Vast Comité I.

VI.5. ADVIES OVER DE STRAFBAARSTELLINGEN TER BEVORDERING VAN DE DEMOCRATISCHE WEERBAARHEID

In september 2021 bracht het Vast Comité I op verzoek van de Voorzitter van de Commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken van

316 Door deze methoden niet als BIM-methoden te kwalificeren heeft de wetgever ervoor gekozen om de controle niet te laten uitvoeren door de BIM-Commissie. Ze heeft daarentegen het Comité hiermee belast. Bij zijn MPLUS-controle heeft het Comité, als regulator van de nationale veiligheidszorg wat betreft de gegevensbescherming in dit domein, eveneens de bevoegdheid om bindende corrigerende maatregelen te nemen ten aanzien van alle persoonsgegevensverwerkingen van de inlichtingendiensten. Ten gevolge hiervan heeft het Comité bijvoorbeeld de bevoegdheid om in het kader van zijn MPLUS-controle een verwerkingsverbod of een gegevenswissing op te leggen.

de Kamer van volksvertegenwoordigers een advies uit over drie wetsvoorstellen, zijnde:

- Wetsvoorstel tot strafbaarstelling van het behoren tot of het samenwerken met een groepering die discriminatie of segregatie voorstaat;
- Wetsvoorstel tot wijziging van de wet van 29 juli 1934 waarbij de private milities verboden waren wat het verbod van ondemocratische groeperingen betreft ;
- Wetsvoorstel tot wijziging van de wet van 29 juli 1934 waarbij de private milities verboden warden, teneinde het in die wet vervatte verbod uit te breiden tot de verenigingen die aanzetten tot haat, discriminatie of geweld, en teneinde de ontbinding van die verenigingen door de uitvoerende macht mogelijk te maken.[317] [318]

De aan het Comité voor advies overgemaakte wetsvoorstellen strekten ertoe enkele nieuwe strafbaarstellingen in te voeren, met als overkoepelende doelstelling de bevordering van de democratische weerbaarheid. Het Comité beperkte zijn advies tot de aspecten van de betrokken wetsvoorstellen die een invloed hebben of kunnen hebben op de opdrachten en de werking van de inlichtingen- en veiligheidsdiensten.

VI.5.1. VOORAFGAANDE OBSERVATIE

Het Comité kon vooreerst vaststellen dat de voorgestelde strafbare gedragingen, in bepaalde gevallen, eveneens gekwalificeerd kunnen worden als dreigingen voor de nationale veiligheid, en dus overeenkomen met de activiteiten die door de VSSE, de ADIV en het OCAD dienen opgevolgd te worden. Betekenisvol is dat de strafbaarstelling van nationale veiligheidsdreigingen een invloed heeft op de werking van de vernoemde inlichtingen- en veiligheidsdiensten.

Immers, de VSSE heeft onder meer als opdracht het inwinnen, verwerken, analyseren en verspreiden van inlichtingen omtrent extremistische activiteiten die een gevaar vormen of kunnen vormen voor de nationale veiligheid. Ook de ADIV heeft als wettelijke taakstelling onderzoek te verrichten naar extremistische activiteiten ingeval hierin een militair aspect aanwezig is.

317 *Parl. St.* Kamer 2021-22, 55K450/001, 55K943/001 en 55K2024/001.

318 De drie wetsvoorstellen, nog hangende in de Kamer in april 2022, vormden in juni en juli 2021 het voorwerp van discussies in de Kamercommissie Binnenlandse Zaken. Een verslag van de debatten werd gepubliceerd in april 2022.

VI.5.2. SAMENWERKING EN UITWISSELING VAN INFORMATIE MET GERECHTELIJKE ACTOREN

Het Comité is van oordeel dat een (onrechtstreekse) uitbreiding van het strafrechtelijk arsenaal binnen de nationale veiligheidszorg de nood doet toenemen om te voorzien, op algemeen en geformaliseerde wijze, in een operationele samenwerking tussen het openbaar ministerie, de gerechtelijke politie, de VSSE, de ADIV en het OCAD.

Heden wordt deze operationele samenwerking en informatie-uitwisseling binnen het gerechtelijk ressort Brussel in belangrijke mate georganiseerd via het zogenaamde *Joint Intelligence Centre (JIC) /Joint Decision Centre (JDC)* systeem.[319] Het Comité adviseerde om te onderzoeken in welke mate het JIC/JDC-systeem dient uitgebreid te worden voor de opvolging van dreigingen andere dan terrorisme, meer in het bijzonder voor de opvolging van de strafbaarstellingen voorgesteld in de voor advies overgemaakte wetsvoorstellen. Aansluitend brengt het Comité in herinnering dat het JIC/JDC-systeem uitsluitend van toepassing is in het gerechtelijke ressort Brussel. Het Comité adviseerde te onderzoeken in welke mate dit systeem uitgebreid moet worden naar de andere ressorten. Gelet op zijn belang voor voorliggende aangelegenheid bracht het Comité tot slot de aanbeveling van de parlementaire onderzoekscommissie Terroristische Aanslagen in herinnering om een Kruispuntbank Veiligheid op te richten.

VI.5.3. SAMENWERKING EN UITWISSELING VAN INFORMATIE MET BESTUURLIJKE ACTOREN

De voorgestelde strafbaarstellingen raken in belangrijke mate de vrijheid van meningsuiting, de vrijheid van vereniging en de vrijheid van vergadering, aldus het Comité.

Het Comité herinnerde aan de wettelijke verplichtingen van de VSSE, de ADIV en het OCAD in het kader van de samenstelling van de lijsten van de door de politie op te volgen 'fenomenen' en op te volgen 'groeperingen' : krachtens artikel 44/5, §2 van de Wet op het politieambt (WPA) zijn de VSSE, de ADIV en het OCAD – logischerwijs samen met de Federale Politie – jaarlijks belast met het opstellen

[319] Het *Joint Intelligence Center* (JIC), samengesteld uit de Federale Gerechtelijke Politie Brussel (FGP Bxl), de Centrale Dienst Terrorisme binnen de federale politie (DJSOC/Terro), de VSSE, de ADIV en het OCAD, is belast met de structurele informatie-uitwisseling binnen de terrorismebestrijding. Het JIC is eveneens belast met de taak alle nieuwe inlichtingen in verband met de terroristische dreiging die verzameld werden door een van de partnerdiensten gemeenschappelijk te beoordelen en een voorstel te formuleren voor een geschikte opvolging (gerechtelijk/ inlichtingenopvolging/ andere opvolging). Het *Joint Decision Center* (JDC), samengesteld uit de vertegenwoordigers van de JIC-leden alsook het openbaar ministerie en de politionele bestuurlijke directeur-coordinator van Brussel, beslist vervolgens collegiaal over de opvolging.

van 'een gezamenlijk voorstel' aan de minister van Binnenlandse Zaken van een lijst met 'Fenomenen van bestuurlijke politie' alsook van een lijst van 'nationale en internationale groeperingen die de openbare orde zouden kunnen verstoren' en die politionele opvolging behoeven. De minister van Binnenlandse Zaken legt deze lijsten jaarlijks vast. In zijn advies beval het Comité aan te onderzoeken in welke mate de lijsten bedoeld in artikel 44/5, §2 WPA ingeschakeld moeten worden binnen de opvolging van de verboden organisaties en groeperingen bedoeld in de voor advies overgemaakte wetsvoorstellen.

VI.6. GEMEENSCHAPPELIJK ADVIES OP HET VOORONTWERP VAN WET TOT WIJZIGING VAN DE OCAD-WET

In augustus 2021 vroeg de minister van Binnenlandse Zaken, lnstitutionele Hervormingen en Democratische Vernieuwing alsook de Gegevensbeschermingsautoriteit aan de Vaste Comités P en I gevraagd om een gemeenschappelijk advies uit te brengen over het voorontwerp van wet tot wijziging van de wet van 10 juli 2006 betreffende de analyse van de dreiging (W.OCAD).[320] Op bepaalde plaatsen formuleerde het Vast Comité I opmerkingen in eigen naam.

VI.6.1. UITBREIDING VAN DE LIJST VAN ONDERSTEUNENDE DIENSTEN

Het voorontwerp van wet beoogt in de W.OCAD de vier overheidsdiensten die bij koninklijk besluit van 17 augustus 2018 als ondersteunende dienst van het OCAD werden aangewezen, wettelijk te verankeren.[321]

De W.OCAD stelt immers dat het koninklijk besluit dat overheidsdiensten op voorstel van de Nationale Veiligheidsraad aanwijst als ondersteunende dienst van het OCAD binnen een termijn van een jaar, te rekenen vanaf de datum van de inwerkingtreding van dit KB worden bekrachtigd door een wet. De Vaste Comités P en I merkten op dat in onderhavig geval hieraan niet werd voldaan. Het voorontwerp van wet komt deze situatie dus verhelpen, zonder daarbij de reden te vermelden voor de laattijdige tussenkomst van de regering.

---

320 Het wetsontwerp werd in februari 2022 in de Kamer neergelegd en in tweede lezing door de Commissie Binnenlandse Zaken op 3 mei 2022 goedgekeurd (Parl. St. Kamer, 2021-22, 55K2443).

321 Dit uitvoeringsbesluit werd genomen in uitvoering van art. 2, 1ste alinea, 2°, g) W.OCAD. Het gaat om de Dienst Erediensten en Vrijzinnigheid binnen het Directoraat-Generaal Wetgeving, fundamentele rechten en vrijheden van de FOD Justitie, het Directoraat-Generaal Penitentiaire inrichtingen van de FOD Justitie, de Algemene Directie Crisiscentrum van de FOD Binnenlandse zaken en de Algemene Administratie van de Thesaurie binnen de FOD Financiën.

Het Vast Comité I drong daarbij aan op een evaluatie van de wettelijke mogelijkheid om een overheidsdienst als ondersteunende dienst bij KB aan te wijzen. De vraag rijst immers of een door het OCAD opgestelde dreigingsevaluatie met een onwettigheid behept is ingeval deze (o.m.) gebaseerd is op informatie afkomstig van een bij KB aangewezen ondersteunende dienst die overgemaakt werd na het verstrijken van de termijn waarbinnen deze aanwijzing wettelijk moest bekrachtigd worden. In aanvullende orde stelt het Vast Comité I zich de vraag of een maatregel die steunt op een in dergelijke omstandigheden tot stand gekomen dreigingsevaluatie desgevallend onwettig is.

Het Vast Comité I formuleerde tevens een aantal specifieke observaties in verband met de dienst BELPIU, bij KB van 21 december 2017 ondergebracht bij de Algemene Directie Crisiscentrum van de Federale Overheidsdienst Binnenlandse Zaken.[322]

Het Vast Comité I bracht in herinnering dat het onderbrengen van deze dienst in de schoot van het Crisiscentrum geen enkele invloed heeft op het bestaande wettelijke kader rond de verwerking van passagiersgegevens door de dienst BELPIU. De memorie van toelichting laat uitschijnen dat de dienst BELPIU, ten gevolge van de aanduiding van het Crisiscentrum als ondersteunende dienst van het OCAD, eveneens (onrechtstreeks) onderworpen zou worden aan de samenwerkingsmodaliteiten uitgewerkt in de W.OCAD.

lndien er een nood bestaat om de dienst BELPIU als ondersteunende dienst van het OCAD aan te duiden dan dienen zowel de W.OCAD als de Wet van 25 december 2016 aangepast te worden.

Daarnaast is er problematiek van de verhouding tussen de werkzaamheden van het OCAD in zijn hoedanigheid van operationeel verantwoordelijke van de Gemeenschappelijke Gegevensbank (GGB) Terrorist Fighters en de GGB Haatpropagandisten *(cf.* de artikelen 44/11/3bis ev. WPA) enerzijds, en het OCAD in zijn hoedanigheid van dreigingsevaluatieorgaan anderzijds *(cf.* de Wet van 10 juli 2006).

322 Artikel 2 van het koninklijk besluit ter uitvoering van de wet van 25 december 2016 betreffende de verwerking van de passagiersgegevens, houdende de verplichtingen opgelegd aan de luchtvaartmaatschappijen.

VI.6.2. WIJZIGINGEN VAN DE BENOEMINGSVOORWAARDEN VOOR DIRECTEUR EN ADJUNCT-DIRECTEUR

Het wetsvoorstel veranderde een van de voorwaarden om als directeur en adjunct-directeur van het OCAD aangewezen te worden, met name het bezit van de hoedanigheid van magistraat.

Het Vast Comité I onderschrijft dat het schrappen van de vereiste hoedanigheid van magistraat het aantal mogelijke kandidaten zal doen toenemen, maar formuleerde een aantal bedenkingen met in het achterhoofd de complexe juridische omgeving waarin het OCAD zich begeeft. De vraag rijst of de vervangende aanwijzingsvoorwaarde van 'bijkomende juridische expertise' in hoofde van de directeur en adjunct-directeur niet veeleer theoretisch van aard is, dan dat deze daadwerkelijk afdoende is om de schrapping van de hoedanigheid van magistraat te compenseren in het licht van het respecteren van een balans tussen de operationele behoeften van het OCAD en het belang van het respecteren en kennis hebben van de geldende regelgeving. Het Vast Comité I stelde vast dat in het licht van het schrappen van de benoemingsvoorwaarde van magistraat, het wetsontwerp geen bepalingen toevoegt aan de Wet van 10 juli 2006 ter bescherming van de onafhankelijkheid en onpartijdigheid van de leiding van het OCAD. Een dergelijk kader is evenwel noodzakelijk voor de onafhankelijkheid en onpartijdigheid van de werkzaamheden van het OCAD, o.m. binnen de uitvoering van de dreigingsevaluaties en het bepalen van het betrokken dreigingsniveau.

VI.6.3. UITBREIDING VAN DE OPDRACHTEN VAN HET OCAD

Het voorontwerp van wet beoogt nieuwe opdrachten voor het OCAD in te schrijven in artikel 8 van de wet van 10 juli 2006.

VI.6.3.1. Het coördineren van de globale aanpak tegen dreigingen

Deze bepaling voorziet in een coördinerende rol voor het OCAD in de globale aanpak tegen de dreigingen bedoeld in artikel 3 W.OCAD. De memorie van toelichting stelde dat dit een consolidatie betreft van een reeds bestaande praktijk.

De Vaste Comités P en I stellen echter vast dat de inhoud van deze coördinerende rol niet verder verduidelijkt wordt. De memorie van toelichting blijft vaag wat betreft de omschrijving ervan en beperkt zich tot een niet-limitatieve opsomming van voorbeelden zoals de interactie tussen de Lokale Task Forces (LTF's) en de Lokale lntegrale Veiligheidscellen inzake radicalisme, extremisme en terrorisme (LIVC's-R), de optimalisering van de Gemeenschappelijke gegevensbank. Volgens de Comités verdiende de aanbeveling om de opdracht van het OCAD inzake het coördineren van de globale aanpak tegen dreigingen te verduidelijken. Immers, het

OCAD heeft geen operationeel arsenaal ter beschikking om de dreigingen daadwerkelijk en globaal aan te pakken.

Het Vast Comité I stelde tevens vast dat het ontwerp verwarring creëerde met betrekking tot verschillende wettelijke kaders die de opdrachten van het OCAD vastleggen.[323] Volgens het Comité is er verduidelijking nodig in de verhouding tussen de voedingsplicht in hoofde van de 'basisdiensten' en de 'partnerdiensten'[324] en de meldingsplicht aan het OCAD voor de 'ondersteunende diensten van het OCAD'. De uitbreiding van de meldingsplicht naar alle nieuwe opdrachten van het OCAD creëert immers onduidelijkheid.

Daarenboven was volgens het Vast Comité I verduidelijking vereist over de gewijzigde meldingsplicht en de mate waarin de leden van de LIVC's-R verplicht zijn om informatie te verstrekken aan het OCAD, en bij uitbreiding, of de betrokken LIVC-R-leden persoonsgegevens mogen verstrekken aan het OCAD.

VI.6.3.2. Nieuwe opdrachten voor het OCAD van de Nationale Veiligheidsoverheid?

Verder voorziet het voorontwerp dat het OCAD, behalve de exhaustieve lijst van opdrachten die de dienst wettelijk zijn toebedeeld, desgevallend nieuwe opdrachten binnen zijn bevoegdheidsgebied kan krijgen van de Nationale Veiligheidsraad. Deze nieuwe opdrachten zouden dan verduidelijkt worden via een koninklijk besluit overlegd in de Ministerraad. Nu de uitbreiding van de lijst van de ondersteunende diensten bekrachtigd moet worden door een wet, is daarentegen geen dergelijke bekrachtiging vereist voor wat betreft de uitbreiding van de opdrachten van het OCAD en volstaat een KB dat in de Ministerraad overlegd werd. Het advies bracht dit verschil in benadering binnen dezelfde wet op de voorgrond.

Het Vast Comité I adviseerde verder om de term 'bevoegdheidsgebied van het OCAD' in betrokken bepaling nader te verduidelijken. Er bestaat in hoofde van het OCAD immers geen bevoegdheidsgebied dat uniform is voor al zijn opdrachten.[325]

---

323 In het bijzonder de W.OCAD, de regelgeving aangaande de gemeenschappelijke gegevensbanken en de Wet tot oprichting van de LIVC-R.

324 Artikelen 44/2, §2 en *44/11/3ter,* §4 WPA *i.o.* artikel 7, §1, eerste lid van het Koninklijk besluit van 21 juli 2016 KB Terrorist Fighters en artikel 7, §1, eerste lid KB Haatpropagandisten. Zie tevens de omzendbrief van 22 mei 2018 van de minister van Veiligheid en Binnenlandse Zaken en de minister van Justitie 'betreffende de informatie-uitwisseling rond en de opvolging van terrorist fighters en haatpropagandisten' (omzendbrief Terrorist fighters en haatpropagandisten). Ook het College van procureurs-generaal van het Openbaar Ministerie heeft enkele omzendbrieven uitgebracht tot regeling van deze aangelegenheid: COL 10/2015 'betreft: Gerechtelijke aanpak inzake de foreign terrorist fighters', COL 21/2016 'betreft: Gerechtelijke aanpak van haatpredikers' en COL 22/2016 'betreft: Gemeenschappelijke gegevensbank Foreign Terrorist Fighters'.

325 Bij wijze van voorbeeld, heeft de W.OCAD het over terrorisme, extremisme, inbegrepen het radicaliseringsproces terwijl de Wet op het politieambt (WPA) het dan weer heeft over terrorisme en extremisme dat tot terrorisme kan leiden.

Er wordt tevens voorgesteld de meldingsplicht van de steundiensten uit te breiden naar alle nieuwe opdrachten van het OCAD. In deze logica, zullen de steundiensten verplicht worden om alle inlichtingen waarover ze beschikken over te maken aan het OCAD wanneer deze relevant zijn voor OCADopdrachten. Hieronder vallen eveneens persoonsgegevens. In het licht van het grondrecht op bescherming van de persoonlijke levenssfeer, zoals vastgelegd in artikel 22 van de Grondwet, herinnerde het advies aan het feit dat overmaken van persoonsgegevens te allen tijde een regeling behoeft die wordt vastgelegd in een formele wet waarin minstens de basisregels en -doelstellingen vastgelegd worden.

VI.6.4. MEDEDELING EN CONSULTATIE VAN EVALUATIES

Het voorontwerp van wet houdt tevens een wijziging in voor wat betreft de voorwaarden en modaliteiten van de mededeling door het OCAD van strategische en punctuele evaluaties of evaluaties op verzoek van steundiensten. Wat dat betreft, wezen de Vaste Comités I en P op een aantal (voornamelijk taalkundige) incoherenties en suggereerden alternatieve formuleringen.

VI.6.5. MEDEDELING EN CONSULTATIE VAN INLICHTINGEN VAN GERECHTELIJKE AARD ONDER EMBARGO[326]

Het voorontwerp beoogde tevens wijzigingen aan te brengen in de W.OCAD door te voorzien dat de directeur van het OCAD niet de enige is binnen het OCAD die bestemmeling kan zijn van inlichtingen van gerechtelijke aard onder embargo, maar dat deze ook worden toegestuurd aan de bevoegde leden van het OCAD die door hem worden aangewezen om een *ad hoc* evaluatie te maken met de inlichtingen onder embargo.

De Vaste Comités P en I adviseerden de ontwerpers om in het voorontwerp van wet uitdrukkelijk te voorzien dat de kennisname van deze inlichtingen onder embargo door de aangewezen personeelsleden van het OCAD strikt noodzakelijk is voor de uitoefening van hun functie in het kader van de opdrachten van het OCAD.[327] De Comités raadden ook aan om uitdrukkelijk op te nemen dat de directeur van het OCAD ertoe gehouden is een lijst op te stellen van de aangewezen personeelsleden die toegang krijgen tot deze inlichtingen en deze lijst ter beschikking te houden van de Vaste Comités P en I.

---

326 Zie hierover: VAST COMITÉ I, *Activiteitenrapport 2008*, 110.

327 En dus zoals in de Franse versie van de memorie van toelichting werd opgenomen, ze een strikte *'need to know'* hebben.

VI.6.6. MEDEDELING EN CONSULTATIE VAN INLICHTINGEN BEDOELD IN ARTIKEL 12, 1STE LID W.OCAD

Het voorontwerp van wet beoogt dezelfde aanpassingen in te voegen voor wat betreft de inlichtingen onder embargo aangeleverd door de inlichtingen- en veiligheidsdiensten, de Administratie Douane en Accijnzen van de FOD Financiën en de FOD Buitenlandse zaken, die afkomstig zijn van een gelijkaardige buitenlandse dienst die uitdrukkelijk gevraagd heeft deze niet aan andere diensten tot te zenden, of waarvan de toezending de veiligheid van een menselijke bron in gevaar kan brengen.

De Comités adviseerden dan ook hier uitdrukkelijk te voorzien dat de kennisname van deze inlichtingen onder embargo door de aangewezen personeelsleden van het OCAD strikt noodzakelijk is voor de uitoefening van hun functie alsook dat de directeur van het OCAD ertoe gehouden is een lijst op te stellen van de aangewezen personeelsleden die toegang krijgen tot deze inlichtingen en deze lijst ter beschikking te houden van de Vaste Comités P en I.

HOOFDSTUK VII.

DE OPSPORINGS- EN GERECHTELIJKE ONDERZOEKEN

De Dienst Enquêtes I van het Comité doet in opdracht van de gerechtelijke overheden ook onderzoeken naar leden van de inlichtingen- en veiligheidsdiensten en het Coördinatieorgaan voor de dreigingsanalyse (OCAD)[328] die verdacht worden van een misdaad en/of wanbedrijf. Deze bevoegdheid staat omschreven in artikel 40, derde lid van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse (W.Toezicht).

Wanneer zij een opdracht van gerechtelijke politie vervullen, staan de leden en de directeur van de Dienst Enquêtes I onder het toezicht van de procureur-generaal bij het hof van beroep of van de federaal procureur (art. 39 W.Toezicht) en heeft het Vast Comité I geen zeggenschap over hen. De voorzitter van het Vast Comité I moet er echter zorg voor dragen dat de uitvoering van de opdrachten van gerechtelijke politie de uitvoering van de toezichtonderzoeken niet hindert. De reden daarvoor ligt voor de hand: het controleorgaan heeft vele andere wettelijke opdrachten. Deze opdrachten zouden in het gedrang kunnen komen indien een te aanzienlijk deel van de tijd zou besteed worden aan gerechtelijke dossiers. De voorzitter kan in dat geval overleg plegen met de gerechtelijke autoriteiten over de inzet van de leden van de Dienst Enquêtes I in strafonderzoeken (art. 61*bis* W.Toezicht).

In de gevallen waarin de Dienst Enquêtes I strafonderzoeken voert, moet de directeur na het afronden van dit onderzoek verslag uitbrengen bij het Vast Comité I. In dat geval '*beperkt het verslag zich evenwel tot de informatie die nuttig is voor de uitoefening door het Vast Comité I van zijn opdrachten*' (art. 43, derde lid, W.Toezicht).

In 2021 voerde de Dienst Enquêtes I onderzoeksdaden uit in het kader zes opsporingsonderzoeken: vier onder leiding van het Federaal Parket, één onder leiding van het Arbeidsauditoraat van Luik en een laatste bij de procureur des Konings van Brussel. Vijf van de dossiers betroffen mogelijks leden van de Algemene Dienst Inlichting en Veiligheid, één dossier had mogelijks betrekking op leden van de Veiligheid van de Staat. In het kader van deze dossiers kreeg de Dienst

[328] Wat betreft de leden van de andere 'ondersteunende diensten' van het OCAD geldt deze bepaling alleen ten aanzien van de verplichting om relevante inlichtingen aan het OCAD mee te delen (artt. 6 en 14 W.OCAD).

Enquêtes I zes apostilles, waarvan er vier konden worden afgesloten. In totaal werden 10 processen-verbaal en 11 vertrouwelijke rapporten opgesteld. De beoogde strafbare feiten betroffen de 'schending van het beroepsgeheim', 'valsheid in geschrifte' en 'onrechtmatige toegang tot gegevensbanken'.

Verder stelt artikel 50 W.Toezicht dat *'[e]lk lid van een politiedienst dat een misdaad of een wanbedrijf gepleegd door een lid van een inlichtingendienst vaststelt, maakt daarover een informatief verslag op en bezorgt dat binnen de vijftien dagen aan het hoofd van de Dienst Enquêtes I'*. De enquêtedienst ontving in 2021 geen meldingen in die zin.

HOOFDSTUK VIII.
EXPERTISE EN EXTERNE CONTACTEN

VIII.1. EXPERT OP DIVERSE FORA

Leden van het Vast Comité I en van zijn personeel werden in 2021 diverse malen als expert geconsulteerd door binnen- en buitenlandse publieke en private instellingen:

- De dienstdoend griffier van het Vast Comité I werd uitgenodigd in het kader van het opleidingsonderdeel 'Intelligence' van de Master in de Internationale betrekkingen en de diplomatie (Universiteit Antwerpen) om er de werking van het Comité toe te lichten. De uiteenzetting gebeurde via teleconferentie;
- Er werd door medewerkers van het Comité verschillende artikelen gepleegd in wetenschappelijke tijdschriften[329];
- De voorzitter werd in mei 2021 gevraagd deel uit te maken van het selectiecomité voor de aanduiding van een plaatsvervangend lid voor de BIM-Commissie. Doelstelling van deze selectie en de selectiecommissie was het verzamelen van nuttige informatie omtrent de kandidaten zodat een gemotiveerd advies kon worden gegeven aan de minister van Justitie;
- In juni 2021 trad de voorzitter, op verzoek van de *Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, op als moderator voor de RightsCon, 's werelds toonaangevende conferentie over mensenrechten in het digitale tijdperk. Het thema betrof '*When States of Emergency Collide: COVID-19, Counter-Terrorism and Transnational Data Flows*' en werd in samenspraak met het AWO Agency georganiseerd;
- Er vonden videoconferenties plaats tussen juristen van het Vast Comité I en vertegenwoordigers van het Federaal Instituut Mensenrechten (infra) over de actieve kennisgevingsplicht naar aanleiding van de toepassing van bijzondere inlichtingenmethoden;

---

329 F. GIVRON, en S. LIPSZYC, 'Le contentieux en matière de sécurité et son instance spécifique : l'Organe de recours en matière d'habilitations, attestations et avis de sécurité. La recherche de l'équilibre entre la protection des droits de la défense et la préservation des intérêts majeurs de l'État', *J.T.*, 2021/3, 45-53; W. VAN LAETHEM, 'Problemen met veiligheidsadvies van beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen', *Juristenkrant*, 2021, 439, 8-9 ; B. VERSCHAEVE, 'Het Incident Respons Team van de Staatveiligheid. De interne beveiligingsdienst van de burgerlijke inlichtingendienst toegelicht', *Politie en Recht*, nr 1, 2022, 3-20.

- Er vonden gedachtenuitwisselingen plaats met academici (Universiteit Antwerpen) over het stijgend belang van informatie van inlichtingen- en veiligheidsdiensten binnen de motivering van allerhande soorten bestuursbeslissingen;
- In september 2021 werd de dienstdoend griffier uitgenodigd om een uiteenzetting te geven over het theoretisch kader van veiligheidsscreenings in België tijdens een besloten studiedag. Deze werd georganiseerd voor academici en vertegenwoordigers vanuit de inlichtingenwereld en de kritieke infrastructuren. Het geheel paste in een doctoraatsthesis over *insider threat* (Universiteit Antwerpen);
- Nog in september nam het Comité, op verzoek van de minister van de regering van de Federatie Wallonië-Brussel bevoegd voor justitiehuizen, deel aan een meeting over de uitwisseling van informatie tussen de justitiehuizen, het Coördinatieorgaan voor de dreigingsanalyse (OCAD) en de Veiligheid van de Staat (VSSE).
- De Directeur van de Dienst Enquêtes werd ingeschakeld in een opleidingsmoment voor de rekruten bij de ADIV;
- In oktober 2021 sprak de voorzitter van het Vast Comité I op de derde *European Intelligence Oversight Conference* in Rome.[330]
- Een medewerkster van het Vast Comité I finaliseerde haar doctoraat en behaalde in december 2021 de titel van Doctor in de politieke en sociale wetenschappen (UCLouvain, Saint-Louis-Bruxelles).[331]

VIII.2. SAMENWERKINGSPROTOCOL MET DE FEDERALE OMBUDSMANNEN

De Wet van 15 september 2013[332] duidt de Federale Ombudsmannen[333] aan als centraal meldpunt voor veronderstelde integriteitsschendingen in de federale administratieve overheden. In september 2021 werd het 'Samenwerkingsprotocol van 7 oktober 2021 voor de relaties tussen de Federale Ombudsmannen en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van de Wet van 15 september 2013' afgesloten. Het protocol beoogt de samenwerkingsmodaliteiten te regelen tussen de Federale Ombudsmannen en het Comité

330 De titel van zijn uiteenzetting luidde: *'European case law on the notification of secret measures and the Belgian response with particular attention to the future rol of the Standing Committee R'.*

331 C. THOMAS, *Une menace possible et vraisemblable. Dire et faire la sécurité: l'Organe de Coordination pour l'Analyse de la Menace et la structuration du champ antiterroriste belge*, Bruxelles, UCLouvain – Saint-Louis Bruxelles, septembre 2021, 470 p.

332 Wet van 15 september 2013 betreffende de melding van een veronderstelde integriteitsschending in de federale administratieve overheden door haar personeelsleden, *BS* 14 oktober 2013.

333 Wet van 22 maart 1995 tot instelling van de federale ombudsmannen, *BS* 7 april 1995.

wanneer een veronderstelde integriteitsschending in één van beide inlichtingendiensten wordt gesignaleerd bij de Ombudsman.

In voorkomend geval kan deze laatste aan het Vast Comité I vragen om een lid van de Dienst Enquêtes aan te duiden om het Centrum voor Integriteit – een centraal meldpunt opgericht in de schoot van de Federale Ombudsmannen – bij te staan als deskundige bij de uitvoering van het onderzoek. In het protocol werden verder afspraken gemaakt over de onderzoeksmiddelen, het beroepsgeheim, de vertrouwelijkheid en de uitwisseling van *best practices*.

VIII.3. PARTNERSHIP MET HET FEDERAAL INSTITUUT MENSENRECHTEN

Met de Wet van 12 mei 2019 werd het Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens (FIRM) opgericht.[334] Middels een samenwerkingsprotocol kwamen alle deelnemende instanties overeen om praktijken en methoden uit te wisselen, om gemeenschappelijke kwesties te onderzoeken en om de onderlinge samenwerking te bevorderen. In het kader van het uitwerken van een eerste strategisch plan, werden de partner-mensenrechtenactoren om hun inbreng verzocht. Het Comité werd eveneens om een gedachtewisseling verzocht door vertegenwoordigers van het FIRM in het kader van de realisatie van een alternatief rapport voor het VN-Antifoltercomité (CAT). Dit had onder meer betrekking op '*extraordinary renditions*'[335], en viel dus binnen het mandaat van het Vast Comité I.

VIII.4. EEN MULTINATIONAAL INITIATIEF INZAKE INTERNATIONALE INFORMATIE-UITWISSELING

De toegenomen internationale gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten brengt uitdagingen mee voor de nationale toezichtorganen. De toezichtorganen van (oorspronkelijk) vijf Europese landen (België, Denemarken, Nederland, Noorwegen en Zwitserland) overleggen daarom sinds enkele jaren om het hoofd te bieden aan die uitdagingen door werkwijzen te vinden om het risico op een hiaat in het toezicht te verkleinen. Na verloop van tijd werd een nieuwe partner betrokken in dit project, namelijk het *Investigatory Powers Commissioner's Office (IPCO)* uit het Verenigd Koninkrijk. De groep werd herdoopt tot *Intelligence Oversight Working Group (IOWG)* en in 2019 uitgebreid met drie waarnemers, te weten de *Swedisch Foreign Intelligence Inspectorate (Statens inspektion av försvar-*

334 Wet van 12 mei 2019 tot oprichting van een Federaal Instituut voor de bescherming en de bevordering van de rechten van de mens, B.S. 21 juni 2019.

335 Hierover in extenso: VAST COMITÉ I, *Activiteitenverslag 2006*, 34-41 ('II.2. De CIA-vluchten').

underättelse-verksamhet (SIUN)), de *Swedish Board of Inventions (Statens uppfinnarnämnd, (SUN))* en de Duitse *G10 Commission*.

Tengevolge de beperkingen omwille van COVID-19, bleven de internationale activiteiten in 2021 beperkt. In september 2021 vond een door het Zwitserse toezichtorgaan *Autorité de surveillance indépendante des activités de renseignement* (AS-Rens) georganiseerde virtuele vergadering plaats waarop de toekomst van de IOWG stond geagendeerd. Ook werd overleg gepleegd over de wijze waarop de toezichthouders omgingen met de pandemie en de nieuwe technologische ontwikkelingen op het vlak van *intelligence*. In 2022 wordt deze samenwerking geïntensiveerd.

VIII.5. CONTACTEN MET BUITENLANDSE TOEZICHTHOUDERS

In oktober 2021 vond de derde *European Intelligence Oversight Conference* in Rome plaats bij de Italiaanse toezichthouder, de *Procura Generale della Corte di Cassazione*. De conferentie agendeerde thema's als '*The developments in the light of European Case Law*', *'Bulk data collection and targeted interceptions'* en *'International cooperation and other oversight developments in the light of the revised Convention 108+'*.

In het verlengde van een vragenlijst over '*ex ante oversight*', lanceerde de Nederlandse toezichthouder CTIVD (Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten) in juli 2020 een gelijkaardig initiatief. Het betrof een vragenlijst over *complaint handling* (klachtenbehandeling). Het doel van dit initiatief was de beste praktijken in Europa op het gebied van klachtenbehandeling te verzamelen en te analyseren met de betrachting deze vervolgens te kunnen verbeteren. Ook het Vast Comité I leverde hiertoe zijn inhoudelijke bijdrage.

Het Vast Comité I behield zijn voornemen om, samen met de Zwitserse *Autorité de surveillance indépendante des activités de renseignement* (AS-Rens), over te gaan tot de – zij het kortstondige – uitwisseling van personeelsleden in het kader van een stage. Na een opschorting als gevolg van de coronacrisis is deze uitwisseling gepland in de loop van 2022.

De *Danish Intelligence Oversight Board* deelde met de Belgische en andere Europese toezichthouders zijn '*Standards for Danish intelligence oversight activities*'.

Met de Luxemburgse *Cour administrative* ten slotte, werd informatie uitgewisseld over de wetgeving aangaande het gebruik van geclassificeerde stukken in het kader van veiligheidsmachtigingen.

HOOFDSTUK IX.

HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN[336]

Dit hoofdstuk omvat het op 20 mei 2020 goedgekeurde activiteitenverslag van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen alsook een aantal opmerkingen en suggesties van de voorzitter van dit rechtscollege.

IX.1. HET ACTIVITEITENVERSLAG VAN HET BEROEPSORGAAN

IX 1.1. INLEIDING

Het Beroepsorgaan[337] is in België het enige administratief rechtscollege dat bevoegd is voor geschillen die betrekking hebben op administratieve beslissingen in verschillende domeinen: veiligheidsmachtigingen, veiligheidsattesten en, tot slot, veiligheidsadviezen.

Daarnaast kan het Beroepsorgaan ook optreden als 'annulatierechter' tegen beslissingen van publieke of administratieve overheden om in een bepaalde sector, voor een bepaalde plaats of voor een bepaald evenement veiligheidsattesten of -adviezen aan te vragen.[338]

Het Beroepsorgaan is samengesteld uit de voorzitters van het Vast Comité I, het Vast Comité P en de Geschillenkamer van de Gegevensbeschermingsautoriteit (GBA). Als ze verhinderd zijn, kunnen de drie voorzitters worden vervangen

---

336 Dit activiteitenverslag voert artikel 13 uit van de Wet van 11 december 1998 tot oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, waarin wordt bepaald dat het Beroepsorgaan een jaarverslag moet opstellen.

337 GIVRON, F. en LIPSZYC, S., 'Le contentieux en matière de sécurité et son instance spécifique : l'Organe de recours en matière d'habilitations, attestations et avis de sécurité. La recherche de l'équilibre entre la protection des droits de la défense et la préservation des intérêts majeurs de l'État', *J.T.*, 2021/3, 45-53.

338 Voor meer informatie, zie VAST COMITÉ I, *Activiteitenverslag 2006*, 87-120 en VAST COMITÉ I, *Activiteitenverslag 2018*, 111-124.

door een effectief lid-raadsheer van de instelling waartoe de betrokken voorzitter behoort.

De voorzitter van het Vast Comité I neemt het voorzitterschap van het Beroepsorgaan waar. De functie van griffier wordt uitgeoefend door de griffier van het Vast Comité I; het personeel van de griffie is het door het Comité aangestelde personeel. De activiteiten van het Beroepsorgaan vormen al meer dan twintig jaar een perfect voorbeeld van synergie binnen bepaalde satellietinstellingen van het parlement. De samenstelling van het Beroepsorgaan levert bovendien een multidisciplinaire bijdrage aan de beraadslaging betreffende elk dossier.

Op te merken valt dat de administratie en de opvolging van de beroepen integraal ten laste is van het Vast Comité I. Het Comité stelt immers alle personen en middelen ter beschikking die nodig zijn om de administratie, de briefwisseling, het houden van hoorzittingen en het opstellen van de beslissingen voor zijn rekening te nemen. Het gaat daarbij enerzijds om de terbeschikkingstelling van de voorzitter en zijn plaatsvervangende leden en de griffier, maar ook de juristen als '*toegevoegde griffiers*' en het administratief personeel die de griffie van dit administratief rechtscollege vormen. Anderzijds neemt het Vast Comité I in zijn begroting ook de kosten van de kantoren op zich als werkingskosten van het Beroepsorgaan.

Het Beroepsorgaan heeft alle maatregelen getroffen die nodig zijn om zijn werking te garanderen en dit ondanks de COVID-19-pandemie. Zo bleef het Beroepsorgaan zijn hoorzittingen houden à rato van minimaal twee per maand. In 2021 vonden er dertighoorzittingen plaats.[339]

IX.1.2. GEDETAILLEERDE CIJFERS

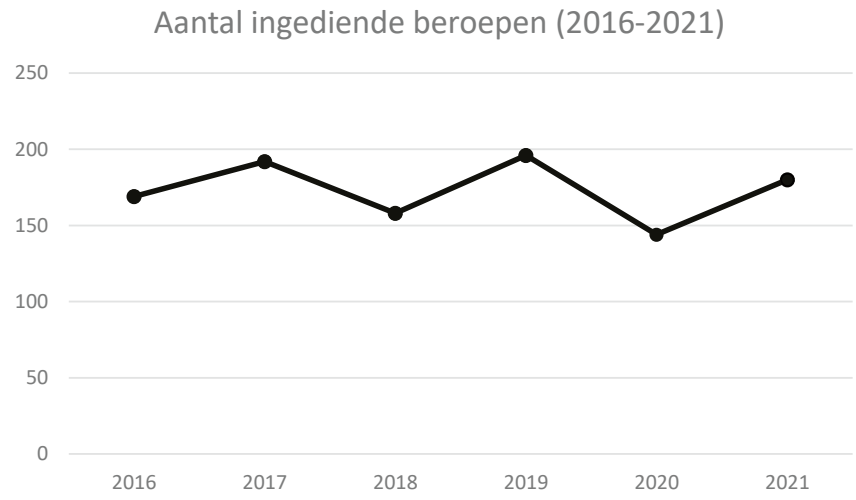
In dit onderdeel worden de aard van de bestreden beslissingen, de hoedanigheid van de bevoegde overheden en de verzoekers, en de aard van de beslissingen van het Beroepsorgaan binnen de verschillende beroepsprocedures cijfermatig weergegeven. Om enige vergelijking mogelijk te maken, werden de cijfers van de vijf vorige jaren eveneens opgenomen.

In 2021 werden 180 beroepen ingesteld tegenover 144 in 2020 en 196 in 2019 (*infra*). Deze cijfers sluiten aan bij het economisch herstel en de vraag naar veiligheidsadviezen, in het bijzonder in de luchtvaartsector en voor de kandidaten voor Defensie.

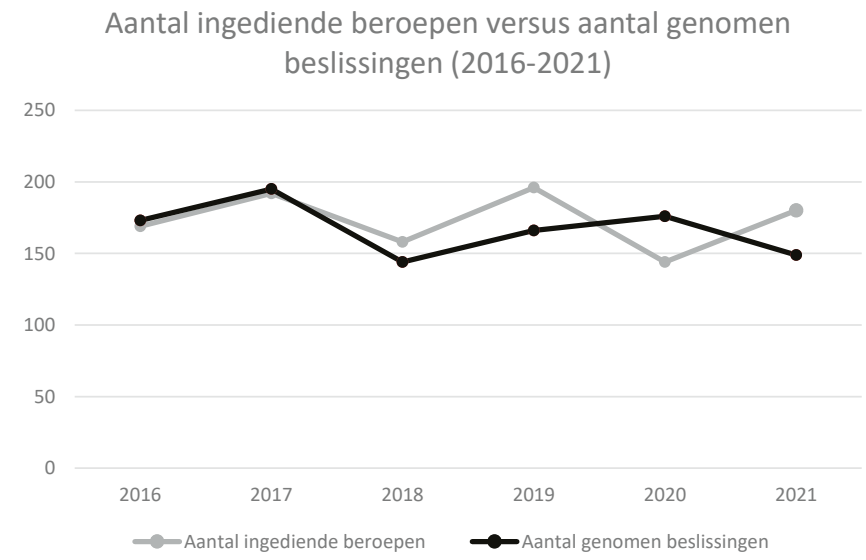
Er zijn 149 definitieve beslissingen genomen.

339 13 in het Nederlands en 17 in het Frans.

Tabel 1. Aantal ingediende beroepen (2016-2021)



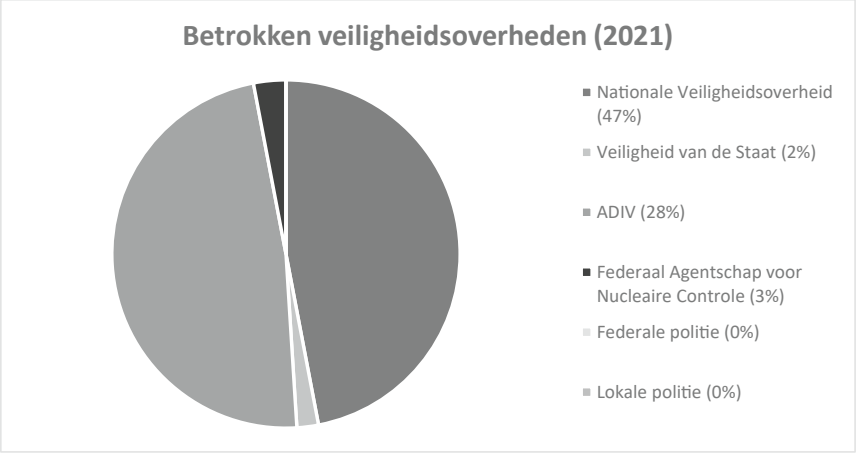
Tabel 2. Aantal ingediende beroepen versus aantal verleende beslissingen (2016-2021)



Tabel 3. Betrokken veiligheidsoverheden (2016-2021)

	2016	2017	2018	2019	2020	2021
Nationale Veiligheidsoverheid	92	129	113	114	91	86
Staatsveiligheid	0	0	0	0	0	4
Algemene Dienst Inlichting en Veiligheid	68	53	32	61	41	84
Federaal Agentschap voor Nucleaire Controle	8	7	10	17	7	6
Federale politie	1	3	3	3	4	0
Lokale politie	0	0	0	1	1	0
TOTAAL	**169**	**192**	**158**	**196**	**144**	**180**

Onderstaande grafiek toont de verdeling van de betrokken veiligheidsoverheden in 2021.



Tabel 4. Aard van de bestreden beslissingen

	2016	2017	2018	2019	2020	2021
Veiligheidsmachtigingen (Art. 12 e.v. W.C&VM)						
Vertrouwelijk	5	1	2	5	0	2
Geheim	38	33	31	39	27	50
Zeer geheim	7	6	3	7	5	8
Weigering	28	30	26	39	23	37
Intrekking	9	7	4	16	8	17
Weigering en intrekking	0	0	0	0	0	4
Machtiging voor beperkte duur	4	1	1	3	0	1
Machtiging voor een lager niveau	1	0	0	0	0	
Geen beslissing binnen de termijn	7	2	5	0	0	1
Geen beslissing binnen de verlengde termijn	1	0	0	0	0	0
Andere					1[340]	
SUBTOTAAL VEILIGHEIDSMACHTIGINGEN	**50**	**40**	**36**	**51**	**32**	**60**
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)						
Weigering	1	3	3	1	0	3
Intrekking	0	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	0	0	0	

340 'Waarschuwing van de verzoeker'. Aan een persoon werd de veiligheidsmachtiging voor een periode van vijf jaar met een waarschuwing toegekend. De betrokkene heeft beroep ingesteld tegen deze waarschuwing.

	2016	2017	2018	2019	2020	2021
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)						
Weigering	9	20	15	12	6	2
Intrekking	0	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	0	0	0	1
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)						
Weigering	7	7	11	17	7	6
Intrekking	1	0	0	0	0	0
Geen beslissing binnen de termijn	0	0	1	0	0	0
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)						
Negatief advies	101	122	92	115	99	108
Geen advies	0	0	0	0	0	0
Herroeping van positief advies	0	0	0	0	0	0
Normatieve rechtshandelingen van een administratieve overheid (Art. 12 W.Beroepsorgaan)						
Beslissing van een overheidsinstantie om veiligheidsattesten te eisen	0	0	0	0	0	0
Weigering van de NVO om verificaties voor veiligheidsattesten te verrichten	0	0	0	0	0	0

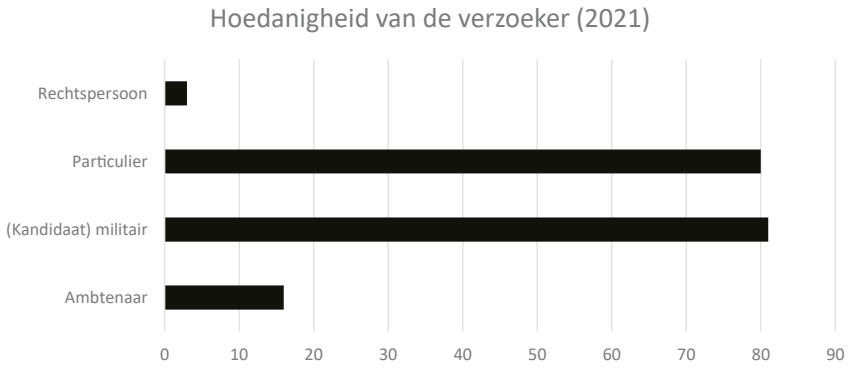
	2016	2017	2018	2019	2020	2021
Beslissing van een administratieve overheid om veiligheidsadviezen te eisen	0	0	0	0	0	0
Weigering van de NVO om verificaties voor veiligheidsadviezen te verrichten	0	0	0	0	0	0
SUBTOTAAL ATTESTEN EN ADVIEZEN	119	152	122	145	112	120
TOTAAL BESTREDEN BESLISSINGEN	**169**	**192**	**158**	**196**	**144**	**180**

Tabel 5. Hoedanigheid van de verzoeker

	2016	2017	2018	2019	2020	2021
Ambtenaar	2	4	5	4	8	16
(kandidaat) Militair	23	20	8	27	39	81
Particulier	139	164	140	163	95	80
Rechtspersoon	5	4	5	2	2	3

Onderstaande grafiek toont de verdeling volgens de 'hoedanigheid van de verzoeker' in 2021.

Tabel 6. Taal van de verzoeker



	2016	2017	2018	2019	2020	2021
Franstalig	99	115	83	101	83	86 (1)
Nederlandstalig	70	77	75	95	61	94 (2)
Duitstalig	0	0	0	0	0	0
Anderstalig	0	0	0	0	0	0

(1) 86 Franstalige dossiers in 2021 + 29 Franstalige dossiers van de vorige jaren maar behandeld in 2021 = 115 Franstalige verzoekers

(2) 94 Nederlandstalige dossiers in 2021 + 18 Nederlandstalige dossiers van de vorige jaren maar behandeld in 2021 = 112 Nederlandstalige verzoekers

Tabel 7. Handelingen van de griffie

	2016	2017	2018	2019	2020	2021
Volledig dossier opvragen (1)	167	191	154	191	141	180
Vraag om bijkomende informatie (2) en herinneringen verstuurd naar de veiligheidsoverheden (3) *	23	36	12	39	41	45

(1) Het Beroepsorgaan kan het gehele dossier opvragen bij de veiligheidsoverheden. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan door de griffie.

(2) Het Beroepsorgaan beschikt over de mogelijkheid om tijdens de procedure aanvullende informatie die het nuttig acht, op te vragen. In de praktijk neemt de griffie de taak op zich om de overheden te vragen de dossiers te vervolledigen.

(3) Art. 6 van het KB Beroepsorgaan bepaalt de termijnen voor de aanlevering van de dossiers door de veiligheidsoverheden. Die termijnen vangen aan wanneer de griffier een kopie van het beroep naar de betrokken veiligheidsoverheid stuurt. Ze variëren naargelang de aard van de betwiste handeling. Zo moet de veiligheidsoverheid haar dossier aanleveren binnen de 15 dagen voor veiligheidsmachtigingen, binnen de 5 dagen voor veiligheidsattesten en binnen de 10 dagen als het beroep betrekking heeft op een veiligheidsadvies. Wanneer die termijnen niet worden nageleefd, legt de griffie de nodige contacten. Deze gegevens worden geregistreerd vanaf 2019.

Tabel 8. Voorbereidende gerechtelijke handelingen van het Beroepsorgaan [341]

	2016	2017	2018	2019	2020	2021
Horen van een lid van een overheidsinstantie (1)	10	0	1	6	1	4
Beslissing van de voorzitter (2)	0	0	0	0	0	0

341 De cijfers voor 'voorbereidende gerechtelijke handelingen' (tabel 6), 'wijze waarop de verzoeker zijn rechten van verdediging uitoefent' (tabel 7) of 'aard van de beslissingen van het Beroepsorgaan' (tabel 8) komen niet noodzakelijkerwijs overeen met het aantal ingediende verzoeken (zie tabellen 1 tot 4). Sommige dossiers werden bijvoorbeeld al opgestart in 2020, terwijl de beslissing pas viel in 2021.

	2016	2017	2018	2019	2020	2021
Verwijderen van informatie uit het dossier door het Beroepsorgaan (3)	54	80	72	77	50	77
Beslissingen alvorens recht te doen (4)	/	/	/	9	9	19

(1) Het Beroepsorgaan kan beslissen om de leden van de inlichtingen- en politiediensten of van de veiligheidsoverheden die aan het veiligheidsonderzoek of de veiligheidsverificatie hebben meegewerkt, te horen.

(2) De voorzitter van het Beroepsorgaan kan beslissen dat het lid van de inlichtingendienst bepaalde gegevens geheim houdt tijdens zijn verhoor.

(3) Indien de betrokken inlichtingen- of politiedienst hierom verzoekt, kan de voorzitter van het Beroepsorgaan beslissen dat bepaalde informatie wordt verwijderd uit het dossier dat ter inzage aan de verzoeker zal worden voorgelegd.

(4) Het kan bijvoorbeeld gaan om een beslissing om twee dossiers samen te voegen of om nadere informatie te vragen over de context van een gerechtelijk dossier. Deze gegevens worden geregistreerd vanaf 2019.

Tabel 9. Wijze waarop de verzoeker zijn rechten van verdediging uitoefent

	2016	2017	2018	2019	2020	2021
Inzage van het dossier door de verzoeker en/of zijn advocaat	87	105	69	96	96	97
Horen van de verzoeker (al dan niet bijgestaan door zijn advocaat)[342]	127	158	111	143	135	151

Tabel 10. Aard van de beslissingen van het Beroepsorgaan

	2016	2017	2018	2019	2020	2021
Veiligheidsmachtigingen (art. 12 e.v. W.C&VM)						
Beroep onontvankelijk	0	3	0	1	1	0
Beroep zonder voorwerp	7	0	4	3	3	3

342 De W.Beroepsorgaan regelt de bijstand door een advocaat tijdens de zitting, maar niet de vertegenwoordiging door die laatste. In bepaalde dossiers wordt de verzoeker (al dan niet bijgestaan door zijn advocaat) meermaals gehoord. In 56% van de gevallen werd de verzoeker bijgestaan door een advocaat.

	2016	2017	2018	2019	2020	2021
Beroep ongegrond	18	13	12	12	16	11
Beroep gegrond (volledige of gedeeltelijke toekenning)	24	24	12	25	14	17
Bijkomende onderzoeksdaden door de overheidsinstantie	2	0	1	1	2	1
Bijkomende termijn voor de overheidsinstantie	2	1	1	0	3	0
Verleent akte van afstand van beroep	0	0	3	2	2	11
Veiligheidsattesten voor geclassificeerde zone (art. 22*bis*, al. 1 W.C&VM)						
Beroep onontvankelijk	0	1	0	0	0	0
Beroep zonder voorwerp	0	1	0	0	0	0
Beroep ongegrond	1	0	1	1	0	2
Beroep gegrond (toekenning)	1	1	0	3	0	2
Verleent akte van afstand van beroep	-	-	-	1	0	0
Veiligheidsattesten voor plaats of evenement (art. 22*bis*, al. 2 W.C&VM)						
Beroep onontvankelijk	0	1	2	4	2	0
Beroep zonder voorwerp	0	1	0	0	0	0
Beroep ongegrond	2	12	2	4	4	1
Beroep gegrond (toekenning)	4	7	3	4	1	0
Verleent akte van afstand van beroep	0	1	2	0	0	0
Veiligheidsattesten voor nucleaire sector (art. 8*bis*, §2 W.C&VM)						
Beroep onontvankelijk	1	1	0	1	0	0
Beroep zonder voorwerp	1	0	1	0	0	0
Beroep ongegrond	0	1	1	5	2	2

	2016	2017	2018	2019	2020	2021
Beroep gegrond (toekenning)	7	5	6	7	4	6
Verleent akte van afstand van beroep	-	-	2	0	0	0
Veiligheidsadviezen (art. 22*quinquies* W.C&VM)						
Beroepsorgaan onbevoegd	0	20[343]	12	0	0	0
Beroep onontvankelijk	15	10	3	7	8	3
Beroep zonder voorwerp	0	1	3	1	6	4
Bevestiging van negatief advies	42	49	46	40	51	47
Omzetting in positief advies	46	41	27	43	52	34
Verleent akte van afstand van beroep	0	1	0	1	5	5
Beroep tegen normatieve rechtshandelingen van een administratieve overheid (art. 12 W.Beroepsorgaan)	0	0	0	0	0	0
TOTAAL	**173**	**195**	**144**	**166**	**176**	**149**

IX.2. OPMERKINGEN EN SUGGESTIES VAN DE VOORZITTER VAN HET BEROEPSORGAAN

IX.2.1. EEN BIJZONDERE EN COMPLEXE PROCEDURE

Als administratief rechtscollege onderscheidt het Beroepsorgaan zich door een administratief beheer van dossiers dewelke bijzonder van aard zijn en meer complex in vergelijking met andere rechtscolleges van de gerechtelijke en administratieve orde.

[343] Het betreft *in casu* de beroepen ingediend tegen (negatieve) veiligheidsadviezen van de Nationale Veiligheidsoverheid met betrekking tot personeel van onderaannemers actief bij Europese instellingen. Het Beroepsorgaan had beslist dat er geen wettelijke basis was voor de adviezen van de Nationale Veiligheidsoverheid. Bijgevolg verklaarde het Beroepsorgaan zich onbevoegd om te oordelen over de al dan niet gegrondheid van de veiligheidsadviezen van de Nationale Veiligheidsoverheid.

Een eerste bijzonderheid is de wettelijke vereiste van artikel 4 Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veilig-heidsattesten en veiligheidsadviezen (W.Beroepsorgaan), dewelke vandaag buitensporig blijkt. De rechtsonderhorige moet zijn beroep inzake veiligheidsattesten en -adviezen immers instellen binnen de strikte termijn van acht dagen en dit per aangetekend schrijven. De rechtspractici zijn van mening dat een dergelijke termijn onbetwistbaar te kort is voor de burger.

Een tweede bijzonderheid houdt in dat de eiser, in het licht van de wet, in zijn beroep een uiteenzetting moet opnemen van de omstandigheden van de zaak en van de aangevoerde redenen. De voorzitter van het Beroepsorgaan is er zich ervan bewust dat dit wettelijk voorschrift geen rekening houdt met de moeilijkheid voor de burger om in rechte te handelen.

Een derde bijzonderheid heeft te maken met de vraag vanwege de veiligheidsoverheden, in bijna één dossier op twee (77/180), tot beperking van het recht van de rechtsonderhorige om kennis te nemen van het geheel van zijn dossier. Aan het Beroepsorgaan wordt immers gevraagd om artikel 5 §3 W.Beroepsorgaan toe te passen. Dit artikel luidt als volgt: "*Op verzoek van de politie- of inlichtingendienst kan het beroepsorgaan beslissen dat sommige inlichtingen uit de verklaring van een lid van de in § 2 bedoelde politie- of inlichtingendienst, uit het onderzoeksverslag of het onderzoeksdossier of het verificatiedossier, om een van de in § 2, vierde lid, genoemde redenen, of als deze onder het geheim van een lopend opsporings- of gerechtelijk onderzoek vallen, geheim zijn en dat de eiser noch zijn advocaat er inzage van krijgen. Als deze geheimen betrekking hebben op een lopend opsporingsonderzoek of gerechtelijk onderzoek, overlegt het beroepsorgaan hierover voorafgaandelijk met de bevoegde magistraat. Wanneer die inlichtingen afkomstig zijn van een buitenlandse inlichtingendienst, wordt de beslissing tot niet-inzage genomen door de inlichtingen- en veiligheidsdienst. Tegen die beslissingen is geen beroep mogelijk.*" Daaruit volgt dat de voorbereiding van de dossiers van het Beroepsorgaan vereist dat ze worden gescand en vervolgens dat de gevoelige informatie eruit wordt verwijderd. Dit werk wordt pagina per pagina, paragraaf per paragraaf of zelfs woord per woord uitgevoerd door de griffie. *In concreto* gaat het om een juridische analyse die wordt goedgekeurd door de voorzitter van het rechtscollege, en daarna wordt uitgevoerd door de leden van de griffie. Voor het rechtscollege gaat het erom garanties te bieden voor het recht van de rechtsonderhorige om in bezit te worden gesteld van zoveel mogelijk informatie tegenover een wettelijke eis tot beperking van de toegang.

Een vierde bijzonderheid betreft de termijnen voor het toesturen van de administratieve dossiers door de veiligheidsoverheden, in weerwil van de wettelijke voorschriften. Voor 45 van de 180 ingediende dossiers zag de griffie van het Beroepsorgaan zich genoodzaakt een of meerdere herinneringen te versturen naar de veiligheidsoverheden om hen ertoe te bewegen het administratieve dossier toe te sturen. Dergelijke vertragingen doen zich steeds vaker voor en hebben nu betrekking op één dossier op vier, tegenover één dossier op tien vijf jaar geleden.

Daardoor kan het Beroepsorgaan geen beslissingen nemen binnen de opgelegde termijnen. Daarnaast is er vooral sprake van nadeel voor de rechtsonderhorige voor wie het verkrijgen van een veiligheidsmachtiging of -advies vaak de *conditio sine qua non* is voor de uitoefening van een functie.

Een vijfde bijzonderheid tot slot heeft te maken met de vermeerdering van de beroepen die worden ingesteld door buitenlandse aanvragers of aanvragers die in het buitenland hebben verbleven en het feit dat de wettelijke instrumenten waarover de veiligheidsoverheden beschikken, ongeschikt zijn om aan deze maatschappelijke realiteit te beantwoorden. Als gevolg daarvan moeten de veiligheidsoverheden soms verdragen sluiten die de uitwisseling van informatie en inlichtingen met buitenlandse veiligheidsoverheden mogelijk maken. Bij gebrek aan dergelijke akkoorden, volgen de veiligheidsoverheden de rechtspraak van het Beroepsorgaan inzake de problematiek van onderzoeken of verificaties naar personen die niet beschikken over de Belgische nationaliteit niet, en zonder dit op een omstandige wijze te motiveren. De voorzitter van het Beroepsorgaan is van mening dat de Belgische veiligheidsoverheden zouden moeten trachten om informatie in te winnen bij de homologe diensten in het buitenland.[344]

Volgens de voorzitter van het Beroepsorgaan zijn de wet en zijn koninklijke besluiten niet aangepast aan de moderne eisen van toegang tot justitie. De artikelen 2 en 3 van het KB Beroepsorgaan bepalen immers dat "*alle processtukken aan het beroepsorgaan worden toegezonden bij ter post aangetekende brief*" en dat "*de beroepsakte wordt ondertekend en gedagtekend door de eiser of door een advocaat*". Heel wat rechtsonderhorigen nemen deze regels niet in acht en meestal is dit het gevolg van een onvoldoende beheersing van de procedureregels (begrijpelijk gezien de complexiteit van deze regels).

Het wetsvoorstel dat door de voorzitter van het Beroepsorgaan werd opgesteld in samenwerking met voormalig voorzitter van het Hof van Cassatie, Ivan Verougstraete, tracht daaraan te verhelpen. Er moet immers meer rekening worden gehouden met de hoedanigheid en zelfs de kwetsbaarheid van heel wat verzoekers. Daarenboven moet worden voorzien in wettelijke bepalingen die geen nietigheid van rechtswege noch de onontvankelijkheid van het verzoek met zich meebrengen.

De tekst voor hervorming werd op 24 november 2020 toegezonden aan de Kamer van volksvertegenwoordigers. Rekening gehouden met de verschillende wetsvoorstellen in voorbereiding tot wijziging van onder meer de Classificatiewet, is het Beroepsorgaan van mening dat er met deze voorstellen rekening dient te worden gehouden. Per slot van rekening moet de regelgeving betreffende de veilig-

344 Met de Wet van 23 februari 2018 (*B.S.* 1 juni 2018) heeft de wetgever aan de politie- en de inlichtingendiensten uitdrukkelijk de bevoegdheid verleend om relevante informatie op te vragen bij buitenlandse partnerdiensten in het kader van een veiligheidsverificatie (zie artikel 22*sexies*, 3de W.C&VM en *Parl. st*. Kamer, 2017-2018, 54 2767/001, 13). Via deze bepaling heeft de wetgever beslist dat, naast het feit dat een veiligheidsverificatie zich niet altijd beperkt tot een eenvoudige verificatie van sommige databanken, ook buitenlandse informatie relevant kan zijn voor een veiligheidsverificatie.

heidsmachtigingen, - attesten en -adviezen op harmonieuze wijze kunnen worden samen gelezen met de regelgeving aangaande het eventuele beroep tegen deze administratieve beslissingen.

Op 14 februari 2022 stuurde de voorzitster van de Kamer haar antwoord naar de voorzitter van het administratieve rechtscollege, waarin ze aandrong op nieuw overleg met het Vast Comité P en de Geschillenkamer van de Gegevensbeschermingsautoriteit.

De toegankelijkheid van het administratieve rechtscollege blijft prioritair voor het Beroepsorgaan. De tekst, zoals opgesteld, had tot doel het Beroepsorgaan te bevestigen in zijn rol van natuurlijke rechter inzake veiligheidsaangelegenheden, de beroepstermijnen te harmoniseren, de procedure minder ingewikkeld te maken en de digitalisering ervan mogelijk te maken.

IX.2.2. BESLISSING VAN DE RAAD VAN STATE

In een specifiek dossier ging de verzoeker voor de Raad van State in cassatie tegen een beslissing van het Beroepsorgaan. Dit gebeurde sinds de oprichting van het Beroepsorgaan in 1998 nooit eerder. De Raad van State verklaarde het beroep ontvankelijk[345], maar ongegrond.[346]

IX.2.3. AANSPRAKELIJKHEID VAN HET BEROEPSORGAAN

Niettegenstaande het ontbreken van een rechtspersoonlijkheid van het Beroepsorgaan stelde een rechtsonderhorige, volgend op een beslissing van het administratieve rechtscollege en een arrest van onbevoegdheid van de Raad van State, een aansprakelijkheidsvordering in. Er werd een dagvaarding ingeleid voor de Franstalige rechtbank van eerste aanleg van Brussel. Daarbij werd niet enkel de Belgische Staat, maar ook het Beroepsorgaan zelf gedagvaard. Deze zaak is hangende voor het hof van beroep van Brussel volgend op het vonnis van 7 september 2018 waarbij het Beroepsorgaan werd veroordeeld tot de betaling van een schadevergoeding.

345 *In extenso*: W. VAN LAETHEM, 'Problemen met veiligheidsadvies van beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen', *Juristenkrant* 2021, 439, 8-9.

346 Raad van State, arrest nr. 251.927, 26 oktober 2021 (www.raadvst-consetat.be).

IX.2.4. TWEE KWESTIES MET BETREKKING TOT ARTIKEL 6 VAN HET EUROPEES VERDRAG VOOR DE RECHTEN VAN DE MENS (EVRM)

De voorzitter van het Beroepsorgaan acht het aangewezen om de Kamer van volksvertegenwoordigers attent te maken op twee kwesties die worden opgeworpen ten gevolge de Europese rechtspraak en waarmee de Wet op het Beroepsorgaan voorals nog geen rekening hield.

Artikel 6 van het Verdrag voor de Rechten van de Mens (EVRM) bekrachtigt het recht op een eerlijk proces, en dit zowel op gerechtelijk als bestuurlijk vlak. Het eerste lid van het artikel betreft in het bijzonder de kwestie van de openbaarheid van de zittingen en van de publicatie van de beslissingen:

"Bij het vaststellen van zijn burgerlijke rechten en verplichtingen of bij het bepalen van de gegrondheid van een tegen hem ingestelde vervolging heeft een ieder recht op een eerlijke en openbare behandeling van zijn zaak, binnen een redelijke termijn, door een onafhankelijk en onpartijdig gerecht dat bij de wet is ingesteld. De uitspraak moet in het openbaar worden gewezen maar de toegang tot de rechtszaal kan aan de pers en het publiek worden ontzegd, gedurende de gehele terechtzitting of een deel daarvan, in het belang van de goede zeden, van de openbare orde of nationale veiligheid in een democratische samenleving, wanneer de belangen van minderjarigen of de bescherming van het privé leven van procespartijen dit eisen of, in die mate als door de rechter onder bijzondere omstandigheden strikt noodzakelijk wordt geoordeeld, wanneer de openbaarheid de belangen van een behoorlijke rechtspleging zou schaden."

De situatie ten aanzien van het huidige recht en de Europese rechtspraak vereist op dat vlak een denkoefening in het belang van de rechtsonderhorige. Het gaat enerzijds om de publicatie van de beslissingen en anderzijds om de openbaarheid van de zittingen.

IX.2.4.1. De publicatie

Eind juni 2014 bracht de Commissie voor de Modernisering van de Rechterlijke Orde (CMRO) deze kwestie ter sprake.[347] In België bestaan drie zogenaamde 'hooggerechtshoven': het Hof van Cassatie, de Raad van State en het Grondwettelijk Hof. Voor elk van deze colleges geldt een verschillende regeling inzake de publicatie van zijn beslissingen; elk college staat autonoom in voor de bekendmaking ervan. De toegankelijkheid van de rechtspraak in België wordt in het algemeen voorzien door middel van openbare (Juridat…) of private gegevensbanken (Jura, Stradalex, Jurisquare…) en via tijdschriften.

347 Commissie voor de Modernisering van de Rechterlijke Orde, *Verslag gewijd aan de bekendmaking van rechterlijke beslissingen. De veer, de Pelikan en de cloud*, 30 juni 2014.

Voor wat betreft de Raad van State, wordt deze kwestie geregeld door een koninklijk besluit en een ministerieel besluit.[348] In de regel geldt de publicatie van alle arresten, met als enig voorbehoud deze in verband met de zeer specifieke materie van de wetgeving betreffende de toegang tot het grondgebied, het verblijf, de vestiging en de verwijdering van vreemdelingen. In tegenstelling tot het Hof van Cassatie, bestaat er geen filter die de toegang tot een deel van de rechtspraak verhindert. De Raad van State hanteert immers een tweeledige aanpak wat betreft de publicatie van zijn beslissingen: enerzijds wordt de volledige rechtspraak zeer snel *online* geplaatst, anderzijds wordt in een afzonderlijke databank een beredeneerde en gestructureerde selectie gemaakt van de interessante arresten. De databank is openbaar en kosteloos. Het aan het koninklijk besluit voorafgaand verslag aan de Koning is bijzonder verhelderend in verband met het belang om zekerheden te bieden voor wat betreft de toegankelijkheid van de rechtspraak van dit college. In het koninklijk besluit zelf komt ook de kwestie van de anonimisering aan bod.

Meer in het bijzonder stelde de CMRO vast dat de niet-beschikbaarheid van de rechtspraak van de hoven en rechtbanken een '*democratisch deficit*' doet ontstaan: hoe kan de toegang voor iedereen tot de rechter worden gegarandeerd indien de rechtspraak niet toegankelijk is? Hoe kan het recht worden onderwezen en beoefend wanneer niemand weet hoe er recht wordt gesproken en gedaan?

Wat betreft het Beroepsorgaan, bevat de Wet van 11 december 1998 hierover geen enkele bepaling. De verschillende veiligheidsoverheden hebben ondertussen al wel hun bezorgdheid uitgesproken wat betreft de publicatie van de beslissingen.

De voorzitter van het Beroepsorgaan is zich ervan bewust dat zijn rechtspraak betrekking heeft op specifieke kwesties, waarvan sommige verband kunnen houden met de veiligheid van de Staatsbelangen. Het lijdt geen twijfel dat anonimisering in dit opzicht stelselmatig en op zeer voorzichtige wijze moet gebeuren. De problematiek van de anonimisering hangt in België nauw samen met die van de bescherming van de persoonlijke levenssfeer in het domein van de gegevensbanken. In het licht van zijn bevoegdheid – beperkt tot natuurlijke personen – stelde

348 Koninklijk besluit van 7 juli 1997 betreffende de publicatie van de arresten en de beschikkingen van niet-toelaatbaarheid van de Raad van State en ministerieel besluit van 3 februari 1998 tot bepaling van het informatienetwerk dat toegankelijk is voor het publiek en van de magnetische drager met het oog op de raadpleging en de registratie van de arresten van de Raad van State.

de gewezen Commissie voor de bescherming van de persoonlijke levenssfeer eerder al een doorgedreven anonimisering voor.[349]

Een debat over de publicatie van de beslissingen van het Beroepsorgaan door de Kamer van volksvertegenwoordigers in het kader van de democratische versterking van de instellingen lijkt dan ook aangewezen.

IX.2.4.2. De openbaarheid van de zittingen

Artikel 6 van het EVRM voorziet in het recht op een eerlijk proces en behandelt in het bijzonder in zijn eerste lid de kwestie van de openbaarheid van de zittingen en van de uitspraak van de genomen beslissingen. De Belgische wetgever heeft in 1998 geen bepalingen aangaande de openbaarheid van de zittingen opgenomen in de organieke wet op het Beroepsorgaan.

Uit een analyse van het Europees Hof komen de volgende algemene principes naar voren inzake zittingen[350]:

"In principe heeft de rechtsonderhorige recht op een openbare zitting, daar hij op deze manier beschermd is tegen een geheime justitie die aan de controle van het publiek ontsnapt. Door de transparantie die ze aan de rechtsbedeling verleent, helpt de openbare zitting het doel van artikel 6 § 1, i.e. een eerlijk proces, verwezenlijken. Hoewel het houden van een openbare zitting een fundamenteel beginsel is dat wordt bekrachtigd door artikel 6 § 1, gaat het niet om een absolute verplichting (De Tommaso t. Italië [GC], 2017, § 163). Om te bepalen of een proces voldoet aan de vereiste van openbaarheid, dient men de hele procedure te bekijken (Axen t. Duitsland, 1983, § 28).

In een procedure die voor een enkele rechtbank wordt gehouden, houdt het recht van eender wie op het feit dat zijn zaak 'in het openbaar zou worden gehoord', in de betekenis van artikel 6 § 1, het recht op een 'zitting' in (Göç t. Turkije [GC], 2002, § 47; Fredin t. Zweden (nr. 2), 1994, §§ 21-22; Allan Jacobsson t. Zweden (nr. 2), 1998, § 46; Selmani e.a. t. de Voormalige Joegoslavische Republiek Macedonië, 2017, §§ 37-39).

---

349 Advies nr. 42/97 van 23 december 1997 en aanbeveling nr. 03/2012 van 8 februari 2012. In 1997 schreef de Commissie voor de bescherming van de persoonlijke levenssfeer: *"De bescherming is des te noodzakelijker daar de navigatieprogrammatuur en het vermogen van de informatiesystemen wat de onderlinge verbindingen tussen gegevens betreft, steeds krachtiger worden en er zo goed als geen controle bestaat op het gebruik dat van de systemen wordt gemaakt via deze opvragingen op afstand. Men kan zich aldus indenken hoe makkelijk het voor een goed geïnformeerd internaut is om de ganse rechtspraak te verzamelen over ontslagen wegens ernstige redenen, om er naam en adres van de betrokken werknemers uit te halen, of de geneesheren te identificeren wier aansprakelijkheid voor de rechtbank zou zijn gebracht. Het gedrag van een rechter tegenover een bepaald type conflict zal statistisch kunnen worden geëvalueerd en de naam van een advocaat zal kunnen worden geassocieerd met een percentage van processen die een gunstige afloop kennen."* (Advies CBPL nr. 42/97 van 23 december 1997).

350 RAAD VAN EUROPA, EUROPEES HOF VOOR DE RECHTEN VAN DE MENS, *Guide sur l'article 6 de la Convention européenne des droits de l'homme*, 31 december 2021 (vrije vertaling) https://www.echr.coe.int/documents/guide_art_6_fra.pdf

De openbaarheid van de debatten moet ook worden gelezen vanuit de invalshoek van de aanwezigheid van publiek en pers: De openbaarheid van de gerechtelijke debatten beschermt de rechtsonderhorigen tegen een geheime justitie die ontsnapt aan de controle van het publiek en vormt aldus een van de middelen die bijdragen tot het behoud van het vertrouwen in de rechtbanken. Ze helpt het doel van een eerlijk proces bereiken (Martinie t. Frankrijk [GC], 2006, § 39; Diennet t. Frankrijk, 1995, § 33; Gautrin e.a. t. Frankrijk, 1998, § 42; Hurter t. Zwitserland, 2005, § 26; Lorenzetti t. Italië, 2012, § 30). Artikel 6 § 1 belet echter niet dat rechtscolleges kunnen beslissen, rekening houdend met de bijzonderheden van een zaak, om af te wijken van dit beginsel (Martinie t. Frankrijk [GC], 2006, §§ 40-44). Een zaak achter gesloten deuren, volledig of gedeeltelijk, moet dan strikt worden geregeld door de omstandigheden van de zaak (Lorenzetti t. Italië, 2012, § 30). De tekst van artikel 6 § 1 voorziet in meerdere uitzonderingen. Dit artikel bepaalt: "[...] de toegang tot de rechtszaal kan aan de pers en het publiek worden ontzegd, gedurende de gehele terechtzitting of een deel daarvan":

– "in het belang van de goede zeden, van de openbare orde of nationale veiligheid in een democratische samenleving" (B. en P. t. Verenigd Koninkrijk, 2001, § 39; Zagorodnikov t. Rusland, 2007, § 26);

– "wanneer de belangen van minderjarigen of de bescherming van het privé leven van de procespartijen dit eisen": de belangen van minderjarigen of de bescherming van het privéleven van de partijen bij het proces staan bijvoorbeeld op het spel in het kader van procedures betreffende de hoede over minderjarige kinderen als gevolg van de echtscheiding of de feitelijke scheiding van de ouders, of bij geschillen tussen leden van eenzelfde familie (ibidem, § 38). In zaken die echter betrekking hebben op de plaatsing van een kind in een openbare instelling, moeten de redenen om de zaak aan het onderzoek van het publiek te onttrekken aandachtig worden onderzocht (Moser t. Oostenrijk, 2006, § 97). In het geval van een tuchtrechtelijke procedure tegen een arts, waarbij de noodzaak om het beroepsgeheim of de persoonlijke levenssfeer van de patiënten te beschermen een reden kan zijn om de zaak achter gesloten deuren te houden, moet deze laatste strikt worden geregeld door de omstandigheden (Diennet t. Frankrijk, 1995, § 34). Voor een voorbeeld van een procedure tegen een advocaat, zie Hurter t. Zwitserland, 2005, §§ 30-32;

– " in die mate als door de rechter onder bijzondere omstandigheden strikt noodzakelijk wordt geoordeeld, wanneer de openbaarheid de belangen van een behoorlijke rechtspleging zou schaden": het is mogelijk om af te wijken van het principe van de openbaarheid van de debatten om de veiligheid en de intimiteit van de getuigen te beschermen of ter bevordering van de vrije uitwisseling van informatie en meningen in de voortzetting van de zaak (B. en P. t. Verenigd Koninkrijk, 2001, § 38; Osinger t. Oostenrijk, 2005, § 45).

Het Hof heeft toegevoegd dat de rechtspraak betreffende het houden van een zitting als zodanig – vooral met betrekking tot het recht zich uit te drukken voor de rechtbank zoals bedoeld in artikel 6 § 1 – van toepassing kon zijn naar analogie met het

houden van debatten die voor het publiek toegankelijk zijn. Aldus moet een zitting die plaatsvindt krachtens het nationaal recht in principe openbaar zijn. Het houden van een openbare zitting is echter niet absoluut, waarbij de omstandigheden die toelaten ervan af te wijken voornamelijk afhankelijk zijn van de aard van de vragen die bij interne rechtbanken aanhangig worden gemaakt (De Tommaso t. Italië [GC], 2017, §§ 163-167). "Uitzonderlijke omstandigheden – meer bepaald het uiterst technische karakter van de vragen waarover een uitspraak moet worden gedaan – kunnen het ontbreken van openbaarheid rechtvaardigen, op voorwaarde dat de specificiteit van de materie geen controle van het publiek vereist" (Lorenzetti t. Italië, 2012, § 32).

De loutere aanwezigheid van geclassificeerde documenten in een gerechtelijk dossier leidt er niet automatisch toe dat het publiek wordt uitgesloten van de debatten. Alvorens het publiek uit te sluiten van een bijzondere zaak, zou de rechtbank op specifieke wijze moeten nagaan of een dergelijke uitsluiting noodzakelijk is om een openbaar belang te beschermen en die uitsluiting beperken tot wat strikt noodzakelijk is om het beoogde doel te bereiken (Nikolova en Vandova t. Bulgarije, 2013, §§ 74-77 in verband met een zaak achter gesloten deuren wegens documenten die als staatsgeheim zijn geklasseerd; zie ook over de principes, Vasil Vasilev t. Bulgarije, 2021,§§ 105-106)." [vrije vertaling]*

De kwestie van de openbaarheid van de zittingen vereist een bijzondere aandacht van en een grondig debat in de Kamer van volksvertegenwoordigers. De voorzitter van het Beroepsorgaan is bereid om op actieve wijze mee te werken aan dit proces.

IX.2.5. DE DOELTREFFENDHEID VAN DE BESLISSINGEN VAN HET BEROEPSORGAAN

Een kwestie van de doeltreffendheid van de beslissingen van het Beroepsorgaan doet zich voor ten aanzien van de Nationale Veiligheidsoverheid (NVO). Naast de weigering om administratieve dossiers toe te sturen in het kader van bepaalde beroepen, wijst de voorzitter van het Beroepsorgaan op wat wordt bepaald in artikel 12 § 6 van de organieke wet: "*De beslissingen van het beroepsorgaan zijn vanaf hun kennisgeving rechtstreeks uitvoerbaar.*"

Het Beroepsorgaan had in een zaak aan de betrokkene een veiligheidsmachtiging (niveau 'GEHEIM EU') verleend die hem was geweigerd door de NVO. Op 19 juli 2021 gaf de Franstalige rechtbank van eerste aanleg van Brussel (A.R. 2021/51/C) bij een op tegenspraak verleende beschikking in kort geding aan de Belgische Staat het bevel, via de NVO, om aan de verzoeker zijn veiligheidsmachtiging te verlenen binnen de maand volgend op de betekening van de beschikking. Dit op straffe van een dwangsom die werd vastgesteld op € 500 per dag vertraging, met een maximum van € 10.000.

In hetzelfde dossier waren de Federale Ombudsmannen, tot wie de betrokkene zich had gewend wegens de niet-uitvoering van de beslissing van het Beroepsorgaan, tussengekomen, doch zonder succes. Ze beschouwden de klacht als gegrond, en gaven volgende motivering: *"[...] In een rechtsstaat doet de niet-uitvoering van een beslissing die is genomen in het kader van een administratief beroep op ernstige wijze afbreuk aan de rechtszekerheid."*

IX.2.6. VOORUITZICHTEN

In uitvoering van de aanbevelingen van het Vast Comité I, neemt de minister van Defensie zich voor om wetsontwerpen in te dienen met als doel het principe van een veiligheidsverificatie voor zowel het burger- als het militair personeel van Landsverdediging te systematiseren. Dit veiligheidsadvies zou niet langer enkel bij de kandidaatstelling vereist zijn, maar voor de volledige duur van de loopbaan van de verschillende medewerkers van Landsverdediging. We kunnen aannemen dat een dergelijk veiligheidsadvies om de vijf jaar zal worden vernieuwd. Eventuele beroepen zullen in principe tot de bevoegdheid van het Beroepsorgaan behoren.

Naar aanleiding van het toezichtonderzoek van september 2021 van het Vast Comité I naar de wijze waarop de Veiligheid van de Staat de regeringscommissaris Ihsane Haouach opvolgde, beval dit Comité aan dat de uitoefening van bepaalde 'openbare functies' de voorafgaande controle vereist van de integriteit, de loyaliteit en de discretie, zoals reeds vereist in sommige Europese landen. De uitvoering van deze aanbeveling zou moeten leiden tot een uitbreiding van de veiligheidsadviezen dewelke eveneens het voorwerp zullen uitmaken van een jurisdictionele controle door het Beroepsorgaan.

Ten slotte moet er worden tegemoetgekomen aan de vrijstelling van de portkosten, alsook met de mogelijkheid een beroep op digitale wijze in te dienen en toe te staan dat de akten van betekening, volgens de voorkeur van de rechtsonderhorige, via de post of op digitale wijze worden toegestuurd in het kader van de procedure hangende voor het Beroepsorgaan.

HOOFDSTUK X.

DE INTERNE WERKING VAN HET VAST COMITÉ I

X.1. SAMENSTELLING VAN HET VAST COMITÉ I

De samenstelling van het Comité bleef in 2021 ongewijzigd: Serge Lipszyc (F), eerste substituut arbeidsauditeur bij het arbeidsauditoraat van Luik bleef zijn opdracht als voorzitter vervullen. Pieter-Alexander De Brock (N) en Thibaut Vandamme (F), substituut procureur des Konings van het arrondissement Luxemburg oefenden het mandaat van lid uit.[351], [352]

In afwachting van de benoeming van een griffier, werd Wauter Van Laethem (N) aangesteld als plaatsvervangend griffier.[353]

Bij de Dienst Enquêtes I, sinds 1 januari 2021 onder leiding van Fabian Poncelet (F), werden enkele wijzigingen opgetekend. In juni 2021 trad een nieuwe Franstalige commissaris-auditor aan; hij wordt gedetacheerd vanuit de Federale Politie. Een commissaris-auditor nam ontslag en zal in de loop van 2022 worden vervangen.

Ten slotte bleef ook de administratieve staf van het Vast Comité I niet ongewijzigd. De in december 2020 aangeworven Franstalige statutaire jurist van de Afdeling documentatie en juridische analyse keerde in augustus 2021 terug naar zijn dienst van oorsprong. Aan dezelfde afdeling werden in oktober 2021 twee

---

351 Thibaut Vandamme legde op 11 januari 2021 de eed af. Met toepassing van art. 157, nr. 6 van het Kamerreglement, werd in de plenaire vergadering van 20 mei 2021 Thierry Werts verkozen verklaard voor het mandaat van eerste plaatsvervanger van Thibaut Vandamme (CRABV55PLEN105, 20 mei 2021, 46).

352 Wauter Van Laethem nam eind 2021 ontslag als tweede plaatsvervangend lid van het Nederlandstalige lid (*Hand*. Kamer 2021-22, 10 november 2021, CRIV55PLEN139, 68). Hij werd in maart 2022 vervangen door Filip Vanneste, substituut-procureur-generaal bij het Hof van Beroep te Antwerpen (*Hand.* Kamer 2021-22, 24 maart 2022, CRIV55PLEN171, 67).

353 Een oproep tot benoeming van griffier van het Vast Comité I verscheen halfweg mei 2020 in het Belgisch Staatsblad. Op 21 juni 2021 werd een wetsvoorstel ingediend tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van de Vaste Comités I en P (*Parl. St.* Kamer 2020-21, 55K2064/001). De aangelegenheid werd eerst besproken in de Conferentie van voorzitters (24 februari en 3 maart 2021) (*Hand*. Kamer 2020-21, 55K1924/001). De 'Wet van 14 augustus 2021 tot wijziging van de wet van 18 juli 1991 […], alsook tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van het Vast Comité I en het Vast Comité P' verscheen in het Belgisch Staatsblad op 8 december 2021. Een nieuwe vacature verscheen in het Staatsblad 19 juli 2021. Op 26 april 2022 legde Frédéric Givron (F) in handen van de Kamervoorzitster de eed af als nieuwe griffier van het Vast Comité I.

Franstalige medewerkers toegevoegd. Ook werd in april 2021 een Nederlandstalige statutaire secretaresse aangeworven. Eind 2021 telde de administratieve staf 18 personeelsleden.

Halfweg juni 2021 werd door de voorzitter van het Vast Comité I bij de voorzitster van de Kamer van Volksvertegenwoordigers het personeelsgebrek en de sterk toegenomen takenpakket opnieuw aangekaart.[354] Niettegenstaande de dynamiek die de Kamer aan de dag legt in het kader van de synergiedoelstellingen, die onderschreven worden door het Comité, zag het Comité zich genoodzaakt om een dringende versterking te bepleiten. Het Comité verkeert immers in de onmogelijkheid om alle wettelijke opdrachten uit te voeren en adequaat te reageren op de verschillende verzoeken van de Kamer.

X.2. EEN WELZIJNSAUDIT OP HET COMITE

Naar aanleiding van signalen van onwelzijn op het Vast Comité I, werd IDEWE, een externe dienst voor preventie en bescherming op het werk, de opdracht gegeven om een analyse van de psychosociale risico's uit te voeren. De audit analyseerde thema's die overeenstemmen met de vijf domeinen van psychosociale risico's op het werk (arbeidsinhoud, arbeidsorganisatie, arbeidsomstandigheden, arbeidsvoorwaarden en interpersoonlijke relaties op het werk). Dit resulteerde in een omstandig rapport[355], met daarin de resultaten van de analyse en een advies aan de werkgever.[356]

Op basis daarvan werd een veranderingstraject opgestart. Het Vast Comité I zal daarin begeleid worden door de FOD Beleid en Ondersteuning. Er wordt onder meer voorzien in een stakeholdersbevraging en een grondige SWOT- en PESTEL-analyse[357]. De afronding van het project wordt voorzien eind juni 2022.

Naar aanleiding van de resultaten van de welzijnsaudit, werd half december 2021 alvast een nieuwe Nederlandstalige vertrouwenspersoon aangesteld. De benoeming van een Franstalige vertrouwenspersoon volgde eind januari 2022.[358]

---

354 Brief van de Voorzitter van het Vast Comité I aan de Voorzitster van de Kamer van Volksvertegenwoordigers d.d. 16 juni 2021.

355 IDEWE, Analyse van de psychosociale risico's, 23 november 2021, 31 p.

356 Er werd voorgesteld het 'teamdoelmatigheidsmodel' (SDRPI) te hanteren om de vastgestelde probleemsituaties te verhelpen. Daarbij wordt ingezet op de **S**ituatie (context waarbinnen wordt gewerkt), de **D**oelen (creëren van heldere en gedeelde doelen), de **R**ollen (wat mag van wie verwacht worden), de **P**rocedures (ontwikkeling van gepaste werkwijzen) en de **I**nterpersoonlijke relaties.

357 De PESTEL-analyse is een bedrijfskundig model dat wordt gebruikt voor het identificeren van de invloed van externe factoren op een organisatie. PESTEL staat voor politiek, economisch, sociologisch, technologisch, ecologisch en legal (juridisch).

358 De wetgeving (2014) rond psychosociale risico's op het werk verplicht vertrouwenspersonen een basisopleiding van 30 lesuren te volgen. Een werknemer die aangesteld is als vertrouwenspersoon moet binnen de twee jaar na zijn aanstelling een opleiding volgen.

X.3. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE

De Bijzondere commissie belast met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de veiligheids- en inlichtingendiensten kende in 2021 een andere samenstelling. Maakten als stemgerechtigde leden deel uit van de commissie: Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen)[359], Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Denis Ducarme (MR), Servais Verherstraeten (CD&V), Nabil Boukli (PVDA-PTB), Patrick Dewael[360] (Open Vld) en Bert Moyaers (Vooruit). Kamervoorzitster Eliane Tillieux (PS) neemt het voorzitterschap van de commissie waar. Georges Dallemagne (Les Engagés) neemt deel als niet-stemgerechtigd lid.

In de loop van 2021 vonden, ondanks de sanitaire crisis, meerdere (negen in totaal) vergaderingen plaats. Tijdens deze commissievergaderingen werden – achter gesloten deuren – diverse door het Vast Comité I afgesloten toezichtonderzoeken besproken.[361] Eind april en begin juli 2021 werd in vergaderingen samen met het Vast Comité P voorzien voor de bespreking van respectievelijk de gemeenschappelijke toezichtonderzoeken over het Coördinatieorgaan voor de dreigingsanalyse (OCAD) en de steundiensten enerzijds en naar de rol van het OCAD in de opvolging van Jürgen Conings anderzijds. Verder werd tijd uitgetrokken voor de bespreking van het verslag opgesteld in het kader van zijn controlebevoegdheid – samen met het Controleorgaan op de politionele informatie (COC) – aangaande de gemeenschappelijke gegevensbanken (art. 44/6 WPA). Tijdens haar vergadering van 22 september 2021 werd het algemeen *Activiteitenverslag 2020* besproken.[362] De Commissie benadrukte onder meer "*dat het jaarverslag niet alleen belangrijk is om rekenschap aangaande de activiteiten van het Vast Comité I ten aanzien van het Parlement af te leggen, maar ook om buitenstaanders (academici, journalisten, medewerkers van de inlichtingendiensten enzovoort op volstrekt transparante wijze te informeren*". Een aantal thema's weerhielden de bijzondere aandacht van de Kamerleden, zoals de *follow-up* van klachten, het Memorandum of Understanding (MoU) tussen de ADIV en de inlichtingendiensten van Rwanda, COVID-19 en de rol van de inlichtingendiensten of nog, de buitenlandse intercepties. De Commis-

359 Ondertussen vervangen door Julie Chanson (Ecolo-Groen).
360 Ondertussen vervangen door Tim Vandenput (Open Vld).
361 Eenmaal werd een vergadering belegd waarin de tussentijdse rapportage (stand van zaken) van het toezichtonderzoek m.b.t. Jürgen Conings werd geagendeerd.
362 De Commissie verwijst daartoe naar artikel 66*bis*, §3, 1°W.Toezicht, zoals gewijzigd bij de wet van 6 januari 2014 tot wijziging van diverse wetten tot hervorming der instellingen (*BS* 31 januari 2014).

sie nam als eindconclusie "*akte van het activiteitenverslag 2020 van het Vast Comité I en verleent haar goedkeuring aan de aanbevelingen van het Vast Comité I*".[363]

De Commissie boog zich ten slotte ook over de interne problematiek[364] aan de top van het Vast Comité I; daartoe werden in het najaar van 2021 drie commissievergaderingen achter gesloten deuren georganiseerd.

X.4. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITE P

In 2021 vonden, behoudens enkele (informele) contacten op de werkvloer, geen gemeenschappelijke vergaderingen plaats.[365]

In 2021 waren drie gemeenschappelijke toezichtonderzoeken aan de orde: het opvolgonderzoek naar de implementatie van de door de Vaste Comités I en P geformuleerde aanbevelingen in het kader van het onderzoek naar de ondersteunende diensten van het OCAD (cf. I.1) en het toezichtonderzoek naar de vier 'bijkomende' ondersteunende diensten van het OCAD (cf. I.2). Het derde gemeenschappelijk onderzoek betrof dit naar de 'rol van het OCAD in de opvolging van de militair Jürgen Conings' (cf. I.10). Daartoe werd actief samengewerkt door de ondersteunende diensten van beide Comités.

Wel werden door beide Comités aan hun enquêtediensten de opdracht gegeven om werkprocessen voor te bereiden voor de afhandeling van gemeenschappelijke klachten en toezichtonderzoeken. Ook werd door het Vast Comité P ingestemd met het verzoek van het Vast Comité I, meer in het bijzonder van zijn Dienst Enquêtes, tot het verkrijgen van een opleiding in het kader van de raadpleging van de Algemene Nationale Gegevensbank (ANG).[366] Ten slotte werden, conform art. 52 W.Toezicht, ook activiteitenverslagen en toezichtrapporten onderling uitgewisseld.

---

363 *Parl. St.* Kamer 2020-21, nr. 55K2209/001, 20 oktober 2021 (Activiteitenverslag 2020 van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten, Verslag namens de Bijzondere commissie belat met de parlementaire begeleiding van het Vast Comité van Toezicht op de politiediensten en het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten).

364 De Commissie vergaderde onder meer na het verschijnen van een artikel in de nasleep van het rapport in de zaak-Jürgen Conings (Q. JARDON, 'Serge Lipszyc. Gendarme des services secrets', *Wilfried*, Automne 2021, Nr. 17, 1-7) en een verzoek dat bij de Kamervoorzitster werd neergelegd door twee raadsheren.

365 Art. 52 W.Toezicht stelt dat minstens twee maal per jaar gemeenschappelijke vergaderingen dienen plaats te vinden.

366 In oktober 2017 ondertekende het Vast Comité I een protocolakkoord met de Federale Politie aangaande de toepassing van het Koninklijk Besluit van 30 oktober 2015 betreffende de rechtstreekse toegang van het Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten en de Dienst Enquêtes ervan tot de gegevens en de informatie van de Algemene Nationale Gegevensbank bedoeld in artikel 44/7 van de wet op het politieambt (BS 20 november 2015).

X.5. EEN AANZIENLIJKE AANDACHT VANUIT DE MEDIA

Anders dan voorgaande jaren, was het Vast Comité I in 2021 voorwerp van een aanzienlijke media-aandacht. Vier gebeurtenissen (opgenomen in chronologische volgorde) lagen hieraan ten grondslag.

Vooreerst was er de publicatie van het toezichtsonderzoek naar de opvolging van extreemrechts door de Belgische inlichtingendiensten.[367] De voornaamste bevindingen van dit onderzoek werden overgenomen door meerdere Belgische media.

Vervolgens werd de zaak-Jürgen Conings, en de rol daarin toegemeten aan het Vast Comité I, sterk gemediatiseerd. Ter herinnering, het Vast Comité I werd door de minister van Defensie verzocht een toezichtonderzoek te openen om de betrouwbaarheid van informatie over vermoedelijke geradicaliseerden binnen Defensie na te gaan, en aanbevelingen te doen om de goede werking van de ADIV, maar ook van Defensie als geheel, te waarborgen.[368] De (sterk ingewachte) conclusies van dit rapport werden breed uitgemeten in de media.

Daarnaast werd het Vast Comité I gevat in de zaak-Ishane Haouach, voormalig regeringscommissaris bij het Instituut voor de gelijkheid van mannen en vrouwen (IGMV).[369] De aandacht voor deze zaak was groot en begon toen in de media het bestaan van een nota van de Veiligheid van de Staat werd bekendgemaakt waarin sprake was van 'nauwe contacten' tussen de Moslimbroederschap en de regeringscommissaris, al dan niet bewust wat deze laatste betrof.

Tot slot was er het interview dat de voorzitter van het Comité gaf aan het tijdschrift *Wilfried* en dat in oktober 2021 werd gepubliceerd *(supra)*. Hierin gaf de voorzitter uiting aan enkele van zijn persoonlijke zorgen naar aanleiding van verschillende belangrijke gebeurtenissen en dossiers, zoals bijv. over de zaak-Jürgen Conings. Dit interview, en de reacties die erop volgden alsook de daaropvolgende deining binnen de directie van het Comité, kreeg veel de aandacht in de pers.

Vermist het Comité er zich van bewust is dat communicatie omtrent zijn opdrachten een complexe maar essentiële aangelegenheid is, nam het Comité zich voor om in de toekomst meer aandacht aan deze kwestie te besteden, met name door de informatieverstrekking te verbeteren. De toekomstige herziening van zijn website is volledig in overeenstemming met deze aanpak.

---

367 VAST COMITÉ I, *Activiteitenverslag 2020,* 38 e.v. ('I.7. De opvolging van extreemrechts door de Belgische inlichtingendiensten').

368 Hierover 'I.9. Het opsporen en opvolging van de radicalisering van een militair: de zaak-Jürgen Conings'.

369 Hierover 'I.11. De opvolging van een regeringscommissaris door de VSSE'.

X.6. DE *DATA PROTECTION OFFICER* OP HET COMITÉ

Binnen het Comité is al enkele jaren een *Data Protection Officer* (DPO) aangesteld voor alle verwerkingen van persoonsgegevens die buiten de 'nationale veiligheid' vallen. In het kader van de synergie-oefening vanuit de Kamer van volksvertegenwoordigers vervult de functionaris voor gegevensbescherming deze rol ook voor andere dotatiegerechtigde instellingen die in het Forumgebouw resideren. De functionaris voor gegevensbescherming verleende advies inzake camerabewaking waarbij een register werd opgesteld en de aangifte werd geformaliseerd naar aanleiding van de zgn. 'nieuwe Camerawet'.[370] Daarnaast gaf de DPO ook advies- en informatieverlening inzake het intern beheer van de persoonsgegevens van de personeelsleden, onder andere in het kader van de COVID-19-pandemie.

X.7. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Het 'budget 2020' van het Vast Comité I werd vastgelegd op 5,215 miljoen euro, wat een vermeerdering inhield van 13% ten aanzien van het budget 2020.[371]

De voornaamste reden voor deze stijging was de indiening van een operationeel project voor de digitalisering van de werkprocessen. Dit project werd voorgesteld in partnerschap met een industriële operator dewelke vertrouwd is met overheidsdiensten en hun administratieve procedures. Hoewel de Commissie voor de Comptabiliteit het door het Comité voorgestelde initiatief steunde, werd vooralsnog besloten het geautomatiseerd documentenbeheer te bevriezen in afwachting van de bevindingen van het lopende overleg tussen de diensten van de Quaestuur en het Comité, opdat het project zou kunnen worden geïntegreerd in eventuele synergiën.

De financieringsbronnen van het budget werden door de Kamer van Volksvertegenwoordigers[372] als volgt toegewezen: 74,44 % dotatiebudget en 25,56 % boni van 2019.

De uitvoering van het budget 2020 leverde een budgettaire bonus op van 1,87 miljoen euro's (niet geaudite cijfers) euro, te weten het vastgestelde verschil tussen de inkomsten en de samengestelde uitgaven.

Het budget is traditiegetrouw gebaseerd op verschillende financieringsbronnen en de enige nieuwe bijdrage in termen van eigen beheer, staat ingeschreven in de

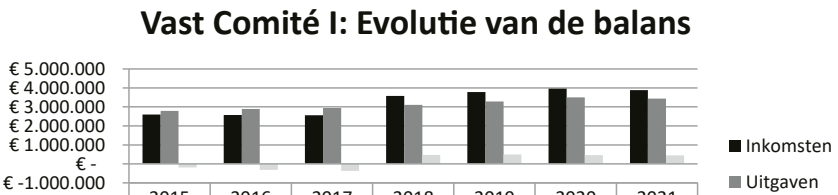
370 Wet van 30 juli 2018 tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's met het oog op het verbeteren van de samenhang van de tekst en de overeenstemming ervan met de Algemene Verordening Gegevensbescherming (AVG), BS 31 augustus 2018.

371 *Hand.* Kamer 2020-21, CRIV55PLEN081, 63.

372 *Parl. St.* Kamer 2020-21, 55K01676/001, 30-34.

dotatie van de algemene uitgavenbegroting van de Staat. Tot 2017 was deze dotatie onvoldoende om de reële uitgaven van het Comité te dekken, wat een structureel verlies als gevolg met zich meebracht. De tendens om zoveel mogelijk artikel 57, lid 1, W.Toezicht toe te passen hetwelke vermeldt dat de kredieten die noodzakelijk zijn voor de werking dienen te worden uitgetrokken op de begroting van de dotaties, laat heden ten dage het Comité toe zijn activiteiten te financieren.

Het aanzienlijk boekhoudkundig overschot is vooral te wijten aan het tijdsverloop tussen de goedkeuring van de begroting en met name de daadwerkelijke indiensttreding van het personeel als gevolg van de langdurige aanwervingsprocedures en het verkrijgen van de vereiste veiligheidsmachtigingen. Deze tendens was bijzonder uitgesproken in 2021 aangezien het Comité geconfronteerd werd met een aantal samenlopende omstandigheden, zoals de oprustestelling van diverse personeelsleden en vertragingen bij de vervanging daarvan. Er kan worden gesteld dat er in 2021 een aanzienlijk personeelsverloop was in zowat elke personeelscategorie, zowel op leidinggevend als op uitvoerend niveau: de post van griffier bleef bijvoorbeeld het hele jaar vacant totdat de Kamer van volksvertegenwoordigers recent een opvolger benoemde. Verschillende medewerkers opteerden dan weer voor een andere carrièrekeuze. Samen met de bevriezing van het budget voor het digitaliseringsproject (zie hierboven), waartoe de Kamer heeft besloten, leverde dit alles een aanzienlijke boni op, dewelke waarschijnlijk zal worden toegewezen aan de operationele begroting voor 2023 wanneer de begrotingsvoorstellen door de Kamer van volksvertegenwoordigers worden besproken.



	2015	2016	2017	2018	2019	2020	2021
Inkomsten	€ 2.597	€ 2.570	€ 2.565	€ 3.582	€ 3.780	€ 3.963	€ 3.882
Uitgaven	€ 2.792	€ 2.889	€ 2.937	€ 3.106	€ 3.284	€ 3.500	€ 3.437
Resultaat	€ -194.	€ -318.	€ -372.	€ 475.4	€ 496.0	€ 463.0	€ 444.8

Vanaf het begrotingsjaar 2023 zal het Comité volledig worden geïntegreerd in het door de Kamer geïnitieerde synergie-project[373], hetgeen onmiskenbare gevolgen zal hebben voor de werking van de dotatiegerechtigde instellingen in het algemeen en van het Vast Comité I in het bijzonder. Deze veranderingen zullen gevolgen hebben voor zowel het personeelskader als voor de werkingskredieten, die zoveel mogelijk zullen worden samengevoegd. De spildatum voor de invoegetreding van deze veranderingen werd vastgesteld op 1 januari 2023.

373 *Parl. St.* Kamer 2020-21, 55K01924/001.

X.8. IMPLEMENTATIE VAN DE AANBEVELINGEN VAN DE AUDIT VAN HET REKENHOF

Op verzoek van de Commissie van de Comptabiliteit van de Kamer van Volksvertegenwoordigers startte het Rekenhof al in december 2017 samen met Ernst and Young een onderzoek naar de dotatiegerechtigde instellingen.[374] Het auditverslag, daterend van eind maart 2018, formuleerde aanbevelingen voor de 'opdrachten' van de negen bij de audit betrokken dotatiegerechtigde instellingen, waaronder het Vast Comité I.[375]

Tussen januari en begin februari 2021 werden alle betrokken instellingen, waaronder ook het Vast Comité I, door de diensten van de Quaestuur en het secretariaat van de Commissie voor de Comptabiliteit bevraagd.

In april 2021 werd in de schoot van de Commissie voor de Comptabiliteit een akkoord bereikt over de synergiën die tussen de betrokken instellingen op gang moeten worden gebracht. Het gaat onder meer om de oprichting van een gemeenschappelijk dienstencentrum (Incentris) en een burgerportaal. Verder werd besloten het statuut en de salarisschalen van het personeel van de betrokken instellingen te harmoniseren en het wagenpark van de instellingen te rationaliseren. Ook werd beslist om een deel van de kantoren van het Vast Comité I toe te wijzen aan de BIM-Commissie. Om deze beleidslijnen te concretiseren, werden thematische werkgroepen opgericht waaraan leden van de Kamer en bepaalde instellingen deelnemen, met als logica een vertegenwoordiging per 'familie' van instellingen (een familie wordt gevormd door instellingen met verwante opdrachten).[376] [377]

In september 2021 werd door de Kamer een bijeenkomst georganiseerd voor de personeelsleden van de betrokken instellingen, om hen te informeren over de beleidslijnen waartoe werd besloten alsook over de stand van zaken van de projecten.

Voor het toewijzen van bepaalde kantoren van het Vast Comité I aan de BIM-Commissie, werden vanaf oktober 2021 verscheidene bezoeken georganiseerd, in aanwezigheid van de architect van de Kamer. Er werden ook vergaderingen gehouden met de BIM-Commissie, het Vast Comité I en de architect om

---

374 Het Rekenhof richtte zich vooral op de budgettaire aspecten (een analyse van de inkomsten en uitgaven) en op de afbakening van de taken van de diverse instellingen. Ernst and Young op zijn beurt analyseerde de processen, de systemen en de organisatie die in elk van deze instellingen aanwezig zijn.

375 *Dotatiegerechtigde instellingen. Opdrachten – Ontvangsten – Uitgaven.* Audit op vraag van de Commissie voor de Comptabiliteit van de Kamer van Volksvertegenwoordigers, Verslag goedgekeurd op 28 maart 2018 door de algemene vergadering van het Rekenhof.

376 Het Vast Comité I behoort tot de familie 'Veiligheid en bescherming', en dit samen met het Vast Comité P, de Gegevensbeschermingsautoriteit, het Controleorgaan op de politionele informatie en de BIM-Commissie.

377 Halfweg oktober 2021 werd door de Kamervoorzitster aangedrongen op een meer actieve participatie en een performante informatiedoorstroming vanuit het Vast Comité I opdat de in het kader van het synergieproject tussen de dotatiegerechtigde instellingen opgerichte werkgroepen, in staat zouden worden gesteld hun taken naar behoren uit te voeren. De Voorzitster was er zich van bewust dat het ontbreken van een griffier deze opdracht kon bemoeilijken.

de implicaties en de kosten van een dergelijk project in te kunnen schatten. In de loop van 2022 zal, met het oog op de verhuis van de BIM-Commissie, een dossier worden voorgelegd aan Commissie voor de Comptabiliteit.

X.9. VORMING

In het belang van zijn organisatie, moedigt het Vast Comité I zijn leden en medewerkers aan om algemene (informatica, management…) of sectoreigen opleidingen en conferenties te volgen.[378] Door de strikte coronamaatregelen konden geen interne of externe opleidingen worden bijgewoond in de loop van 2021.

[378] Er vonden wel de door de medewerkers verplicht bij te wonen veiligheidsbriefings plaats.

HOOFDSTUK XI.
AANBEVELINGEN

Op basis van de in 2021 afgesloten toezichtonderzoeken, controles en inspecties formuleert het Vast Comité I onderstaande aanbevelingen. Zij hebben zowel betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen, op de coördinatie en de efficiëntie van de inlichtingendiensten, het Coördinatieorgaan voor de dreigingsanalyse (OCAD) en de ondersteunende diensten als op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I.

XI.1. AANBEVELINGEN IN VERBAND MET DE BESCHERMING VAN DE RECHTEN DIE DE GRONDWET EN DE WET AAN PERSONEN WAARBORGEN

XI.1.1. UITWERKEN VAN EEN VOORSTEL VAN RICHTLIJN I.V.M. MEDELING VAN INFORMATIE DOOR DE VSSE OF DE ADIV AAN WERKGEVERS EN AANPASSING VAN BESTAANDE RICHTLIJNEN[379]

Het Comité beveelde aan dat de Veiligheid van de Staat (VSSE) en de Algemene Dienst Inlichting en Veiligheid (ADIV) binnen zes maanden na het afsluiten van zijn toezichtonderzoek naar '*De uitwisseling van informatie over een werknemer tussen de inlichtingendiesnten en een private- of publieke werkgever*' een voorstel tot richtlijn ter uitvoering van de laatste zinsnede van artikel 19, eerste lid, van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (W.I&V) zou opstellen ten behoeve van respectievelijk de minister van Justitie en van Defensie met het verzoek het voorstel ter goedkeuring voor te leggen aan de Nationale Veiligheidsraad (NVR).

Tevens dient de VSSE zijn richtlijnen ter zake te evalueren en aan te passen aan het wettelijke kader. Gelet op het belang van deze materie, dient deze aanpassing ook te gebeuren binnen een termijn van zes maanden.

---

379 Zie Hoofdstuk 'I.3. De uitwisseling van informatie over een werknemer tussen de inlichtingendiensetn en een private- of publieke werkgever'

Verder beveelt het Comité aan dat de wetgever zou verduidelijken of artikel 19, eerste lid, laatste zin W.I&V ook een verplichting inhoudt om onder bepaalde gevallen *verplicht* te antwoorden op een vraag of om *op eigen initiatief* gegevens te verstrekken. In afwachting van een wetgevend initiatief moet deze kwestie geregeld worden in de richtlijn van de Nationale Veiligheidsraad.

XI.1.2. RICHTLIJNEN INZAKE DE OPVOLGING VAN POLITIEKE MANDATARISSEN[380]

Het Vast Comité I herhaalt met klem zijn eerdere aanbeveling uit 2013 dat de ADIV eenduidige richtlijnen moet opstellen met betrekking tot de inwinning, de verwerking, de raadpleging, de opslag en de archivering van gegevens van politieke mandatarissen.

Het Vast Comité I beveelt ook aan dat de inlichtingendiensten in hun rapportage de nodige aandacht moeten besteden aan de positie van een in een verslag vermeld persoon ten aanzien van de dreiging (slachtoffer, actor, passant, …).

XI.2. AANBEVELINGEN IN VERBAND MET DE COÖRDINATIE EN DE EFFICIËNTIE VAN DE INLICHTINGENDIENSTEN, HET OCAD EN DE ONDERSTEUNENDE DIENSTEN

XI.2.1. AANBEVELINGEN M.B.T. HET OCAD EN ZIJN (NIEUWE) ONDERSTEUNENDE DIENSTEN[381]

Informatieverstrekking of opleiding voor bij het OCAD gedetacheerde personeelsleden van het Directoraat-generaal Penitentiaire Inrichtingen

Er werd vastgesteld dat de personeelsleden gedetacheerd uit het directoraat-generaal Penitentiaire Inrichtingen (DG EPI) weinig of zelfs helemaal geen bezoeken brengen aan hun dienst van oorsprong en zeggen dat ze niet op de hoogte worden gebracht van eventuele wijzigingen die zijn doorgevoerd binnen hun vroegere dienst. Een regelmatige informatieverstrekking of opleiding die hen in staat stelt hun kennis van hun ondersteunende dienst van oorsprong bij te werken en op de hoogte te blijven van eventuele wijzigingen, zoals wetgevende of van inwendige orde bijvoorbeeld, zou een meerwaarde zijn.

380 Zie Hoofdstuk 'I.8. De opvolging van politieke mandatrissen'

381 Zie hoofdstukken 'I.1 De ondersteunende diensten van het OCAD' en 'I.2. Het OCAD en de 'bijkomende' ondersteunende diensten'.

BINII voor het DG EPI en de dienst Erediensten en Vrijzinnigheid

Het zou opportuun zijn dat de FOD Justitie snel beschikt over het BINII-systeem (*B*elgian Intelligence Network Information Infrastructure) om beide diensten toe te laten makkelijker geclassificeerde gegevens uit te wisselen.

Toegang Thesaurie tot GGB

Het zou opportuun zijn dat de Thesaurie zo snel mogelijk beschikt over haar toegangen tot de Gemeenschappelijke gegevensbanken (GGB).

Een functionele mailbox voor de dienst Erediensten en Vrijzinnigheid

Het zou opportuun zijn dat de dienst Erediensten en Vrijzinnigheid beschikt over een functionele mailbox want dergelijke mailbox zou een opvolging van elk verzoek of elk inkomend en uitgaand document garanderen door alle leden van de cel "terrorisme en radicalisme".

Een toegang tot de GGB voor de dienst Erediensten en Vrijzinnigheid in overeenstemming met het wettelijk kader

Er werd vastegesteld dat de dienst Erediensten en Vrijzinnigheid beschikte over een toegang tot de Gemeenschappelijke gegevensbank 'Haatpropagandisten' (GGB HP) die ruimer was dan de toegang waarin het Koninklijk besluit van 23 april 2018 betreffende de gemeenschappelijke gegevensbank Haatpropagandisten (KB HP) voorziet. Het Controleorgaan voor politionele informatie (COC) en het Vast Comité I verzochten de verwerkingsverantwoordelijken een einde te stellen aan de gevallen van onregelmatige toegang en bevolen de Federale Politie aan om de technische oplossingen te ontwikkelen die nodig zijn om de toegang door deze dienst in overeenstemming te brengen met de geldende wetgeving (i.e. enkel onrechtstreekse toegang tot de GGB HP). Het COC en het Vast Comité I bevolen de verwerkingsverantwoordelijken ook aan om op juridisch en operationeel vlak na te gaan of de regelgeving betreffende de toegang van de dienst Erediensten en Vrijzinnigheid al dan niet moest worden herzien.

XI.2.2. CORRECTE TOEPASSING VAN DE MOGELIJKHEID OM VEILIGHEIDSSCREENINGS AAN TE VRAGEN[382]

Het Comité nodigt spelers uit de publieke en private sector uit om te onderzoeken voor welke functies, toelatingen of vergunningen bepaalde potentiële dreigingen preventief kunnen ondervangen worden door een beroep te doen op het systeem van de veiligheidsscreenings uit de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (W.C&VM). Het Comité benadrukt wel dat dit systeem oordeelkundig moet gebruikt worden en niet mag leiden tot een ongebreidelde toepassing.

XI.2.3. VERPLICHTE MELDING NAAR WERKGEVER IN GEVAL VAN OPNAME IN EEN GEMEENSCHAPPELIJKE GEGEVENSBANK[383]

Het Comité suggereert om te onderzoeken of het nuttig zou zijn om een verplichte melding naar de werkgever in het leven te roepen ten aanzien van iedere (kandidaat-)werknemer die is opgenomen in de Gemeenschappelijke gegevensbank Terrorist Fighters of Haatpredikers.

XI.2.4. EEN BREED DEBAT OVER DE TAKEN EN DE PRIORITEITEN VAN DE INLICHTINGENDIENSTEN[384]

Het Vast Comité I beveelt een breder maatschappelijk (parlementair) debat aan over het in de Inlichtingenwet van 1998 voorziene takenpakket van de twee inlichtingendiensten en de hieraan gekoppelde prioriteitenstelling. Dit vergt een wetenschappelijk of 'strategisch' onderbouwde discussie, want daarvoor bestaat momenteel geen wetenschappelijke methode, over de beschikbaarstelling van voldoende capaciteiten en middelen om elk dienst in staat te stellen alle bedreigingen van de (inter)nationale veiligheid naar behoren op te sporen, te bewaken en te beheersen. De inlichtingen- en veiligheidsdiensten moeten het voorwerp van parlementaire aandacht uitmaken, en dit niet alleen op het moment dat er zich individuele problemen voordoen (steekvlampolitiek).

---

382 Zie Hoofdstuk 'I.3. De uitwisseling van informatie over een werknemer tussen inlichtingendiensten en een private- of publieke werkgever'

383 *Ibid.*

384 Zie Hoofstukken 'I.5. De opvolging van schadelijke sektarische organisaties en criminele organisaties' en 'I.9. Het opsporen en opvolgen van de radicalisering van een militair: de zaak Jürgen Conings'. Deze aanbeveling kreeg een zeer hoge prioriteit.

XI.2.5. MEER VEILIGHEIDSSCREENINGS VAN MILITAIREN EN BURGERPERSONEEL BIJ DEFENSIE[385]

Het Vast Comité I stelt vast dat de militairen van het departement Defensie, met uitzondering van degenen met een veiligheidsmachtiging, slechts aan één veiligheidsverificatie worden onderworpen, namelijk helemaal aan het begin van hun aanwerving, terwijl duidelijk blijkt dat de integriteit van sommige militairen in de loop van hun opeenvolgende activiteiten of in de loop van de tijd wel degelijk een probleem zou kunnen vormen. Dit betekent dat deze leden alleen als zodanig bekend zullen zijn wanneer zij een bedreiging vormen die door de ADIV werd opgespoord.

Het Vast Comité I merkt op dat burgers van het departement Defensie en reservisten, in tegenstelling tot militairen, op enkele uitzonderingen na, bij hun aanwerving niet worden onderworpen aan een veiligheidsverificatie. Dit verschil in behandeling kan slechts worden gerechtvaardigd indien het ongepaste gebruik van de functie die zij uitoefenen de fundamentele belangen van de Staat niet in gevaar kan brengen. Het Vast Comité I beveelt daarom aan dat de bevoegde administratieve overheid onderzoekt of de door de Wet van 23 februari 2018 gecreëerde mogelijkheid om veiligheidsverificaties te vragen, niet moet worden geactiveerd. Deze wet maakt het mogelijk om na een risico-, dreigings- en impactanalyse te bepalen voor welke functies een veiligheidsadvies is aangewezen.

De wet staat ook toe dat een dergelijke beoordeling om de vijf jaar wordt uitgevoerd en dat in de tussentijd een positief advies wordt omgezet in een negatief advies. In die zin biedt deze wet een interessante mogelijkheid die momenteel niet geldt voor militairen; zij kunnen slechts één keer worden gescreend (d.w.z. bij hun aanwerving). Er moet echter voor ogen worden gehouden dat het huidige 'negatieve advies' voor militairen een *de facto* 'negatieve beslissing' impliceert, terwijl de gevolgen van een 'negatief advies' onder de Wet van 2018 toekomt aan de overheid die het advies vraagt.

Het Vast Comité I merkt op dat leerlingen van de Koninklijke Militaire School (KMS) en van andere scholen die afhangen van het departement Defensie, in tegenstelling tot militairen, op enkele zeldzame uitzonderingen na, bij hun aanwerving niet worden onderworpen aan een veiligheidsverificatie. Dit verschil in behandeling valt niet te rechtvaardigen en deze situatie vormt noodzakelijkerwijs een risico voor departement Defensie dat medewerkers in dienst neemt zonder dat het idealiter degenen heeft kunnen opsporen die een bron van bedreiging zouden kunnen vormen of die niet over de morele kwaliteiten zouden beschikken die de uitoefening van hun taken onontbeerlijk zijn, waarbij de tijd ook voorbijgaat.

Het Vast Comité I merkt op dat buitenlandse studenten van de KMS bij hun toelating niet worden onderworpen aan een veiligheidsverificatie. Die zou in elk

[385] Zie Hoofdstuk 'I.7. Veiligheidsscreenings van militairen en burgerpersoneel bij Defensie'

geval moeten worden voorafgegaan door een risicoanalyse door de ADIV. Ze zou voorafgaand en systematisch zijn per geval van kandidaat-leerling.

Deze aanbevelingen zouden moeten worden toegepast voor alle scholen die afhangen van het departement Defensie.

XI.2.6. DE OPRICHTING VAN EEN COHERENT 'INTELLIGENCE' GEHEEL[386]

Het Vast Comité I beveelt de oprichting aan van een coherent 'intelligence' geheel bij Defensie die de volledige militaire inlichtingendienst omvat en de permanente opleiding en ontwikkeling van het betrokken personeel mogelijk maakt. Dit moet de beschikbaarheid van binnen de ADIV opgeleid militair personeel van hoge kwaliteit mogelijk maken. Deze eenheid moet over een maximale autonomie beschikken bij het beheer en de ontwikkeling van haar personeel. Deze aanbeveling is van fundamenteel belang en wordt al vele jaren door het Comité naar voren gebracht.

XI.2.7. STABILITEIT IN HET PERSONEELSBELEID BIJ DE ADIV

Het Vast Comité I beveelt ook aan om stabiliteit te brengen in de inzet van militair personeel en om frequent verloop, zoals dat elders bij Defensie voorkomt, te vermijden. Stabiliteit van vijf jaar moet het doel zijn voor sleutelposities.

XI.2.8. BEKRACHTIGING INLICHTINGEN- (EN VEILIGHEIDS-) STUURPLAN

Het Vast Comité I beveelt aan om het Inlichtingen- (en Veiligheids-) stuurplan onverwijld te bekrachtigen en dat dit jaarlijks wordt goedgekeurd en geëvalueerd en aan de Minister van Defensie (MOD) ter bekrachtiging wordt voorgelegd. Dit strategisch plan bepaalt, overeenkomstig de wettelijke verplichtingen en opdrachten van de ADIV, de middelen die moeten worden ingezet en, rekening houdend met deze middelen, de prioriteiten die worden toegekend.

---

386 De aanbevelingen opgenomen in de punten XI.2.6. tot en met XI.2.16. zijn ontleend aan het toezichtonderzoek naar het opsporen en opvolgen van de radicalisering van een militair: de zaak Jürgen Conings (zie Hoofdtsuk I.9.). Deze aanbevelingen kregen een zeer hoge prioriteit.

XI.2.9. BETERE INTERNE COMMUNICATIE BINNEN ADIV

Het Vast Comité I beveelt aan dat de ADIV aanvullend communiceert naar het personeel toe om hen beter vertrouwd te maken met de structuur, de communicatie en de beslissingslijnen, vooraleer wijzigingen te overwegen. Het heeft geen zin om alle realisaties zomaar in twijfel te trekken. Wel moet waar nodig de nieuwe structuur verankerd worden. Het Comité was er zich wel van bewust dat de "Covid"-periode niet bevorderlijk was voor de interne communicatie die essentieel is voor de lancering van een nieuwe structuur.

XI.2.10. BETERE COMMUNICATIE TUSSEN ADIV EN ANDERE OVERHEDEN BIJ TUCHT- OF STRAFBARE FEITEN

Het Vast Comité I beveelt aan om de communicatiekanalen en –procedures, zowel met de tuchtrechtelijke overheden van Defensie als met de politiediensten en gerechtelijke overheden, te evalueren. De ADIV moet steeds tijdig op de hoogte worden gebracht van de administratieve maatregelen, beslissingen (plaatsing onder aanhoudingsmandaat, inbeschuldigingsstelling,…) of strafrechtelijke veroordelingen met betrekking tot een personeelslid van Defensie. Dit soort communicatie moet systematische gebeuren zodat te nemen maatregelen kunnen worden onderzocht, meer bepaald met betrekking tot de veiligheidsmachtigingen.

XI.2.11. BETERE INTERNE COMMUNICATIE DOOR ADIV NAAR COMMANDO EN MOD

Het Comité beveelt aan dat de ADIV duidelijke interne richtslijnenn opstelt voor de informatiestroom naar het Commando en de minister van Defensie. Deze informatiestroom moet gestandaardiseerd en nauwkeurig zijn en de informatie bevatten die nodig is voor besluitvorming op het hoogste niveau. Dit is een voorwaarde voor een adequate controle van de werking van de organisatie en maakt deel uit van de organisatie en ontwikkeling van een intern controlesysteem.

XI.2.12. ACTIEVERE OPVOLGING VAN EXTREMISME BINNEN DEFENSIE DOOR DE ADIV

Het Vast Comité I beveelt aan dat de ADIV de nodige maatregelen treft om een actieve deelname aan de Local Task Forces (LTF) te verzekeren. Het Comité beveelt tevens aan dat er dringend interne richtlijnen en een strategie worden opgesteld over de rol van de ADIV binnen het Strategie TER (de opvolger van het Plan R)

wat betreft het opvolgen van actieve (reserve-) militairen. Meer bepaald dient te worden vastgelegd wat de precieze inbreng van de ADIV dient te zijn in enerzijds de werking van de nationale en thematische werkgroepen, en anderzijds in de LTF.

Het Vast Comité I beveelt ook aan dat de ADIV voldoende middelen inzet om tegemoet te komen aan de detectie van extremisme binnen Defensie. Dit dient het resultaat te zijn van een voorafgaande analyse van welke middelen voor welke opdracht/dreiging vereist zijn.

Tevens formuleerde het Comité de aanbeveling dat de ADIV richtslijnen opstelt met betrekking tot de raadpleging en de voeding van de GGB TF door zijn medewerkers.

XI.2.13. EVALUATIE VAN HET NATIONAAL STRATEGISCH INLICHTINGENPLAN (NSIP)

Het Vast Comité I verzoekt de ministers van Justitie en Defensie een evaluatie te verrichten van het eerste NSIP, teneinde de synergieën tussen de twee diensten in het licht van deze evaluatie te versterken.

XI.2.14. BETERE REGELS EN KENNIS INZAKE OPNAME ENTITEIT IN DE GEMEENSCHAPPELIJKE GEGEVENSBANK

Het Vast Comité I nodigt de minister van Defensie uit om samen met de bevoegde ministers de nodige initiatieven te nemen opdat de wetgevende en/of regelgevende teksten voortaan de regels zouden vaststellen voor de eventuele inschrijving van een entiteit in de Gemeenschappelijke gegevensbank 'Terrorist Fighters' (GGB TF) of de toewijzing van een bepaald niveau aan een lid door het OCAD.

Het Vast Comité I verzoekt de minister van Defensie om de bevoegde ministers te verzoeken ervoor te zorgen dat het OCAD zijn personeel op dit gebied regelmatig bijschoolt.

Het Vast Comité I beveelt aan dat het IF5-reglement wordt herzien om het in overeenstemming te brengen met de huidige structuur en uitrusting van Defensie. Met name moeten in de herziene IF5 de taken van de veiligheidsbeambte en zijn of haar prerogatieven duidelijk worden omschreven. Ook moeten de maatregelen voor en de controle op munitiedepots, met inbegrip van de rol en de taken van de ADIV, formeel worden vastgelegd.

XI.2.15. INFORMATIEUITWISSELING TUSSEN DE INLICHTINGENDIENSTEN OVER DEFENSIEPERSONEEL

Het Vast Comité I beveelt aan dat de VSSE de ADIV systematisch op de hoogte brengt wanneer het over informatie beschikt betreffende het (burgerlijk of militair) defensiepersoneel. Bovendien lijkt het noodzakelijk dat de twee diensten een samenwerkingsovereenkomst sluiten inzake het toezicht op defensiepersoneel.

XI.2.16. NALEVING HUMINT-AFSPRAKEN [387]

Het Vast Comité I beveelt de naleving aan van de door de Nationale Veiligheidsraad goedgekeurde afspraken tussen de inlichtingendiensten wat betreft de HUMINT-afspraken uit het Nationaal Strategisch Inlichtingenplan.

XI.2.17. NALEVING INFORMATIEOVERDRACHT NAAR HET OCAD

Het Vast Comité I beveelt aan, zoals voorzien in de OCAD-Wet, dat de inlichtingendiensten daadwerkelijk alle informatie die pertinent is voor de analyse en evaluatie van de dreiging stelselmatig en tijdig, binnen de wettelijk voorziene termijnen, bezorgen aan het OCAD.

XI.2.18. EEN FLEXIBEL EN PROACTIEF REKRUTERINGSBELEID VOOR DE INLICHTINGENDIENSTEN

Het Vast Comité I beveelt aan dat de mogelijkheden worden gecreëerd opdat de inlichtingendiensten een flexibel en proactief rekruteringsbeleid kunnen voeren. Dit vereist een betere samenwerking met SELOR, maar ook een versterking van het personeel dat nodig is om de in de komende jaren verwachte toevloed van burgerpersoneel in goede banen te leiden.

---

[387] De aanbevelingen opgenomen in de punten XI.2.17. tot en met XI.2.31. zijn ontleend aan het toezichtonderzoek naar het opsporen en opvolgen van de radicalisering van een militair: de zaak Jürgen Conings (zie Hoofdtsuk I.9.). Deze aanbevelingen kregen een hoge prioriteit.

XI.2.19. EEN KWALITETISVOLLE DIGITALE OMGEVING

Om het personeel aan zich te binden, moet de ADIV bovendien beschikken over een digitale omgeving die in overeenstemming is met zijn verplichtingen en opdrachten. Uit het laatste verslag van het Comité over dit onderwerp blijkt dat de algemene IT-infrastructuur ontoereikend is voor een dienst van dit belang.

XI.2.20. EEN UNIFORME METHODOLOGIE INZAKE DREIGINGSEVALUATIE IN DE INLICHTINGENSECTOR

Het Vast Comité I beveelt aan, met het oog op het verbeteren van de communicatie tussen de verschillende partners in de inlichtingensector (VSSE en OCAD in het bijzonder) dat de ADIV zich zo veel als mogelijk op dezelfde lijn plaatst van de methodologieën die al zijn ontwikkeld en goedgekeurd door zijn partners, zodat dezelfde dreiging in dezelfde mate aandacht krijgt binnen de inlichtingengemeenschap.

Deze methodologie dient een actualisering van de individuele fiches in te houden, zowel voor wat betreft de te verzamelen gegevens als voor de te ondernemen acties om de dreiging te beteugelen.

Het geheel van de 'watchlist' dient het voorwerp uit te maken van een periodieke herbeoordeling, aan het eind waarvan de dreigingsniveaus worden geëvalueerd en de vastgestelde dreigingen worden gehandhaafd, naar boven of beneden worden bijgesteld, of zelfs volledig uit het informatiesysteem worden verwijderd wanneer uit de uitgevoerde analyse blijkt dat de aandacht van de ADIV niet langer (of niet) vereist is.

Het Vast Comité I beveelt tevens aan dat het beginsel van de 'watchlist' systematisch wordt toegepast voor alle bedreigingen die onder de bevoegdheid van de ADIV vallen, d.w.z. ook die welke slechts een minimaal niveau van toezicht vereisen (passief toezicht), maar niettemin toezicht vereisen. Zodra de 'watchlist' de dreigingsniveaus en de te nemen follow-up-maatregelen bevat, is er geen reden meer om twee afzonderlijke documenten te handhaven: het moet een alomvattend beeld kunnen geven van de dreiging.

XI.2.21. HET BELANG VAN DIVERSE REGLEMENTEN

Het Vast Comité I nodigt de Minister van Defensie uit om de COL 8/2014, geactualiseerd in januari 2018, bij de Minister van Justitie in herinnering te brengen en er op aan te dringen dat die systematisch wordt nageleefd.

Het Vast Comité I beveelt aan om de regels (SOP's) te harmoniseren en te centraliseren.

Het Vast Comité I beveelt aan dat de ADIV, en in het verlengde daarvan Defensie, het plan Strategie TER ter harte neemt en meer in een constructieve geest samenwerkt.

XI.2.22. TUCHTRECHTELIJK GEZAG OVER HET BURGERPERSONEEL ADIV

Het Vast Comité I beveelt andermaal aan om tegemoet te komen aan de actuele situatie dat het hoofd van de ADIV geen tuchtrechtelijk gezag heeft over het burgerpersoneel van de ADIV. Er moet absoluut een eenheid van bevel komen en geen twee parallelle commandostructuren (een civiele en een militaire), zoals nu het geval is.

XI.2.23. INZET INLICHTINGENMETHODEN

Het Vast Comité I beveelt aan om maximaal gebruik te maken van de mogelijkheden (o.a. bijzondere inlichtingenmethoden (BIM), Humint), in samenwerking met de VSSE teneinde de middelen te maximaliseren, die de wetten toelaten om de informatie te verzamelen.

XI.2.24. AANWERVING JURISTEN

Het Vast Comité I beveelt aan dat meer juristen zouden worden aangeworven die belast zijn met een juridisch-operationele functie ter ondersteuning van de collecte-medewerkers en analisten.

XI.2.25. INVESTEREN IN MANAGEMENT

Het Vast Comité I beveelt aan dat de ADIV investeert in een '*knowledge management* strategie'.

Het Vast Comité I beveelt aan om het *Steering Committee* te hervormen tot een volwaardig en daadwerkelijk directiecomité dat moet worden aangevuld met een verantwoordelijke collecte, een verantwoordelijke analyse en eventueel een jurist om de coördinatie en de synchronisatie van alle inlichtingenactiviteiten te verzekeren. Zij moet worden onttrokken aan het beheer van projecten op middellange en lange termijn en aan haar betrokkenheid bij de basislogistiek. Binnen de ADIV is

voorzien in andere entiteiten om deze taken uit te voeren, maar door personeelsgebrek worden zij niet naar behoren uitgevoerd.

XI.2.26. VERDUIDELIJKING COUNTERINTELLIGENCE BINNEN ADIV

Het Vast Comité I beveelt aan dat er binnen Defensie bijkomende inspanningen worden geleverd om de opdracht van counter*intelligence* te verduidelijken en uit te dragen naar alle geledingen van de Krijgsmacht.

XI.2.27. WERKING VEILIGHEIDSOFFICIEREN BINNEN ADIV

Het Vast Comité I beveelt aan dat de ADIV de veiligheidsofficieren (S2) meer bewust maakt van alle mogelijke veiligheidsproblemen, hen responsabiliseert en hen aanzet tot proactieve samenwerking met de eenheden en de ADIV. De ADIV dient dan ook een vertrouwensrelatie uit te bouwen met de diverse veiligheidsofficieren.

XI.2.28. VASTSTELLING RADICALISERINGSINDICATOREN DOOR ADIV

Het Vast Comité I beveelt met betrekking tot de opsporing van radicalisering aan dat de ADIV specifieke instructies geeft om duidelijke indicatoren van radicalisering vast te stellen.

XI.2.29. WEDERZIJDS ZICHT OP OPGEVOLGDE ENTITEITEN DOOR VSSE EN ADIV

Het Vast Comité I beveelt aan dat naar een informaticaoplossing (hit/no hit) moet gezocht worden zodat de inlichtingendiensten kennis kunnen nemen van elkaars op te volgen entiteiten, met alle respect voor elkaars finaliteit en het brongeheim.

XI.2.30. MIDDELEN IN DE STRIJD TEGEN EXTREMISME

Het Vast Comité I beveelt aan dat de ADIV voldoende middelen inzet om tegemoet te komen aan de detectie van extremisme binnen Defensie. Dit dient het

resultaat te zijn van een voorafgaande analyse van welke middelen voor welke opdracht/dreiging vereist zijn.

XI.2.31. ACTUALISERING BESTAANDE REGLEMENTERINGEN[388]

De richtlijnen van het Ministerieel Comité voor inlichting en veiligheid handelend over allerhande veiligheidsvoorschriften zouden moeten geactualiseerd worden (omvang veiligheidsonderzoeken, classificatieregels, bewaring geclassificeerde stukken, informatieveiligheid, taken veiligheidsofficieren). Deze richtlijnen dateren allen van het jaar 2001.

Het Vast Comité I nodigt de minister van Defensie uit om met haar bevoegde collega's de opmaak van een gemeenschappelijke richtlijn voorop te stellen om de wettelijke criteria (Wet 11 december 1998) nader te bepalen.

XI.2.32. CUMUL BINNEN DEFENSIE

Het Vast Comité I beveelt Defensie aan na te gaan of het passend is militairen toe te staan een bijkomende beroepsactiviteit uit te oefenen en of dit strookt met de waardigheid van het ambt, en zo ja, welke taken in aanmerking kunnen komen.

XI.2.33. WERKING VAN DE GEMEENSCHAPPELIJKE GEGEVENSBANKEN BINNEN DE ADIV

Het Vast Comité I beveelt aan dat de ADIV zijn personeel informeert over het bestaan van de GGB TF en hen sensibiliseert over zijn belang en zijn gebruik. Tevens moet een scenario worden opgesteld voor de eventuele opname van een lid in de GGB TF of de toekenning van een bepaald dreigingsniveau aan een lid door het OCAD.

Het Vast Comité I beveelt aan dat de inlichtingendiensten verantwoordelijken aanzetten om op systematische en dagelijkse wijze de GGB TF te consulteren en de informatie waar nodig te delen met de hiërarchische lijn tot op het hoogste niveau. De ADIV dient ook hoogdringend de finaliteit (raadplegen, voeden…) van de gemeenschappelijke gegevensbanken op te nemen in zijn werking. Overigens dient de ADIV de lijst van gebruikers van de GGB TF systematisch te actualiseren.

---

388 De aanbevelingen opgenomen in de punten XI.2.32. tot en met XI.2.36. zijn ontleend aan het toezichtonderzoek naar het opsporen en opvolgen van de radicalisering van een militair: de zaak Jürgen Conings (zie Hoofdtsuk I.9.). Deze aanbevelingen kregen een prioriteit van 'gemiddelde urgentie'.

XI.2.34. MELDING EN OPVOLGING VEILIGHEIDSINCIDENTEN BINNEN DE ADIV

Het Vast Comité I beveelt aan dat de ADIV van ieder veiligheidsincident een uitvoerig verslag opmaakt dat alle dimensies (niet alleen technisch, maar ook op het vlak van het gedrag), onderzoekt en analyseert, maar vooral wanneer één van de betrokkenen houder is van een veiligheidsmachtiging. Dit verslag moet worden bezorgd aan de bevoegde veiligheidsautoriteit, eventueel samen met een voorstel van besluit.

XI.2.35. SAMENWERKING VEILIGHEIDSBUREAUS ADIV EN VSSE

Het Vast Comité I beveelt aan dat het veiligheidsbureau van de VSSE en de Directie S van de ADIV nauwer en formeler samenwerken, middels het afsluiten van een protocolakkoord.

XI.2.36. COHERENT GEBRUIK VAN DREIGINGSNIVEAUS EN COMMUNICATIE VAN EVALUATIES DOOR HET OCAD[389]

Bij het toekennen van een dreigingsniveau (1,2,3 of 4) wordt bij de registratie in de GGB ook een categorie voor de opvolging (A, B of C) toegekend. De beide parameters staan los van elkaar. De Vaste Comités I en P bevelen aan om een grotere coherentie en harmonisatie tussen het dreigingsniveau enerzijds en de opvolgingscategorie anderzijds na te streven.

Voor wat betreft de communicatiewijze en de bestemmelingen van de dreigingsanalyses van het OCAD bestaat er een verschil naargelang het om een punctuele dreigingsevaluatie gericht tegen personen, groeperingen of gebeurtenissen gaat, dan wel of het een evaluatie van de individuele dreiging door een persoon betreft. De Vaste Comités I en P bevelen aan om op het vlak van de communicatie van de evaluatie van de dreiging door een persoon, naast de registratie in de GGB, deze dreigingsanalyse ook te communiceren naar de belanghebbende diensten die de dreigingsevaluaties tegen personen ontvangen overeenkomstig de OCAD-wet.

---

389 Zie Hoofdstuk 'I.10. De rol van het OCAD in de opvolging van de militair Jürgen Conings'. Dit onderzoek werd samen met het Vast Comité P uitgevoerd.

Ondanks het pragmatisme dat het OCAD hanteert bij de toepassing van de Omzendbrief van de minister van Binnenlandse Zaken en de minister van Justitie betreffende de informatie-uitwisseling rond en de opvolging van terrorist fighters en haatpropagandisten lijkt het de Vaste Comités I en P aangewezen om de Omzendbrief aan te passen aan de nieuwe categorieën die met het wijzigingsbesluit d.d. 20/12/2019 aan de GGB werden toegevoegd, m.n. de potentieel gewelddadige extremisten (PGE) en terrorismeveroordeelden (TV).

In de lijn met de voorgaande aanbeveling zou het zinvol kunnen zijn om bij een aanpassing van de Omzendbrief van de ministers van Binnenlandse Zaken en de Justitie betreffende de informatie-uitwisseling rond en de opvolging van terrorist fighters en haatpropagandisten de mogelijkheden te evalueren om de bestaande maatregelen voor het reduceren van de dreiging uit te breiden en verder te specifieren naar de bestaande en nieuwe categorieën.

XI.2.37. SCHRIFTELIJKE COMMUNICATIE BIJ TOEPASSING VAN ARTIKEL 19 W.I&V[390]

In artikel 19 W.I&V wordt niet gespecificeerd hoe de informatie aan de betrokken ministers e.a. moet worden meegedeeld. Het Vast Comité I is van mening dat de mededeling om redenen van rechtszekerheid schriftelijk dient te geschieden, behalve in uiterst dringende gevallen. Het doel is discussies achteraf te voorkomen en parlementaire (of zelfs juridische) controle mogelijk te maken. Het Comité beveelt aan dat het beginsel van systematische schriftelijke communicatie onverwijld wordt toegepast.

XI.2.38. OMGANG MET GECLASSIFICEERDE INFORMATIE DOOR DERDE OVERHEDEN[391]

Ontvangers van geclassificeerde informatie moeten voorzichtige omspringen met dergelijke nota's en zich bewust zijn van de schade die zij kunnen toebrengen aan de personen op wie de nota's betrekking hebben en aan de goede werking van de inlichtingen- en veiligheidsdiensten zelf.

Het Vast Comité I roept de Veiligheid van de Staat en de nationale veiligheidsoverheid op om binnen zes maanden de nodige initiatieven te nemen om de ontvangers bewust te maken van en te herinneren aan de plichten van veiligheidsofficieren.

---

390 Zie Hoofdstuk 'I.11. De opvolging van een regeringscommissaris door de VSSE'

391 *Ibid.*

XI.2.39. VEILIGHEIDSSCREENINGS VOOR VERTROUWENSFUNCTIES[392]

Het Vast Comité I is van mening dat de uitoefening van bepaalde 'openbare functies' een voorafgaande toetsing van de integriteit, loyaliteit en discretie vereist, zoals de vigerende wetgeving in sommige Europese landen voorschrijft.

Volgens het Comité zou die controle in het bijzonder moeten worden uitgevoerd voor kandidaten voor de functie van regeringscommissaris, maar ook voor andere openbare functies zoals die van aalmoezenier of andere belangrijke functies op federaal, gewestelijk en gemeenschapsniveau.

Bijgevolg vraagt het Vast Comité I aan de regering om tegen het einde van april 2022 de nodige wetgevende initiatieven te nemen, samen met de bevoegde federale ministers. Aan de minister van Defensie wordt gevraagd nader te bepalen of sleutelfuncties bij Defensie moeten worden opgenomen in deze initiatieven. In het tegenovergestelde geval wordt aan de minister gevraagd om de noodzakelijke parallelle wetgevende initiatieven te nemen om het rechtskader vast te stellen voor de controles met betrekking tot de functies die een controle vereisen bij Defensie. Tot slot zou de minister van Justitie ook het initiatief moeten nemen om de kwestie van een voorafgaande controle van sleutelfuncties op de andere bevoegdheidsniveaus op de agenda van een vergadering van het Overlegcomité te plaatsen.

XI.2.40. VERMELDING ONTVANGERS OP UITGAANDE NOTA'S[393]

Het Vast Comité I beveelt aan dat de VSSE in de nota's die zij opstelt, alle ontvangers van de nota's vermeldt en de nota's 'individualiseert' wanneer zij worden verzonden, en dit om lekken te voorkomen.

Als algemene regel beveelt het Vast Comité I aan dat de door het directiecomité gevalideerde nota's van de VSSE onverwijld worden toegezonden aan de in de nota vermelde geadresseerden.

---

392 Zie Hoofdstukken 'I.11. De opvolging van een regeringscommissaris door de VSSE' & 'I.12. Een vernieuwde aandacht voor de Moslimbroederschap'

393 Zie Hoofdstuk 'I.11. De opvolging van een regeringscommissaris door de VSSE'

XI.2.41. HET MEEDELEN VAN DE BEHOEFTEN VAN DE NATIONALE VEILIGHEIDSRAAD AAN DE INLICHTINGENDIENSTEN [394]

Het Vast Comité I verzoekt de NVR aan de inlichtingendiensten het soort en de aard te specificeren van de nota's die hij wenst te ontvangen, alsmede de termijnen voor de toezending ervan.

XI.2.42. SAMENWERKING IN HET KADER VAN DE PROBLEMATIEK VAN DE MOSLIMBROEDERS[395]

Volgens het Vast Comité I is het de taak van de ministers van Justitie en Defensie om met hun collega's van Binnenlandse Zaken de samenwerking tussen de inlichtingendiensten en hun partners (Federale Politie, OCAD enz.) te versterken en samen met de diensten te bepalen wat het geschikte samenwerkingskader is. In 2022 moet een actieplan betreffende de problematiek van de Moslimbroeders worden opgemaakt. Het moet:

- een gemeenschappelijke definitie vaststellen:
  - van het fenomeen en zijn componenten;
  - van het niveau van dreiging dat uitgaat van het fenomeen;
  - een strategie voor opvolging van het fenomeen (met een eventuele taakverdeling overeenkomstig het rechtskader)[396], rekening houdend met de middelen waarover de diensten beschikken;
  - een strategie van bewustmaking van de overheden en administraties (met een bevoegdheidsverdeling overeenkomstig het rechtskader);
- een bijgewerkte lijst opstellen van de verenigingen die verbonden zijn met de Moslimbroeders, alsook van de leden en de sympathisanten van de beweging;
- verzekeren dat er voldoende manschappen zijn om de passende opvolging te garanderen.

XI.2.43. ANALYSE VAN DE MIDDELEN VAN ADIV M.B.T. DE PROBLEMATIEK VAN DE MOSLIMBROEDERS

Het Vast Comité I beveelt de ADIV aan om in 2022 een analyse te maken om te bepalen of de middelen die ze inzet bij de opvolging van de Moslimbroeders voldoende zijn ten opzichte van de ingeschatte waarschijnlijkheid van het risico van

---

394 *Ibid.*

395 De aanbevelingen opgenomen in de punten XI.2.43. tot en met XI.2.46. zijn ontleend aan het toezichtonderzoek 'Een vernieuwde aandacht voor de Moslimbroederschap' (Hoofdstuk I.12.)

396 Deze oefening werd al gemaakt voor de ADIV en de VSSE, en werd opgenomen in de strategische plannen (zie *supra*).

poging tot beïnvloeding door de Moslimbroeders bij Defensie, en dit rekening houdend met de prioriteit die de dienst toekent aan de opvolging van het fenomeen. Als dat niet het geval blijkt te zijn, is het de taak van de ADIV om aan de minister van Defensie te vragen een passend aanwervingsplan op te stellen.

XI.2.44. ALGEMENE BEWUSTMAKING M.B.T. DE PROBLEMATIEK VAN DE MOSLIMBROEDERS

Het Vast Comité I looft de ambitie van de VSSE om een brochure over de Moslimbroeders samen te stellen en die op grote schaal te verspreiden met het oog op bewustmaking; het Comité beveelt de VSSE aan om de brochure ten laatste eind 2022 te verspreiden.

XI.2.45. BEWUSTMAKING VEILIGHEIDSOFFICIEREN DEFENSIE M.B.T. DE PROBLEMATIEK VAN DE MOSLIMBROEDERS

Het Vast Comité I vraagt aan de ADIV ook om interne briefings te organiseren voor de aangewezen veiligheidsofficieren met als doel hen bewust te maken van de problematiek en hun vermogen te vergroten om een concrete dreiging voor Defensie op het spoor te komen.

XI.2.46. ICT IN HET INLICHTINGENPROCES BIJ DE DIRECTIE CYBER VAN DE ADIV[397]

Het Vast Comité I beveelt aan om op ICT-vlak met de volgende punten rekening te houden, zodat een optimale doeltreffendheid van de dienstverlening kan worden gewaarborgd om de strategische doelstellingen te halen:

- De nodige verbintenissen aangaan in verband met het personeelsplan dat aan het Vast Comité I werd voorgesteld;
- Bijkomende maatregelen treffen (*no-break*, bijkomende UPS, monitoring) om de problemen met betrekking tot de elektrische infrastructuur in de wijk op te vangen;
- De *hardware resources* vergroten indien dit nodig zou blijken om een betere dienstverlening aan de gebruikers te waarborgen;
- Voldoende aandacht schenken aan de contracten met externe bedrijven, bijv. door de mogelijkheid van '*on premises*'-software te overwegen (op eigen infrastructuur).

[397] Zie Hoofdstuk 'I.13. Informatie- en communicatietechnologie in het inlichtingenproces bij de Directie Cyber van de ADIV en bij de VSSE'

XI.3. AANBEVELINGEN IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT

XI.3.1. MELDING DOOR DE ADIV VAN DE OPVOLGING VAN POLITIEKE MANDATARISSEN[398]

Het Vast Comité I beveelt de ADIV aan om haar driemaandelijks een overzicht te bezorgen van alle documenten waarin politieke mandatarissen worden vermeld; desgevallend met een '*blanco hit*' zo geen dergelijke vermeldingen werden gemaakt.

[398] Zie Hoofdstuk 'I.8. De opvolging van politieke mandatarissen'

BIJLAGEN

BIJLAGE A.
OVERZICHT VAN DE BELANGRIJKSTE REGELGEVING MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2021 TOT 31 DECEMBER 2021)

Wet van 27 juni 2021 houdende de derde aanpassing van de Algemene uitgavenbegroting voor het begrotingsjaar 2021, *BS* 9 juli 2021

Wet van 14 augustus 2021 tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, alsook tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van het Vast Comité I en van het Vast Comité P, *BS* 8 december 2021

Wet van 23 december 2021 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2022, *BS* 29 december 2021

K.B. 30 september 2021 tot vaststelling van de begunstigden van de acties die door de Federale Overheidsdienst Beleid en Ondersteuning worden gevoerd in het kader van zijn opdracht om culturele, promotie-, amusements-, opleidings- en sportinitiatieven te ontwikkelen, *BS* 4 november 2021

Gemeenschappelijke richtlijn van de Ministers van Justitie en van Binnenlandse Zaken met betrekking tot de bepaling van de nadere regels voor de mededeling van persoonsgegevens en informatie die door de politiediensten worden verwerkt in het raam van hun opdrachten van bestuurlijke en gerechtelijke politie, bedoeld in de artikelen 14 en 15 van de wet op het politieambt, door de politiediensten en tot de rechtstreekse toegang en de rechtstreekse bevraging van de ANG, *BS* 2 februari 2021

Oproep tot kandidaten voor de bestuurlijke Commissie door de inlichtingen- en veiligheidsdiensten belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, *BS* 12 februari 2021

Verlenging bij ministerieel besluit van 3 februari 2021 voor het mandaat van stafdirecteur van de Veiligheid van de Staat van de heer Hugues Brulin voor een periode van 5 jaar, vanaf 1 september 2020, *BS* 16 februari 2021

Bericht voorgeschreven bij artikel 3*quater* van het besluit van de Regent van 23 augustus 1948 tot regeling van de rechtspleging voor de afdeling bestuursrechtspraak van de Raad van State - De vereniging zonder winstoogmerk Syndicaat van de Belgische Politie, "Sypol.be", heeft de nietigverklaring gevorderd van het koninklijk besluit van 24 september 2020 'tot wijziging van het koninklijk besluit van 13 december 2006 houdende het statuut van de ambtenaren van de buitendiensten van de Veiligheid van de Staat', *BS* 16 februari 2021

Beëindiging van de aanstelling voor de Directeur van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 24 februari 2021

Aanstelling ad interim Directeur van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 24 februari 2021

Vast Comité van Toezicht op de Inlichtingen- en Veiligheidsdiensten, vacature voor een Franstalige attaché (m/v/x) van universitair niveau, *BS* 5 maart 2021

Aanwerving bij wijze van detachering en samenstelling van een wervingsreserve van Franstalige commissarissen-auditors (m/v/x) met een bijzondere kennis van gerechtelijk onderzoek en informatiebeheer (Intelligence-led Policing) voor de Dienst Enquêtes van het Vast Comité I, *BS* 18 maart 2021

Oproep tot kandidaten voor de bestuurlijke Commissie door de inlichtingen- en veiligheidsdiensten belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens, *BS* 2 april 2021

Benoeming van de griffier van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *BS* 19 juli 2021

Grondwettelijk Hof: uittreksel uit arrest nr. 64/2021 van 22 april 2021, rolnummer 7416, in zake: de prejudiciële vraag betreffende artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, gesteld door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *BS* 20 september 2021

Aanwerving bij wijze van detachering en samenstelling van een wervingsreserve van Franstalige commissarissen-auditors met een bijzondere kennis van ICT/Data (m/v/x) voor de Dienst Enquêtes van het Vast Comité I, *BS* 1 oktober 2021

Grondwettelijk Hof: uittreksel uit arrest nr. 107/2021 van 15 juli 2021, rolnummer 7261, in zake: het beroep tot vernietiging van de wet van 23 maart 2019 'betreffende de organisatie van de penitentiaire diensten en van het statuut van het penitentiair personeel', ingesteld door Michel Jacobs, *BS* 6 oktober 2021

Oproep tot kandidaten voor het mandaat van tweede Nederlandstalig plaatsvervangend lid van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *BS* 25 november 2021

Aanwerving bij wijze van detachering en samenstelling van een wervingsreserve van Franstalige Commissarissen-auditors met een bijzondere kennis van ICT/Data (m/v/x) voor de Dienst Enquêtes van het Vast Comité I, *BS* 23 december 2021

Vergelijkende selecties, voorafgaande proeven in de vergelijkende selecties, resultaten van de vergelijkende selecties van :

- Nederlandstalige HR Business Partners voor de militaire inlichtingendienst (m/v/x) (niveau A1) voor het Ministerie van Defensie, selectienummer: ANG21132, *BS* 17 mei 2021
- Franstalige HR Business Partners voor de militaire inlichtingendienst (m/v/x) (niveau A1) voor het Ministerie van Defensie, selectienummer: ANG21132, *BS* 17 mei 2021
- Franstalige Data Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21100, *BS* 1 juni 2021
- Nederlandstalige Data Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21130, *BS* 1 juni 2021
- Franstalige Technical Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21102, *BS* 1 juni 2021
- Nederlandstalige Technical Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21134, *BS* 1 juni 2021
- Franstalige Windows/Linux systeembeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21119, *BS* 13 juli 2021
- Nederlandstalige Netwerkbeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21153, *BS* 13 juli 2021

- Nederlandstalige Imagery Intelligence medewerkers voor de Algemene Dienst Inlichting en Veiligheid (ADIV) (m/v/x) (niveau B) voor het Ministerie van Defensie, selectienummer: ANG21216, *BS* 19 juli 2021
- Nederlandstalige Documentalisten Inlichtingen en Veiligheid (m/v/x) (niveau B) voor het Ministerie van Defensie, selectienummer: ANG21218, *BS* 26 juli 2021
- Franstalige Specialisten Query & Reporting (m/v/x) (niveau A1) voor Ministerie van Defensie, selectienummer: AFG21134, *BS* 6 augustus 2021
- Franstalige Attachés veiligheidsmachtiging analisten (niveau A1) voor het Ministerie van Defensie, selectienummer: AFG21135, *BS* 6 augustus 2021
- Franstalige Cyberdefensie Onderzoeker (m/v/x) (niveau A2) voor het Ministerie van Defensie, selectienummer: AFG21156, *BS* 16 augustus 2021
- Franstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B) van de Veiligheid van de Staat, selectienummer: ANG21149, *BS* 29 september 2021
- Nederlandstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B) van de Veiligheid van de Staat, selectienummer: ANG21212, *BS* 29 september 2021
- Nederlandstalige Finance Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21303, *BS* 30 september 2021
- Franstalige Technical Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21102, *BS 2*6 oktober 2021
- Franstalige Windows/Linux systeembeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: AFG21119, *BS 2*6 oktober 2021
- Nederlandstalige Technical Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21134, *M.B.* 26 oktober 2021
- Nederlandstalige Netwerkbeheerders (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21153, *BS 2*6 oktober 2021
- Franstalige Attachés veiligheidsmachtiging analisten (m/v/x) (niveau A1) voor het Ministerie van Defensie, selectienummer AFG21135, *BS* 17 november 2021
- Nederlandstalige voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat, selectienummers: BNG21341 - BNG21342, *BS* 8 december 2021
- Franstalige voor bevordering naar niveau B (specifiek gedeelte) voor de Veiligheid van de Staat, selectienummers: BFG21188 - BFG21189, *BS* 8 december 2021
- van Nederlandstalige Data Officers (m/v/x) (niveau B) voor Veiligheid van de Staat, selectienummer: ANG21130, *BS* 16 december 2021
- Franstalige Data Officers (m/v/x) (niveau B) voor Veiligheid van de Staat, selectienummer: AFG21100, *BS* 16 december 2021
- Nederlandstalige Finance Officers (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21303, *BS* 27 december 2021
- Franstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B) van de Veiligheid van de Staat, selectienummer: AFG21149, *BS* 30 december 2021
- Nederlandstalige Inspecteurs voor de buitendiensten (m/v/x) (niveau B) voor de Veiligheid van de Staat, selectienummer: ANG21212, *BS* 30 december 2021

BIJLAGE B.
OVERZICHT VAN DE BELANGRIJKSTE WETSVOORSTELLEN, WETSONTWERPEN, RESOLUTIES, ORDE MOTIES EN PARLEMENTAIRE BESPREKINGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2021 TOT 31 DECEMBER 2021)

Senaat

Informatieverslag betreffende de noodzakelijke samenwerking tussen de federale overheid en de Gemeenschappen inzake de bestrijding van fake news van S. D'Hose, E. Ampe, R. Daems, W.-F. Schiltz, C. Van Cauter, F. Ahallouch, L. Gahouchi, G.-L. Bouchez, Ph. Dodrimont, V. Durenne, S. Laruelle, A. Miesen, G. Van Goidsenhoven, J.-P. Wahl, K. Brouwers, B. Anciaux, K. De Loor, A. Lambrecht, K. Segers, A. Antoine, A.-C. Goffinet, F. Ben Chikha, S. Bex, R. Demeuse, S. Hoessen, F. Masai, J. Pitseys, H. Ryckmans, Ch. Steenwegen en F. Tahar, Stuk 7-110, *Hand*. Senaat 2021-22, 17 november 2021, nr. 24, 5

Grondwettelijk Hof: het arrest nr. 158/2021, uitgesproken op 18 november 2021, inzake het beroep tot vernietiging van de wet van 1 september 2016 tot wijziging van artikel 127 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 16/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst, ingesteld door Patrick Van Assche en anderen (rolnummer 6672), *Hand*. Senaat 2021-22, 17 december 2021, nr. 25, 43

Kamer van volksvertegenwoordigers

Commissies, adviescomités en afvaardigingen naar de internationale vergaderingen, Parl. St. Kamer 2020-21, nr. 55K0008/008

Moties ingediend in openbare commissievergadering (artikelen 133 tot 141 van het Reglement van de Kamer) op 17 maart 2021 tot besluit van de interpellatie van N. Boukili tot de eerste minister over 'Smals en de openbare aanbestedingen betreffende de digitalisering van de openbare diensten', Parl. St. Kamer 2020-21, nr. 55K105/001

Voorstel van resolutie teneinde te voorzien in evenwaardige middelen voor sites met dreigingsniveau 3 in het afbouwplan van Operation Vigilant Guardian (OVG), Parl. St. Kamer 2020-21, nr. 55K1413/002

Wetsvoorstel tot wijziging van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, met het oog op het invoeren van een actieve kennisgevingsplicht met betrekking tot bepaalde specifieke methoden voor het verzamelen van gegevens, Parl. St. Kamer 2020-21, nr. 55K1763/001

Vast Comité van Toezicht op de inlichtingen en veiligheidsdiensten – benoeming van de eerste plaatsvervanger van een Franstalig lid – ingediende kandidaturen, *Hand*. Kamer 2020-21, 28 januari 2021, CRIV55PLEN085, 38

Voorstel van resolutie betreffende cyberdefensie en de attributie van statelijke cyberaanvallen, Parl. St. Kamer 2020-21, nr. 55K1788/001

Rekenhof, Grondwettelijk hof, Hoge Raad voor de Justitie, Vast comité van toezicht op de politiediensten, Vast comité van toezicht op de inlichtingen- en veiligheidsdiensten, Federale ombudsmannen, Gegevensbeschermingsautoriteit, Benoemingscommissies voor het notariaat, BIM-Commissie, Controleorgaan op de politionele informatie, Federale Deontologische Commissie, Centrale Toezichtsraad voor het Gevangeniswezen,

Mensenrechteninstituut - opvolgingsaudit van het Rekenhof -implementatie van de aanbevelingen, Parl. St. Kamer 2020-21, nr. 55K1924/001

Ordemotie ingediend door P. De Roover, P. Buysrogge en J. Donné: 'de Kamer van Volksvertegenwoordigers: - gelet dat er bewust informatie uit een gedachtewisseling over een toekomstig toezichtonderzoek werd gelekt naar de media, dit door leden van de parlementaire begeleidingscommissie van het Comité P en I; - gelet dat de begeleidingscommissie onder art. 67 van het Kamerreglement valt en de geheimhoudingsplicht geldt met betrekking tot alle informatie die ter zitting verkregen wordt; verzoekt de Kamervoorzitster om een onderzoek te voeren naar de overtreders, om vervolgens onder art. 67 van het Kamerreglement de gepaste sancties te treffen', *Hand*. Kamer 2020-21, 27 mei 2021, CRIV55PLEN106, 26

Mededeling over de inachtneming van artikel 67 van het Reglement, *Hand*. Kamer 2020-21, 27 mei 2021, CRIV55PLEN106, 27

Wetsontwerp houdende de eerste aanpassing van de middelenbegroting voor het begrotingsjaar 2021 (1920/1-8) - wetsontwerp houdende de derde aanpassing van de algemene uitgavenbegroting voor het begrotingsjaar 2021 (1921/1-27) - aanpassing van de begrotingen van ontvangsten en uitgaven voor het begrotingsjaar 2021, algemene toelichting (1919/1), *Hand*. Kamer 2020-21, 24 juni 2021, CRIV55PLEN113, 1

Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, alsook tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van het Vast Comité I en van het Vast Comité P (2064/1-3), *Hand*. Kamer 2020-21, 8 juli 2021, CRIV55PLEN117, 51

Motie ingediend door de heer P. De Roover over: 'vorderen van de aanwezigheid van de premier – art. 100 GW en art. 50 Reglement aangezien de premier maandag in de commissie Gezondheid een verklaring heeft afgelegd over het onderzoek van de Staatsveiligheid in hoofde van de voormalige regeringscommissaris voor het Instituut voor de gelijkheid van mannen en vrouwen en de communicatie van het onderzoek aan het kabinet van de minister van Justitie, *Hand*. Kamer 2020-21, 14 juli 2021, CRIV55PLEN119, 2

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten - vervanging van de griffier - oproep tot kandidaten, *Hand*. Kamer 2020-21, 15 juli 2021, CRIV55PLEN122, 44

Voorstel tot verwerping door de commissie voor Binnenlandse Zaken, Veiligheid, Migratie en Bestuurszaken van het voorstel van resolutie teneinde te voorzien in evenwaardige middelen voor sites met dreigingsniveau 3 in het afbouwplan van Operation Vigilant Guardian (OVG) (1413/1-2), *Hand*. Kamer 2020-21, 15 juli 2021, CRIV55PLEN122, 62

Voorstel van resolutie betreffende cyberdefensie en de attributie van statelijke cyberaanvallen, Parl. St. Kamer 2020-21, nr. 55K1788/001

Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, alsook tot verruiming van de voorwaarden tot benoeming van de respectieve griffiers van het Vast Comité I en van het Vast Comité P, Parl. St. Kamer 2020-21, nrs. 55K2064/001 tot 55K2064/004

Wetsontwerp houdende instemming met de Overeenkomst tussen het Koninkrijk België en het Koninkrijk Spanje inzake de uitwisseling en wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 15 oktober 2015, Parl. St. Kamer 2020-21, nrs. 55K2074/001 tot 55K2074/003

Wetsontwerp houdende instemming met de overeenkomst tussen het Koninkrijk België en de Republiek Finland inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Helsinki op 20 juli 2016, Parl. St. Kamer 2020-21, nr. 55K2075/001

Wetsontwerp houdende instemming met de overeenkomst tussen het Koninkrijk België en de Republiek Cyprus inzake de wederzijdse bescherming van geclassificeerde informatie, gedaan te Brussel op 20 juli 2015, Parl. St. Kamer 2020-21, nr. 55K2085/001

Wetsontwerp houdende instemming met de overeenkomst tussen het Koninkrijk België en Hongarije inzake de uitwisseling en wederzijdse bescherming van geclassificeerde informatie, gedaan te Boedapest op 21 september 2015, Parl. St. Kamer 2020-21, nr. 55K2121/001

Actualisatie van de strategische visie – gedachtewisseling met de minister van Defensie, Parl. St. Kamer 2020-21, nr. 55K2150/001

Voorstel van resolutie betreffende het beschermen van onze nationale veiligheid en strategische onafhankelijkheid tegenover buitenlandse cyberaanvallen door het opstellen van een lijst van hoogrisicoleveranciers, Parl. St. Kamer 2020-21, nr. 55K2167/001

Cyberaanvallen op het IT-systeem van de staat en de overheidsdiensten, Parl. St. Kamer 2020-21, nr. 55K2169/001

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – benoeming van de griffier – ingediende kandidaturen, *Hand.* Kamer 2021-22, 23 september 2021, CRIV55PLEN125, 27

Zaak Jürgen Conings, Parl. St. Kamer 2020-21, nr. 55K2206/001

Activiteitenverslag 2020 van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Parl. St. Kamer 2021-22, nr. 55K2209/001

Voorstel van resolutie over de onafhankelijkheid en de werking van de Gegevensbeschermingsautoriteit, Parl. St. Kamer 2021-22, nr. 55K2246/001

Wetsontwerp houdende omzetting van het Europees wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie, Parl. St. Kamer 2021-22, nrs. 55K2256/001, 55K2256/007 en 55K2256/008

Wetsontwerp houdende de wijziging van de wet van 13 juni 2005 betreffende de elektronische communicatie, Parl. St. Kamer 2021-22, nrs. 55K2257/001 tot 55K2257/004

Onthullingen in de pers met betrekking tot de rol van de banken bij witwaspraktijken (FINCEN FILES), Parl. St. Kamer 2021-22, nr. 55K2261/001

Wetsontwerp houdende de Middelenbegroting voor het begrotingsjaar 2022, Parl. St. Kamer 2021-22, nr. 55K2291/001

Wetsontwerp houdende de Algemene uitgavenbegroting voor het begrotingsjaar 2022, Parl. St. Kamer 2021-22, nrs. 55K2292/001 en 55K2292/006

Verantwoording van de algemene uitgavenbegroting voor het begrotingsjaar 2022, Parl. St. Kamer 2021-22, nrs. 55K2293/006 en 55K2293/007

Beleidsnota, Parl. St. Kamer 2021-22, nrs. 55K2294/002, 55K2294/008, 55K2294/014, 55K2294/016, 55K2294/017, 55K2294/018 en 55K2294/022

Wetsontwerp tot wijziging van diverse bepalingen betreffende de overgang binnen dezelfde personeelscategorie of de opname in een andere hoedanigheid of personeelscategorie van de beroepsmilitair of van de militair met een loopbaan van beperkte duur, Parl. St. Kamer 2021-22, nr. 55K2302/001

Comité I – ontslag van het tweede plaatsvervangend lid van het Nederlandstalig lid, *Hand.* Kamer 2021-22, 10 november 2021, CRIV55PLEN139, 68

Rekenhof, Grondwettelijk hof, Hoge Raad voor de Justitie, Vast Comité van Toezicht op de politiediensten, Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Federale Ombudsmannen, Gegevensbeschermingsautoriteit, Benoemingscommissies voor het Notariaat, BIM-Commissie, Controleorgaan op de politionele informatie, Federale Deontologische Commissie, Centrale Toezichtsraad voor het Gevangeniswezen, Mensenrechteninstituut - Werkzaamheden van de werkgroepen in het kader van het synergieproject - rekeningen van het begrotingsjaar 2020 - begrotingsaanpassingen van het begrotingsjaar 2021- begrotingsvoorstellen voor het begrotingsjaar 2022,

Parl. St. Kamer 2021-22, nrs. 55K2368/001 tot 55K2368/003, *Hand.* Kamer 2021-22, 22 december 2021, CRIV55PLEN152, 27 en *Hand.* Kamer 2021-22, 22 december 2021, CRIV55PLEN154, 17

Wetsvoorstel tot wijziging van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid, teneinde de aanbieders van essentiële diensten in de publieke sector die afhankelijk zijn van netwerk- en informatiesystemen te onderwerpen aan bepaalde eisen inzake beveiliging en meldingen, Parl. St. Kamer 2021-22, nr. 55K2401/001.

BIJLAGE C
OVERZICHT VAN INTERPELLATIES, VRAGEN OM UITLEG EN MONDELINGE EN SCHRIFTELIJKE VRAGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2021 TOT 31 DECEMBER 2021)

Senaat

Schriftelijke vraag van G. D'haeseleer aan de minister van Justitie over de 'personen veroordeeld voor terrorisme - aantal - redenen - nationaliteit' (Senaat 2020-21, 3 maart 2021, Vr. nr. 7-1107)

Schriftelijke vraag van T. Ongena aan de minister van Justitie over 'Turkije - salafisme - buitenlandse staatsinmenging - cijfers en tendensen' (Senaat 2020-21, 5 maart 2021, Vr. nr. 7-1140)

Schriftelijke vraag van T. Ongena aan de minister van Binnenlandse Zaken over 'Turkije - salafisme - buitenlandse staatsinmenging - cijfers en tendensen' (Senaat 2020-21, 5 maart 2021, Vr. nr. 7-1141)

Schriftelijke vraag van R. Daems aan de minister van Justitie over 'sociale media - online privacy - encryptie - Staatsveiligheid - cijfers en tendensen - mogelijke maatregelen' (Senaat 2020-21, 31 maart 2021, Vr. nr. 7-1154)

Schriftelijke vraag van A. Frédéric aan de minister van Justitie over 'sekten - nieuwe praktijken - bestrijding - evolutie van de wetgeving - menselijke, financiële en institutionele middelen - versterking - Coronacrisis - gevolgen - evaluatie' (Senaat 2020-21, 28 april 2021, Vr. nr. 7-1219)

Schriftelijke vraag van R. Daems aan de minister van Justitie over 'ecologie - klimaat - vermindering van de uitstoot - doelstellingen - nakoming van de beloften – 'green spying' - monitoring door en van derde landen - dienst Veiligheid van de Staat - deelneming' (Senaat 2020-21, 3 mei 2021, Vr. nr. 7-1227)

Schriftelijke vraag van T. Ongena aan de minister van Justitie over 'Turkije - Gülen-beweging - haatmisdrijven in België - politiebescherming - incidenten - cijfers en tendensen – Turkse gemeenschap - bescherming - maatregelen' (Senaat 2020-21, 3 mei 2021, Vr. nr. 7-1229)

Schriftelijke vraag van T. Ongena aan de minister van Binnenlandse Zaken over 'extreemrechts - bewakings- en beveiligingsfirma's - infiltratie - cijfers en tendensen' (Senaat 2020-21, 21 mei 2021, Vr. nr. 7-1248)

Schriftelijke vraag van T. Ongena aan de minister van Justitie over 'extreemrechts - risico op aanslagen - overleg - geweld – Corona - chatsites (Covid-19)' (Senaat 2020-21, 21 mei 2021, Vr. nr. 7-1249)

Schriftelijke vraag van T. Ongena aan de minister van Binnenlandse Zaken over de 'cyberaanvallen - cybersecurity - cijfers en tendensen - daders - statelijke actoren - privacy - bescherming - maatregelen' (Senaat 2020-21, 22 juli 2021, Vr. nr. 7-1311)

Schriftelijke vraag van A. Miesen aan de minister van Defensie over de 'Militärdienste - Reform der Nachrichtendienste - Extremismusbekämpfung Militaire diensten - hervorming van de inlichtingendiensten - extremismebestrijding' (Senaat 2020-21, 24 augustus 2021, Vr. nr. 7-1322)

Schriftelijke vraag van E. Ampe aan de minister van Justitie over 'smartphones - statelijke actoren - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1385)

Schriftelijke vraag van E. Ampe aan de minister van Binnenlandse Zaken over 'smartphones - statelijke actoren - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7- 1386)

Schriftelijke vraag van E. Ampe aan de minister van Justitie over 'smartphones - stalkerware - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1387)

Schriftelijke vraag van E. Ampe aan de minister van Binnenlandse Zaken over 'smartphones - stalkerware - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1388)

Schriftelijke vraag van R. Daems aan de minister van Justitie over 'cryptografie - quantumcomputers - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1391)

Schriftelijke vraag van R. Daems aan de minister van Binnenlandse Zaken over 'cryptografie - quantumcomputers - privacy - spionage - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1392)

Schriftelijke vraag van T. Ongena aan de minister van Defensie over de 'drones - politie - spionage - buitenlandse actoren - privacy - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1395)

Schriftelijke vraag van T. Ongena aan de minister van Binnenlandse Zaken over de 'drones - politie - spionage - buitenlandse actoren - privacy - cijfers en tendensen' (Senaat 2021-22, 27 oktober 2021, Vr. nr. 7-1396)

Kamer van volksvertegenwoordigers

Vraag van S. Moutquin aan de Staatssecretaris voor Asiel en Migratie over 'de doorstart van de Grote Moskee te Brussel' (*Hand.* Kamer 2020-21, 6 januari 2021, CRIV55COM322, 16, Vr. nr. 11488C)

Samengevoegde interpellatie en vragen van D. Van Langenhove, K. Metsu en Ph. Pivin aan de minister van Justitie over 'het negatieve advies van Justitie over de doorstart van de Grote Moskee te Brussel' (*Hand.* Kamer 2020-21, 6 januari 2021, CRIV55COM324, 1, Vrs. nrs. 58I, 11916C en 12037C)

Vraag van Th. Francken aan de minister van Justitie over 'het subsidiebesluit voor de Moslimexecutieve' (*Hand.* Kamer 2020-21, 6 januari 2021, CRIV55COM324, 36, Vr. nr. 11948C)

Vraag van D. Safai aan de Staatssecretaris voor Asiel en Migratie over de 'opvolging en screening van geradicaliseerde illegalen en geradicaliseerde erkende vluchtelingen in België' (*Vr. en Ant*. Kamer 2020-21, 12 januari 2021, QRVA34, 151, Vr. nr. 59)

Vraag van E. Burton aan de minister van Binnenlandse Zaken over de 'aanhouding van een geradicaliseerde vóór het politiebureau Brussel Hoofdstad Elsene' (*Vr. en Ant*. Kamer 2020-21, 12 januari 2021, QRVA34, 394, Vr. nr. 110)

Vraag van T. Vandenput aan de minister van Binnenlandse Zaken over de 'update OCAD-databank' (*Vr. en Ant*. Kamer 2020-21, 12 januari 2021, QRVA34, 408, Vr. nr. 119)

Samengevoegde vraag en interpellatie van S. De Wit en M. Dillen aan de minister van Justitie over 'de zwaargewonde cipier in de gevangenis van Gent' (*Hand.* Kamer 2020-21, 13 januari 2021, CRIV55COM334, 9, Vr. nrs. 12064C en 75I)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'de aanpak van het gewelddadige extremisme' (*Hand.* Kamer 2020-21, 13 januari 2021, CRIV55COM336, 49, Vr. nr. 11874C)

Vraag van E. Samyn aan de minister van Buitenlandse Zaken over het 'gevaar voor nieuwe terreurcampagnes in Europa door Islamitische Staat - VN-rapport' (*Vr. en Ant.* Kamer 2020-21, 18 januari 2021, QRVA35, 91, Vr. nr. 117)

Vraag van J. Pillen aan de minister van Defensie over 'het dragen van het uniform door militairen' (*Vr. en Ant.* Kamer 2020-21, 18 januari 2021, QRVA35, 297, Vr. nr. 83)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over 'aanhoudingen voor bedreiging van publieke figuren' (*Vr. en Ant.* Kamer 2020-21, 18 januari 2021, QRVA35, 405, Vr. nr. 171)

Actualiteitsdebat en toegevoegde vragen van B. Segers, H. Rigot, S. Moutquin, T. Vandenput en G. Daems aan de Staatssecretaris voor Asiel en Migratie over 'de zaak-Kucam' (*Hand.* Kamer 2020-21, 19 januari 2021, CRIV55COM337, 1, Vr. nrs. 12673C, 12674C, 12721C, 12723C, 12735C en 12756C)

Vraag van Th. Francken aan de Staatssecretaris voor Asiel en Migratie over 'het terugsturen van extremisten' (*Hand.* Kamer 2020-21, 19 januari 2021, CRIV55COM337, 18, Vr. nr. 12073C)

Vraag van K. Jadin aan de minister van Justitie over 'extreemrechts in België' (*Hand.* Kamer 2020-21, 21 januari 2021, CRIV55PLEN084, 42, Vr. nr. 1286P)

Vraag van J. Pillen aan de minister van Defensie over 'trespassing militaire domeinen' (*Vr. en Ant.* Kamer 2020-21, 27 januari 2021, QRVA36, 349, Vr. nr. 80)

Vraag van A. Ponthier aan de minister van Defensie over 'telefoonfraude vanuit Syrië' (*Vr. en Ant.* Kamer 2020-21, 27 januari 2021, QRVA36, 352, Vr. nr. 92)

Vraag van J. Pillen aan de minister van Defensie over 'verdachte telefoons' (*Vr. en Ant.* Kamer 2020-21, 27 januari 2021, QRVA36, 356, Vr. nr. 98)

Samengevoegde vragen van B. Moyaers, P. Pivin, S. Matheï en K. Van Vaerenbergh aan de minister van Justitie over 'de oproepen op sociale media tot rellen in België' (*Hand.* Kamer 2020-21, 28 januari 2021, CRIV55PLEN085, 2, Vr. nrs. 1303P, 1311P, 1312P en 1315P)

Vraag van M. Freilich aan de minister van Ambtenarenzaken over 'de intimidatiecampagne van Huawei tegen de Belgische regering' (*Hand.* Kamer 2020-21, 24 februari 2021, CRIV55COM387, 6, Vr. nr. 12479C)

Samengevoegde vragen van Th. Francken, D. Ducarme en G. Dallemagne aan de minister van Justitie over 'het CCIF in België' (*Hand.* Kamer 2020-21, 24 februari 2021, CRIV55COM389, 17, Vr. nrs. 14172C, 14331C en 14455C)

Vraag van L. Dierick aan de minister van Justitie over 'de betalingstermijnen bij de FOD Justitie' (*Vr. en Ant.* Kamer 2020-21, 4 maart 2021, QRVA41, 167, Vr. nr. 289)

Vraag van J.-M. Delizée aan de minister van Justitie over de 'declassificering van het zogenaamde Afrika-archief' (*Vr. en Ant.* Kamer 2020-21, 4 maart 2021, QRVA41, 178, Vr. nr. 369)

Actualiteitsdebat en toegevoegde vragen van H. Rigot, B. Segers, P. De Roover, S. Moutquin, G. Daems en E. Platteau aan de Staatssecretaris voor Asiel en Migratie over 'de humanitaire visa' (*Hand.* Kamer 2020-21, 9 maart 2021, CRIV55COM397, 1, Vr. nrs. 14898C, 14920C, 15041C, 15045C, 15067C en 15086C)

Actualiteitsdebat toegevoegde vragen van Th. Francken, J. Pillen, A. Ponthier, H. Bayet, G. Defossé en K. Verduyckt aan de minister van Defensie over 'de verbetering van de voorwaarden van militairen' (*Hand.* Kamer 2020-21, 10 maart 2021, CRIV55COM402, 1, Vr. nrs. 12466C, 13889C, 14028C, 14251C, 14265C, 15097C, 15109C en 15144C)

Vraag van E. Van Hoof aan de minister van Buitenlandse Zaken over een 'Iraanse diplomaat' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 115, Vr. nr. 60)

Vraag van W. Vermeersch aan de minister van Financiën over de 'douane - groeiende bezorgdheid om Chinese scanners' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 205, Vr. nr. 230)

Vraag van M. Freilich aan de minister van Financiën over de 'Nuctech - Chinese scanners' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 208, Vr. nr. 231)

Vraag van K. Metsu aan de minister van Justitie over de 'huiszoekingen in onderzoek naar financiering terreurgroepen' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 288, Vr. nr. 368)

Vraag van A. Ponthier aan de minister van Defensie over de 'samenwerking tussen Belgische universiteiten en de Seven Sons of National Defence in China' (*Vr. en Ant.* Kamer 2020-21, 11 maart 2021, QRVA42, 304, Vr. nr. 124)

Samengevoegde vragen van B. Segers, F. Demon en K. Gabriëls aan de minister van Justitie over 'Operatie Sky' (*Hand.* Kamer 2020-21, 11 maart 2021, CRIV55PLEN091, 24, Vr. nrs. 1428P, 1431P en 1430P)

Samengevoegde vragen van K. Aouasti, N. Gilson, N. Boukili, G. Dallemagne en G. Vanden Burre aan de minister van Digitalisering over 'de eerbiediging van de privacy en het project 'Putting data at the center'' (*Hand.* Kamer 2020-21, 11 maart 2021, CRIV55PLEN091, 35, Vr. nrs. 1427P, 1435P, 1438P, 1445P en 1449P)

Vraag van S. Van Hecke aan de minister van Justitie over 'de opvolging van sektarische organisaties in het kader van de coronacrisis' (*Vr. en Ant.* Kamer 2020-21, 17 maart 2021, QRVA43, 218, Vr. nr. 381)

Vraag van S. Goethals aan de minister van Binnenlandse Zaken over 'de organen onder uw bevoegdheid' (*Vr. en Ant.* Kamer 2020-21, 17 maart 2021, QRVA43, 269, Vr. nr. 313)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'beschermende maatregelen voor leerkrachten – dreiging van radicalisme en terrorisme' (*Vr. en Ant.* Kamer 2020-21, 17 maart 2021, QRVA43, 279, Vr. nr. 318)

Interpellatie van N. Boukili aan de eerste minister over 'Smals en de openbare aanbestedingen betreffende de digitalisering van de openbare diensten' (*Hand.* Kamer 2020-21, 17 maart 2021, CRIV55COM411, 31, Vr. nr. 105I)

Vraag van K. Gabriëls aan de minister van Justitie over 'de digitalisering van de Staatsveiligheid' (*Hand.* Kamer 2020-21, 17 maart 2021, CRIV55COM415, 36, Vr. nr. 15422C)

Vraag van S. Cogolati aan de minister van Justitie over 'de bedreiging en intimidatie van opposanten in België door de Turkse regering' (*Hand.* Kamer 2020-21, 17 maart 2021, CRIV55COM415, 42, Vr. nr. 15442C)

Samengevoegde vragen van B. Pas en K. Metsu aan de eerste minister over 'de groeiende terreurdreiging in Europa' (*Hand.* Kamer 2020-21, 18 maart 2021, CRIV55PLEN093, 33, Vr. nrs. 1462P en 1471P)

Toegevoegde vragen en interpellaties van Ph. Pivin, M. Dillen, N. Boukili, K. Van Vaerenbergh, K. Geens en G. Dallemagne aan de minister van Justitie over 'de begeleiding van en schadevergoeding voor de slachtoffers van terreuraanslagen' (*Hand.* Kamer 2020-21, 19 maart 2021, CRIV55COM418, 1, Vr. nr. 15257C, 110I, 111I, 15426C, 15448C, 15490C, 15507C, 15511C, 15519C en 15520C)

Opvolging van de aanbevelingen van de parlementaire onderzoekscommissie "Terroristische aanslagen", gedachtewisseling en toegevoegde vragen van S. Rohonyi aan de minister van Justitie over 'een fonds voor de vergoeding van de slachtoffers van terreuraanslagen' (*Hand.* Kamer 2020-21, 23 maart 2021, CRIV55COM422, 1, Vr. nrs. 15751C, 15752C, 15754C, 15755C en 15760C)

Vraag van Th. Francken aan de Staatssecretaris voor Asiel en Migratie over 'de repatriëring van moslimextremisten en Syriestrijders naar hun thuisland' (*Hand.* Kamer 2020-21, 26 maart 2021, CRIV55COM425, 10, Vr. nr. 15509C)

Samengevoegde vragen van Y. Van Camp, F. Demon, E. Platteau en H. Rigot aan de Staatssecretaris voor Asiel en Migratie over 'outreachteams bij transmigranten' (*Hand.* Kamer 2020-21, 26 maart 2021, CRIV55COM425, 12, Vr. nrs. 15575C, 15585C, 15851C en 15857C)

Vraag van B. Segers aan de Staatssecretaris voor Asiel en Migratie over 'het elektronische platform voor gecombineerde verblijfsaanvraagprocedures' (*Hand.* Kamer 2020-21, 26 maart 2021, CRIV55COM425, 43, Vr. nr. 15814C)

Vraag van V. Scourneau aan de minister van Buitenlandse Zaken over de 'veiligheid van onze diplomaten in de Democratische Republiek Congo' (*Vr. en Ant*. Kamer 2020-21, 31 maart 2021, QRVA45, 99, Vr. nr. 218)

Vraag van A. Ponthier aan de minister van Buitenlandse Zaken over 'Oost-Congo - moord op Italiaans ambassadeur' (*Vr. en Ant*. Kamer 2020-21, 31 maart 2021, QRVA45, 113, Vr. nr. 242)

Vraag van K. Metsu aan de minister van Justitie over 'de terugkomst van Syriëstrijders en de OCAD analyse betreffende IS-vrouwen en -kinderen' (*Hand.* Kamer 2020-21, 31 maart 2021, CRIV55COM436, 35, Vr. nr. 15824C)

Vraag van K. Jadin aan de minister van Buitenlandse Zaken over 'IS-terreur in het gevangenenkamp Al-Hol' (*Vr. en Ant*. Kamer 2020-21, 7 april 2021, QRVA46, 124, Vr. nr. 228)

Vraag van E. Burton aan de minister van Buitenlandse Zaken over de 'risico's voor Belgische diplomaten in de DRC' (*Vr. en Ant*. Kamer 2020-21, 7 april 2021, QRVA46, 130, Vr. nr. 248)

Vraag van M. Freilich aan de minister van Justitie over 'Circles' (*Vr. en Ant*. Kamer 2020-21, 7 april 2021, QRVA46, 221, Vr. nr. 378)

Vraag van M. Vindevoghel aan de minister van Mobiliteit over de 'terreurdreiging voor het spoor' (*Vr. en Ant*. Kamer 2020-21, 15 april 2021, QRVA47, 122, Vr. nr. 112)

Vraag van K. Metsu aan de minister van Binnenlandse Zaken over 'het Brusselse kanaalplan en LIVC's' (*Vr. en Ant*. Kamer 2020-21, 15 april 2021, QRVA47, 294, Vr. nr. 400)

Vraag van B. Segers aan de Staatssecretaris voor Asiel en Migratie over 'de humanitaire visa via tussenpersonen' (*Vr. en Ant*. Kamer 2020-21, 15 april 2021, QRVA47, 352, Vr. nr. 155)

Vraag van P. Buysrogge aan de minister van Defensie over 'de nieuwe mini-drones' (*Hand.* Kamer 2020-21, 20 april 2021, CRIV55COM438, 10, Vr. nr. 14240C)

Vraag van A. Ponthier aan de minister van Defensie over 'de stopzetting van het contract voor het Open Source Intelligence System' (*Hand.* Kamer 2020-21, 20 april 2021, CRIV55COM438, 16, Vr. nr. 14534C)

Samengevoegde vragen van G. Defossé en P. Buysrogge aan de minister van Defensie over 'de offensieve cyberoperaties' (*Hand.* Kamer 2020-21, 20 april 2021, CRIV55COM438, 19, Vr. nrs. 14627C en 16305C)

Samengevoegde vragen van G. Defossé, Ch. Lacroix en K. Verduyckt aan de minister van Defensie over de 'militairen die banden hebben met extreemrechts' (*Hand.* Kamer 2020-21, 20 april 2021, CRIV55COM438, 45, Vr. nrs. 15600C, 5621C en 16526C)

Vraag van K. Metsu aan de minister van Justitie over 'het OCAD' (*Hand.* Kamer 2020-21, 21 april 2021, CRIV55COM442, 32, Vr. nr. 16385C)

Vraag van M. Freilich aan de minister van Justitie over 'de Chinese cyberspionage' (*Hand.* Kamer 2020-21, 21 april 2021, CRIV55COM445, 33, Vr. nr. 16518C)

Vraag van K. Metsu aan de minister van Justitie over 'de medeoprichter van het CCIB als lid van de raad van bestuur van Myria en Unia' (*Hand.* Kamer 2020-21, 21 april 2021, CRIV55COM445, 42, Vr. nr. 16626C)

Samengevoegde vragen van E. Samyn, K. Aouasti, K. Metsu en Th. Francken aan de minister van Buitenlandse Zaken over 'de Belgische IS-vrouwen in Syrië' (*Hand.* Kamer 2020-21, 27 april 2021, CRIV55COM449, 33, Vr. nrs. 14807C, 15558C, 15825C en 16400C)

Samengevoegde vragen van S. Cogolati, E. Samyn en Ch. Lacroix aan de minister van Buitenlandse Zaken over 'de bedreiging en intimidatie van opposanten in België door de Turkse regering' (*Hand.* Kamer 2020-21, 27 april 2021, CRIV55COM449, 82, Vr. nrs. 15441C, 113I en 16346C)

Actualiteitsdebat en toegevoegde vragen van G. Defossé, J. Pillen, Th. Francken, K. Jadin, Ch. Lacroix en A. Ponthier aan de minister van Defensie over 'het einde van Resolute Support Afghanistan' (*Hand.* Kamer 2020-21, 28 april 2021, CRIV55COM452, 1, Vr. nrs. 16438C, 16504C, 16580C, 16622C, 16820C en 16842C)

Vraag van C. Thibaut aan de minister van Binnenlandse Zaken over 'het toezicht op de gegevens in de ANG' (*Hand.* Kamer 2020-21, 28 april 2021, CRIV55COM453, 16, Vr. nr. 16719C)

Vraag van E. Platteau aan de minister van Ambtenarenzaken over 'het arrest van het Grondwettelijk Hof over de opslag van telecomdata' (*Hand.* Kamer 2020-21, 28 april 2021, CRIV55COM456, 13, Vr. nr. 16918C)

Vraag van S. Thémont aan de minister van Binnenlandse Zaken over de 'software om terreurdreigingen of radicalisering op te sporen' (*Vr. en Ant*. Kamer 2020-21, 3 mei 2021, QRVA50, 306, Vr. nr. 456)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over de 'risico van aanslagen op de vaccinatiecentra' (*Vr. en Ant*. Kamer 2020-21, 3 mei 2021, QRVA50, 313, Vr. nr. 461)

Interpellatie van E. Gilissen aan de minister van Ambtenarenzaken over 'de vernietiging van de dataretentiewet door het Grondwettelijk Hof' (*Hand.* Kamer 2020-21, 3 mei 2021, CRIV55COM457, 1, Vr. nr. 122I)

Samengevoegde interpellatie en vragen van K. Bury, S. De Wit, K. Geens en N. Boukili aan de minister van Justitie over 'de dataretentiewetgeving' (*Hand.* Kamer 2020-21, 5 mei 2021, CRIV55COM463, 1, Vr. nrs. 120I, 16763C, 16799C en 17247C)

Samengevoegde vragen van K. Jadin en S. Van Hecke aan de minister van Justitie over 'de strijd tegen schadelijke sekten' (*Hand.* Kamer 2020-21, 5 mei 2021, CRIV55COM463, 19, Vr. nrs. 17266C en 17275C)

Vraag van E. Platteau aan de minister van Binnenlandse Zaken over 'de omvang van de dreiging die uitgaat van extreemrechts' (*Hand.* Kamer 2020-21, 5 mei 2021, CRIV-55COM464, 53, Vr. nr. 17111C)

Vraag van O. Depoortere aan de minister van Binnenlandse Zaken over 'de dreiging van extreemlinks' (*Hand.* Kamer 2020-21, 5 mei 2021, CRIV55COM464, 56, Vr. nr. 17199C)

Vraag van K. Metsu aan de minister van Buitenlandse Zaken over de 'toenemende kracht van de zelfverklaarde Islamitische Staat in het Midden-Oosten' (*Vr. en Ant*. Kamer 2020-21, 10 mei 2021, QRVA51, 140, Vr. nr. 68)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over de 'bestrijding van radicalisme tijdens de coronacrisis' (*Vr. en Ant*. Kamer 2020-21, 10 mei 2021, QRVA51, 323, Vr. nr. 470)

Vraag van V. Scourneau aan de minister van Buitenlandse Zaken over de 'cyberveiligheid' (*Vr. en Ant*. Kamer 2020-21, 18 mei 2021, QRVA52, 117, Vr. nr. 281)

Vraag van M. Freilich aan de minister van Justitie over de 'smartphones - Xiaomi, Oppo en OnePlus' (*Vr. en Ant*. Kamer 2020-21, 27 mei 2021, QRVA53, 317, Vr. nr. 466)

Vraag van V. Scourneau aan de minister van Defensie over de 'aankoop van miniatuurdrones door Defensie' (*Vr. en Ant*. Kamer 2020-21, 27 mei 2021, QRVA53, 331, Vr. nr. 230)

Vraag van Ch. Lacroix aan de minister van Defensie over de 'intrekking van de veiligheidsmachtiging van onze defensieattaché in Parijs' (*Vr. en Ant*. Kamer 2020-21, 27 mei 2021, QRVA53, 343, Vr. nr. 258)

Vraag van K. Jadin aan de minister van Defensie over de 'archieven van Defensie' (*Vr. en Ant*. Kamer 2020-21, 27 mei 2021, QRVA53, 344, Vr. nr. 259)

Samengevoegde vragen van E. Gilissen, Y. Ingels, Ph. Pivin, K. Verhelst, F. Demon en M. Freilich aan de minister van Binnenlandse Zaken over 'de hacking van de FOD Binnenlandse Zaken' (*Hand.* Kamer 2020-21, 27 mei 2021, CRIV55PLEN106, 13, Vr. nrs. 1679P, 1684P, 1685P, 1686P, 1689P en 1695P)

Samengevoegde vragen van A. Ponthier, S. De Vuyst en P. Buysrogge aan de minister van Defensie over 'de zaak-Jürgen Conings en de verantwoordelijkheid van de minister en van Defensie' (*Hand.* Kamer 2020-21, 27 mei 2021, CRIV55PLEN106, 101, Vr. nrs. 131I tot 133I)

Vraag van C. Taquin aan de minister van Binnenlandse Zaken over de 'evaluatie van de LIVC-R's' (*Vr. en Ant*. Kamer 2020-21, 2 juni 2021, QRVA54, 229, Vr. nr. 555)

Actualiteitsdebat en samengevoegde vragen van G. Defossé, P. Buysrogge, Th. Francken, S. De Vuyst, N. Boukili, D. Ducarme, K. Verduyckt, Ch. Lacroix, W. De Vriendt en A. Ponthier aan de minister van Defensie over 'de opvolging van de zaak van de voortvluchtige militair' (*Hand.* Kamer 2020-21, 2 juin 2021, CRIV55COM495, 14, Vr. nrs. 18241C, 18242C, 18309C, 18311C, 18318C, 18320C, 18321C, 18328C, 18388C, 18429C, 18466C en 18482C)

Samengevoegde vragen van J. Chanson, E. Platteau, K. Jadin, Ph. Pivin, D. Ducarme en K. Aouasti aan de minister van Binnenlandse Zaken over de 'politieagenten die op de radar staan van de inlichtingendiensten' (*Hand.* Kamer 2020-21, 2 juin 2021, CRIV55COM500, 7, Vr. nrs. 17992C, 18183C, 18401C, 18420C, 18421C, 18459C en 18460C)

Samengevoegde vragen van S. De Vuyst en N. Boukili aan de eerste minister over 'de zoektocht naar de zwaarbewapende militair' (*Hand.* Kamer 2020-21, 2 juin 2021, CRIV55COM501, 14, Vr. nrs. 18075C en 18161C)

Vraag van N. Boukili aan de minister van Justitie over 'het bespioneren van een aantal Europese landen door de Verenigde Staten' (*Hand.* Kamer 2020-21, 2 juin 2021, CRIV55COM501, 55, Vr. nr. 18457C)

Vraag van P. De Roover aan de eerste minister over 'de perslekken over geheime rapporten van de Staatsveiligheid' (*Hand.* Kamer 2020-21, 9 juin 2021, CRIV55COM511, 12, Vr. nr. 15727C)

Vraag van W. Vermeersch aan de minister van Justitie over de 'erkenning moskeeën' (*Vr. en Ant*. Kamer 2020-21, 12 juni 2021, QRVA55, 247, Vr. nr. 510)

Vraag van C. Thibaut aan de minister van Justitie over de 'verplichte kennisgeving met betrekking tot elke in de GGB Terrorist Fighters opgenomen medewerker' (*Vr. en Ant*. Kamer 2020-21, 12 juni 2021, QRVA55, 274, Vr. nr. 576)

Vraag van W. Vermeersch aan de minister van Binnenlandse Zaken over de 'erkenning moskeeën' (*Vr. en Ant*. Kamer 2020-21, 12 juni 2021, QRVA55, 334, Vr. nr. 561)

Vraag van C. Thibaut aan de minister van Binnenlandse Zaken over de 'meedelen van informatie door de inlichtingendiensten aan instanties of privaatrechtelijke of publiekrechtelijke personen' (*Vr. en Ant*. Kamer 2020-21, 12 juni 2021, QRVA55, 351, Vr. nr. 570)

Samengevoegde vragen van N. Boukili, R. Hedebouw en D. Ducarme aan de minister van Binnenlandse Zaken over 'de zaak-Conings' (*Hand.* Kamer 2020-21, 16 juin 2021, CRIV55COM518, 21, Vr. nrs. 18652C, 18653C en 18943C)

Gedachtewisseling en toegevoegde vragen van P. Buysrogge, Th. Francken, S. De Vuyst, K. Verduyckt, G. Defossé, M. De Maegd, A. Ponthier, D. Ducarme, Ch. Lacroix en H. Bogaert aan de minister van Defensie over 'het intern verslag van de algemene inspectie van Landsverdediging over de zaak Jürgen Conings' (*Hand.* Kamer 2020-21, 16 juin 2021, CRIV55COM519, 1, Vr. nrs. 18607C, 18605C, 18618C, 18656C, 18745C, 18808C, 18835C, 18907C, 18914C, 19011C en 19020C)

Vraag van Th. Francken aan Staatssecretaris voor Asiel en Migratie over 'de interne inspectie Fedasil van overlastgevende asielzoekers in de asielcentra' (*Hand.* Kamer 2020-21, 18 juin 2021, CRIV55COM520, 47, Vr. nr. 19059C)

Vraag van T. Van Grieken aan de minister van Justitie over 'de erkenning van moskeeën' (*Vr. en Ant*. Kamer 2020-21, 22 juni 2021, QRVA56, 177, Vr. nr. 507)

Vraag van T. Van Grieken aan de minister van Justitie over 'de screening van kandidaat-asielzoekers op linken met terroristische groeperingen of met radicale potentieel gewelddadige groeperingen' (*Vr. en Ant*. Kamer 2020-21, 22 juni 2021, QRVA56, 190, Vr. nr. 530)

Vraag van C. Thibaut aan de minister van Defensie over de 'meedelen van informatie door de ADIV aan instanties of privaatrechtelijke of publiekerechtelijke personen' (*Vr. en Ant*. Kamer 2020-21, 22 juni 2021, QRVA56, 233, Vr. nr. 560)

Vraag van C. Thibaut aan de minister van Binnenlandse Zaken over de 'ontruiming van de ZAD in Aarlen' (*Vr. en Ant*. Kamer 2020-21, 22 juni 2021, QRVA56, 252, Vr. nr. 578)

Samengevoegde vragen van M. De Maegd, M. Ben Achour en P. De Roover aan de minister van Buitenlandse Zaken over 'de Belgische missie in het kamp Al-Roj' (*Hand.* Kamer 2020-21, 29 juni 2021, CRIV55COM530, 89, Vr. nrs. 18768C, 18798C en 18884C)

Samengevoegde vragen van O. Depoortere, Y. Ingels en T. Vandenput aan de minister van Binnenlandse Zaken over 'het personeelstekort bij de politie' (*Hand.* Kamer 2020-21, 30 juni 2021, CRIV55COM531, 20, Vr. nrs. 19355C, 19400C en 19429C)

Vraag van E. Burton aan de minister van Buitenlandse Zaken over de 'aanwezigheid van Chinese inlichtingendiensten in Luik' (*Vr. en Ant*. Kamer 2020-21, 30 juni 2021, QRVA57, 118, Vr. nr. 327)

Vraag van C. Thibaut aan de minister van Justitie over de 'beoordeling van de dreiging die uitgaat van de anti-5g-activisten' (*Vr. en Ant*. Kamer 2020-21, 30 juni 2021, QRVA57, 192, Vr. nr. 587)

Vraag van Ph. Pivin aan de minister van Justitie over de 'Cel Radicalisme bij de Dienst Vreemdelingenzakenscreening van buitenlandse investeringen – interdepartementale screeningcommissie' (*Vr. en Ant*. Kamer 2020-21, 30 juni 2021, QRVA57, 196, Vr. nr. 597)

Vraag van D. Safai aan Staatssecretaris voor Asiel en Migratie over 'de humanitaire visa voor IS-vrouwen en -kinderen' (*Hand.* Kamer 2020-21, 2 juli 2021, CRIV55COM535, 21, Vr. nr. 19570C)

Gedachtewisseling, toegevoegde interpellatie en vragen van K. Jadin, A. Ponthier, Th. Francken en G. Defossé aan de minister van Defensie over 'het rapport van Comité I en de psychosociale zorg in het leger' (*Hand.* Kamer 2020-21, 5 juli 2021, CRIV55COM537, 1, Vr. nrs. 18547C, 19099C, 19136C, 00149I, 19252C, 19257C en 19595C)

Vraag van S. Loones aan de minister van Begroting over 'het budget van Defensie' (*Hand.* Kamer 2020-21, 6 juli 2021, CRIV55COM539, 20, Vr. nr. 18077C)

Vraag van A. Ponthier aan de minister van Justitie over de 'invloed Soros' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 250, Vr. nr. 595)

Vraag van Y. Van Camp aan de minister van Justitie over de 'screening haatimam' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 261, Vr. nr. 553)

Vraag van K. Verduyckt aan de minister van Justitie over 'extreemrechts bij penitentiaire bewaking' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 268, Vr. nr. 583)

Vraag van A. Van Bossuyt aan de minister van Justitie over de 'Chine spionage via Thousand Talents programma' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 279, Vr. nr. 612)

Vraag van K. Jadin aan de minister van Defensie over de 'opvolging van het personeel van Defensie' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 291, Vr. nr. 274)

Vraag van Ph. Pivin aan de minister van Binnenlandse Zaken over de 'Cel Radicalisme bij de Dienst Vreemdelingenzaken' (*Vr. en Ant*. Kamer 2020-21, 8 juli 2021, QRVA58, 345, Vr. nr. 148)

Vraag van G. Dallemagne aan de minister van Justitie over 'het OCAD-rapport over het wahabisme, het jihadisme en het terrorisme' (*Hand.* Kamer 2020-21, 14 juli 2021, CRIV55COM556, 7, Vr. nr. 19771C)

Samengevoegde vragen van J. Pillen, S. Creyelman en K. Jadin aan de minister van Defensie over 'de cybercomponent' (*Hand.* Kamer 2020-21, 14 juli 2021, CRIV55COM557, 23, Vr. nrs. 17854C, 18003C en 19321C)

Samengevoegde vragen van G. Defossé, V. Reynaert en Ch. Lacroix aan de minister van Defensie over 'de onthulling van geheime informatie over de in Europa opgeslagen kernwapens' (*Hand.* Kamer 2020-21, 14 juli 2021, CRIV55COM557, 27, Vr. nrs. 18336C, 18384C en 18433C)

Vraag van Th. Francken aan de minister van Defensie over 'Psyops' (*Hand.* Kamer 2020-21, 14 juli 2021, CRIV55COM557, 34, Vr. nr.18783C)

Samengevoegde interpellaties van P. De Roover en B. Pas aan de eerste minister over 'het ontslag van regeringscommissaris Haouach' (*Hand.* Kamer 2020-21, 15 juillet 2021, CRIV55PLEN122, 26, Vr. nrs. 162I en 163I)

Vraag van S. Van Hecke aan de minister van Buitenlandse Zaken over het 'nationaal veiligheidsoverleg – moeizame communicatie' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 105, Vr. nr. 341)

Vraag van C. Thibaut aan de minister van Buitenlandse Zaken over het 'uitblijven van antwoorden van de NVO aan het Comité I inzake veiligheidsmachtigingen' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 108, Vr. nr. 342)

Vraag van Y. Ingels aan de minister van Mobiliteit over de 'toekenning van toegangsbadges voor airside' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 185, Vr. nr. 601)

Vraag van K. Metsu aan de minister van Justitie over de 'erkenning Brusselse geloofsgemeenschappen' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 261, Vr. nr. 617)

Vraag van K. Verduyckt aan de minister van Binnenlandse Zaken over 'extreemrechts bij politie' (*Vr. en Ant.* Kamer 2020-21, 15 juli 2021, QRVA59, 347, Vr. nr. 665)

Gedachtewisseling en toegevoegde vragen van B. Pas, E. Samyn, D. Van Langenhove en K. Metsu aan de eerste minister en de minister van Buitenlandse Zaken over 'het terughalen van IS-terroristen naar België' (*Hand.* Kamer 2020-21, 22 juli 2021, CRIV55COM560, 1, Vr. nrs. 19979C, 19977C, 19981C en 19995C)

Gedachtewisseling en toegevoegde vragen van Th. Francken, A. Ponthier, W. De Vriendt, G. Dallemagne, K. Verduyckt, S. De Vuyst, G. Defossé en Ch. Lacroix aan de minister van Defensie over 'de vervanging van generaal-majoor Boucké aan het hoofd van ADIV' (*Hand.* Kamer 2020-21, 22 juli 2021, CRIV55COM561, 1, Vr. nrs. 19973C, 19974C, 19975C, 19976C, 19983C, 19990C, 19993C en 19994C)

Vraag van Y. Ingels aan de minister van Buitenlandse Zaken over de 'nationale veiligheidsoverheid – rol en opdrachten' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 92, Vr. nr. 347)

Vraag van S. Cogolati aan de minister van Buitenlandse Zaken over 'spionage door NSA met de hulp van Denemarken' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 105, Vr. nr. 363)

Vraag van K. Jadin aan de minister van Buitenlandse Zaken over 'spionage door NSA met de hulp van Denemarken' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 109, Vr. nr. 365)

Vraag van B. Moyaers aan de minister van Buitenlandse Zaken over de 'politieke zoektocht naar hackers' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 120, Vr. nr. 376)

Vraag van S. De Vuyst aan de minister van Buitenlandse Zaken over 'Amerikaanse spionage' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 123, Vr. nr. 380)

Vraag van C. Taquin aan de minister van Justitie over de 'strijd tegen sektarische excessen tijdens de pandemie' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 184, Vr. nr. 567)

Vraag van E. Burton aan de minister van Justitie over de 'Veiligheid van de Staat en spionnage' (*Vr. en Ant.* Kamer 2020-21, 24 juli 2021, QRVA60, 194, Vr. nr. 592)

Vraag van J. Pillen aan de minister van Defensie over het 'personeel van de ADIV' (*Vr. en Ant*. Kamer 2020-21, 24 juli 2021, QRVA60, 303, Vr. nr. 286)

Vraag van Y. Ingels aan de eerste minister over 'het veilig kunnen uitwisselen van gevoelige informatie' (*Vr. en Ant*. Kamer 2020-21, 11 augustus 2021, QRVA61, 135, Vr. nr. 111)

Vraag van D. Safai aan de minister van Binnenlandse Zaken over de 'cursussen radicalisme en meldpunt radicalisering' (*Vr. en Ant*. Kamer 2020-21, 11 augustus 2021, QRVA61, 337, Vr. nr. 227)

Gedachtewisseling en toegevoegde vragen van Th. Francken, A. Flahaut, G. Liekens, S. de Laveleye, G. Defossé, Ch. Lacroix, V. Reynaert, D. Van Langenhove, W. De Vriendt, Fr. De Smet, H. Rigot, K. Jadin, J. Chanson, T. Vandenput, S. Moutquin, E. Platteau, N. Boukili en B. Segers aan de eerste minister over 'de situatie in Afghanistan' (*Hand.* Kamer 2020-21, 26 augustus 2021, CRIV55COM563, 1, Vr. nrs. 20147C, 20148C, 20156C, 20147C, 20118C, 20094C, 20103C, 20104C, 20140C, 20162C, 20122C, 20154C, 20155C, 20083C, 20093C, 20115C, 20158C, 20137C, 20146C, 20157C, 20057C, 20067C, 20095C, 20110C, 20119C, 20120C, 20127C, 20145C, 20130C, 20132C, 20133C, 20134C, 20135C, 20136C, 20138C, 20139C, 20141C, 20142C, 20161C, 20163C, 20164C en 20165C)

Vraag van J. Donné aan de minister van Financiën over de 'raadplegingen CAP2' (*Vr. en Ant*. Kamer 2020-21, 6 september 2021, QRVA62, 216, Vr. nr. 146)

Vraag van W. Vermeersch aan de minister van Financiën over de 'erkenning van moskeeën' (*Vr. en Ant*. Kamer 2020-21, 6 september 2021, QRVA62, 228, Vr. nr. 398)

Vraag van B. Segers aan de minister van Justitie over de 'screening van humanitaire visa' (*Vr. en Ant*. Kamer 2020-21, 6 september 2021, QRVA62, 319, Vr. nr. 606)

Vraag van M. Freilich aan de minister van Justitie over de 'NSO group software' (*Vr. en Ant*. Kamer 2020-21, 6 september 2021, QRVA62, 337, Vr. nr. 658)

Vraag van Y. Ingels aan de eerste minister over de 'projecten van veiligheidsdepartementen bij de Regie der Gebouwen' (*Vr. en Ant*. Kamer 2020-21, 20 september 2021, QRVA 63, 338, Vr. nr. 150)

Samengevoegde vragen van Th. Francken, S. Moutquin en D. Van Langenhove aan de Staatssecretaris voor Asiel en Migratie over 'het humanitaire visaprogramma voor Afghanen' (*Hand.* Kamer 2020-21, 22 september 2021, CRIV55COM575, 31, Vr. nrs. 20703C, 20883C, 20886C, 20888C, 20916C en 20931C)

Samengevoegde vragen van M. Freilich, S. Van Hecke, N. Boukili en E. Van Hoof aan de minister van Justitie over 'de afluistersoftware' (*Hand.* Kamer 2020-21, 22 september 2021, CRIV55COM577, 1, Vr. nrs. 19985C, 20000C, 20448C en 20845C)

Samengevoegde vragen van M. Freilich, E. Gilissen en K. Gabriëls aan de minister van Justitie over 'de seponering in het kader van het onderzoek naar de Chinese spionnen' (*Hand.* Kamer 2020-21, 22 september 2021, CRIV55COM577, 41, Vr. nrs. 20313C, 20325C en 20903C)

Vraag van K. Jiroflée aan de minister van Justitie over 'de niet-naleving van tijdelijke huisverboden' (*Hand.* Kamer 2020-21, 22 september 2021, CRIV55COM577, 45, Vr. nr. 20335C)

Actualiteitsdebat en toegevoegde vragen van P. De Roover, K. Jadin, V. Reynaert, H. Rigot en S. Cogolati aan de minister van Buitenlandse zaken over 'Afghanistan' (*Hand.* Kamer 2020-21, 28 september 2021, CRIV55COM579, 7, Vr. nrs. 20256C, 20270C, 20271C, 20408C, 21142C, 21173C en 21221C)

Samengevoegde vragen van S. Van Hecke en E. Van Hoof aan de minister van Buitenlandse zaken over 'de impact van Pegasus op diplomatieke relaties en de te nemen maatregelen in het kader daarvan' (*Hand.* Kamer 2020-21, 28 september 2021, CRIV55COM579, 19, Vr. nrs. 20007C en 21061C)

Vraag van M. Dillen aan de minister van Justitie over 'Oussama Atar en de aanslagen in Parijs en Brussel' (*Hand.* Kamer 2020-21, 29 september 2021, CRIV55COM586, 15, Vr. nr. 20496C)

Vraag van Ph. Pivin aan de minister van Economie over de 'screening van buitenlandse investeringen – interdepartementale screeningscommissie' (*Vr. en Ant*. Kamer 2020-21, 2 oktober 2021, QRVA 64, 29, Vr. nr. 566)

Vraag van S. Creyelman aan de minister van Defensie over het 'spionagemateriaal in de Belgische ambassade in Ankara' (*Vr. en Ant*. Kamer 2020-21, 2 oktober 2021, QRVA 64, 175, Vr. nr. 315)

Vraag van S. Verherstraeten aan de minister van Defensie over de 'militairen – rechts-extremistische sympathieën' (*Vr. en Ant*. Kamer 2020-21, 2 oktober 2021, QRVA 64, 178, Vr. nr. 320)

Vraag van D. Safai aan Staatssecretaris voor Asiel en Migratie over 'de repatriëring van IS-terroristen en hun kinderen' (*Hand.* Kamer 2020-21, 5 oktober 2021, CRIV55COM588, 31, Vr. nr. 20943C)

Vraag van D. Van Langenhove aan Staatssecretaris voor Asiel en Migratie over 'de resultaten van de veiligheidsscreening' (*Hand.* Kamer 2020-21, 5 oktober 2021, CRIV55COM588, 31, Vr. nr. 20993C)

Vraag van G. Dallemagne aan de minister van Justitie over de 'salafistische kern te Molenbeek' (*Vr. en Ant*. Kamer 2020-21, 6 oktober 2021, QRVA 65, 422, Vr. nr. 724)

Vraag van E. Van Hoof aan de minister van Defensie over de 'spionagesoftware Pegasus' (*Vr. en Ant*. Kamer 2020-21, 6 oktober 2021, QRVA 65, 439, Vr. nr. 326)

Vraag van S. Cogolati aan de minister van Justitie over 'het onderzoek naar de daders van de cyberaanval tegen Belnet op 4 mei 2021' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV55COM596, 4, Vr. nr. 21135C)

Vraag van K. Metsu aan de minister van Justitie over de 'vastgestelde malversaties bij vzw Moslimexecutieve' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV55COM596, 26, Vr. nr. 21579C)

Vraag van S. Verherstraeten aan de minister van Binnenlandse Zaken over 'de toename van de rechts-extremistische dreiging' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV55COM597, 35, Vr. nr. 20009C)

Samengevoegde vragen van M. Freilich en J. Chanson aan de minister van Binnenlandse Zaken over 'het beëindigen van OVG' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV55COM597, 55, Vr. nrs. 20331C en 20404C)

Samengevoegde vragen van M. Freilich en K. Metsu aan de minister van Binnenlandse Zaken over 'de aanhouding van enkele geradicaliseerde mannen' (*Hand.* Kamer 2020-21, 6 oktober 2021, CRIV55COM597, 76, Vr. nrs. 20744C, 21288C en 21384C)

Samengevoegde vragen van A. Ponthier, K. Metsu en P. Dewael aan de eerste minister over 'de aanhoudende problemen met islamfundamentalisme bij de Moslimexecutieve' (*Hand.* Kamer 2020-21, 7 oktober 2021, CRIV55PLEN127, 5, Vr. nrs. 1932P, 1945P en 1948P)

Vraag van M. Freilich aan de eerste minister over de 'NSO group software' (*Vr. en Ant*. Kamer 2020-21, 10 oktober 2021, QRVA 66, 39, Vr. nr. 129)

Actualiteitsdebat en samengevoegde vragen van K. Jadin, A. Ponthier, G. Defossé, Th. Francken en A. FLahaut aan de minister van Defensie over 'het onderzoek naar extremisme' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM606, 1, Vr. nrs. 20281C, 20292C, 20864C, 20942C,21565C, 22019C en 21674C)

Samengevoegde vragen van A. Ponthier en G. Dallemagne aan de minister van Defensie over 'de hervormingen binnen de ADIV na aanstelling van vice-admiraal W. Robberechts als diensthoofd' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM606, 10, Vr. nrs. 20306C en 20923C)

Samengevoegde vragen van T. Vandenput en J. Chanson aan de minister van Binnenlandse Zaken over 'de problemen met het ASTRID-netwerk' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM611, 40, Vr. nrs. 21129C en 21212C)

Vraag van S. Loones aan de minister van Binnenlandse Zaken over 'seining van de heer Puigdemont in het Schengen Information System (SIS)' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM611, 53, Vr. nr. 21308C)

Samengevoegde vragen van S. Goethals en O. Depoortere aan de minister van Binnenlandse Zaken over 'de burgerlijke partijstelling van de minister' (*Hand.* Kamer 2021-22, 20 oktober 2021, CRIV55COM611, 66, Vr. nrs. 21542C en 21575C)

Vraag van E. Van Hoof aan de minister van Justitie over de 'spionagesoftware Pegasus' (*Vr. en Ant*. Kamer 2021-22, 26 oktober 2021, QRVA 67, 247, Vr. nr. 689)

Vraag van A. Ponthier aan de minister van Justitie over de 'kostprijs operatie Jürgen Conings' (*Vr. en Ant*. Kamer 2021-22, 26 oktober 2021, QRVA 67, 252, Vr. nr. 699)

Vraag van S. Creyelman aan de minister van Defensie over 'de mogelijke verspreiding van complottheorieën door Rusland' (*Hand.* Kamer 2021-22, 27 oktober 2021, CRIV55COM618, 13, Vr. nr. 22136C)

Samengevoegde vragen van G. Defossé en P. Buysrogge aan de minister van Defensie over 'de uitspraken van de heer Lipszyc in een interview' (*Hand.* Kamer 2021-22, 27 oktober 2021, CRIV55COM618, 21, Vr. nrs. 22258C en 22364C)

Vraag van M. Freilich aan de eerste minister over 'het ondermijnen van encryptie' (*Hand.* Kamer 2021-22, 27 oktober 2021, CRIV55COM623, 20, Vr. nr. 22038C)

Vraag van K. Geens aan de minister van Binnenlandse Zaken over de 'Operatie Sky' (*Hand*. Kamer 2021-22, 28 oktober 2021, CRIV55PLEN136, 24, Vr. nr. 1990P)

Samengevoegde vragen van A. Ponthier en N. Boukili aan de minister van Justitie over 'de huiszoekingen bij militairen op grond van een vermoeden van aanzetten tot terreur' (*Hand.* Kamer 2021-22, 10 november 2021, CRIV55COM625, 15, Vr. nrs. 22510C en 22521C)

Vraag van M. Freilich aan de minister de Justitie over de 'afluistersoftware NSO' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 257, Vr. nr. 728)

Vraag van S. Creyelman aan de minister van Defensie over 'extremisme bij Defensie - opvolging' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 338, Vr. nr. 321)

Vraag van M. Freilich aan de eerste minister over de 'aanpak dark web' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 129, Vr. nr. 145)

Vraag van M. Freilich aan de eerste minister over de 'repressieve capaciteit inzake cybercriminaliteit' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 130, Vr. nr. 146)

Vraag van Th. Francken aan de minister van Justitie over 'de kolos van Molenbeek' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 260, Vr. nr. 747)

Vraag van S. Creyelman aan de minister van Defensie over de 'extremisme bij Defensie - opvolging' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 338, Vr. nr. 321)

Vraag van S. Van Hecke aan de minister van Defensie over het 'Pegasus-project – de acties van ADIV' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 349, Vr. nr. 355)

Vraag van S. Matheï aan de eerste minister over de 'evaluatie GDPR' (*Vr. en Ant*. Kamer 2021-22, 18 november 2021, QRVA 69, 402, Vr. nr. 221)

Vraag van K. Jadin aan de minister van Defensie over de 'veiligheid van apparaten van Chinese makelij' (*Vr. en Ant*. Kamer 2021-22, 25 november 2021, QRVA 70, 285, Vr. nr. 357)

Vraag van A. Vicaire aan de minister van Digitalisering over 'de zaak Pegasus en de bescherming van Belgische politici' (*Hand*. Kamer 2021-22, 30 november 2021, CRIV55COM630, 1, Vr. nr. 20099C)

Vraag van K. Metsu aan de minister van Justitie over 'de aanpak van geradicaliseerden in onze gevangenissen' (*Hand*. Kamer 2021-22, 2 december 2021, CRIV55PLEN144, 15, Vr. nr. 2090P)

Vraag van Y. Ingels aan de eerste minister over het 'Federaal beleid inzake drugs – georganiseerde misdaad' (*Vr. en Ant.* Kamer 2021-22, 6 december 2021, QRVA 71, 67, Vr. nr. 153)

Vraag van M. Dillen aan de minister van Justitie over de 'verslag Rekenhof DAV – transversale doelstellingen AV' (*Vr. en Ant.* Kamer 2021-22, 6 december 2021, QRVA 71, 225, Vr. nr. 796)

Vraag van E. Burton aan de minister van Justitie over 'deepfakes' (*Vr. en Ant.* Kamer 2021-22, 6 december 2021, QRVA 71, 248, Vr. nr. 823)

Vraag van S. Cogolati aan de minister van Justitie over het 'gevaar voor spionage in het China-Belgium Technology Center' (*Vr. en Ant.* Kamer 2021-22, 6 december 2021, QRVA 71, 250, Vr. nr. 824)

Samengevoegde vragen van B. Pas en K. Metsu aan de eerste minister over 'de manke opvolging van jihadisten in dit land' (*Hand.* Kamer 2021-22, 9 december 2021, CRIV55PLEN145, 23, Vr. nrs. 2099P en 2124P)

Samengevoegde vragen van K. Jadin en M. Vindevoghel aan de minister van Defensie over de 'rekrutering van Belgische militairen' (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM640, 3, Vr. nrs. 23244C en 23388C)

Vraag van G. Defossé aan de minister van Defensie over 'de doodsbedreiging van een minister door een militair' (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM640, 7, Vr. nr. 23346C)

Vraag van K. Jadin aan de minister van Binnenlandse Zaken over 'het extremisme in België' (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM642, 6, Vr. nr. 23074C)

Vraag van E. Platteau aan de minister van Binnenlandse Zaken over 'de bestrijding van extremisme door sociale re-integratie en 'disengagement'" (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM642, 13, Vr. nr. 23104C)

Samengevoegde vragen van E. Platteau, F. Demon, T. Vandenput en O. Depoortere aan de minister van Binnenlandse Zaken over 'het OCAD-rapport over de coronacrisis' (*Hand.* Kamer 2021-22, 15 december 2021, CRIV55COM642, 14, Vr. nrs. 23178C, 23229C, 23393C en 23415C)

Samengevoegde vragen van K. Metsu en Ph. Pivin aan de minister van Justitie over 'het Executief van de Moslims van België' (*Hand.* Kamer 2021-22, 16 december 2021, CRIV55PLEN148, 15, Vr. nrs. 2131P en 2143P)

Samengevoegde vragen van K. Metsu en B. Pas aan de minister van Justitie over 'het foutief informeren van het Parlement' (*Hand.* Kamer 2021-22, 16 december 2021, CRIV55PLEN148, 21, Vr. nrs. 206I en 214I)

Vraag van S. Cogolati aan de minister van Ambtenarenzaken over het 'gevaar voor censuur en cybersurveillance op smarphones van Huawei, Xiaomi en OnePlus' (*Vr. en Ant.* Kamer 2021-22, 16 december 2021, QRVA 72, 180, Vr. nr. 349)

Vraag van S. Creyelman aan de minister van Defensie over 'de uitbouw van de cybercomponent binnen Defensie' (*Vr. en Ant.* Kamer 2021-22, 16 december 2021, QRVA 72, 228, Vr. nr. 346)

Vraag van Th. Francken aan de minister van Binnenlandse Zaken over 'de screening bij de evacuatieoperatie' (*Vr. en Ant.* Kamer 2021-22, 16 december 2021, QRVA 72, 335, Vr. nr. 386)

Vraag van G. Dallemagne aan de minister van Binnenlandse Zaken over 'het jaarverslag van de Veiligheid van de Staat' (*Hand.* Kamer 2021-22, 20 december 2021, CRIV55COM645, 2, Vr. nr. 22634C)

Vraag van K. Bury aan de minister van Justitie over 'de aankoop van kantoorgebouwen in de Brusselse Noordwijk' (*Hand.* Kamer 2021-22, 20 december 2021, CRIV55COM645, 26, Vr. nr. 23267C)