30

DIFFUSION RESTREINTE JUSQU'À LA RÉUNION AVEC LA COMMISSION DE SUIVI

COMITE PERMANENT DE CONTROLE DES SERVICES DE RENSEIGNEMENT ET DE SECURITE

Numéro de notice 2020.281

Suivi de l'enquête de contrôle PRISM (2013)

Rapport final - 17 octobre 2022

TABLE DES MATIÈRES

I. INTRODUCTION

I.1. ENQUÊTE DE CONTRÔLE PRISM (2013)

En 2013, le Comité permanent R a mené une enquête de contrôle sur l'attention que les services de renseignement belges accordaient aux menaces éventuelles pour le potentiel économique et scientifique (PES) belge émanant de programmes de surveillance électronique de systèmes de communication et d'information déployés à grande échelle par les grandes puissances et/ou les services de renseignement étrangers.

Le Comité permanent R a décidé d'examiner de près certaines implémentations des recommandations tirées de l'enquête de 2013 et de vérifier la manière dont les recommandations sont suivies.

I.2. COMPÉTENCE DU COMITÉ PERMANENT R

L'article 33 de la loi du 18 juillet 1991 relative au contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace (Loi Contrôle) stipule que le Comité permanent R enquête sur les activités et les méthodes des services de renseignement.

II. SUIVI DES RECOMMANDATIONS DE L'ENQUÊTE DE CONTRÔLE PRISM (2013)

L'enquête de contrôle PRISM de 2013 a donné lieu à 11 recommandations. La présente enquête de suivi examine comment chacune de ces recommandations a été mise en œuvre.

II.1. PREMIÈRE RECOMMANDATION : INTÉRÊT POUR LA CAPTATION MASSIVE DE DONNÉES ET L'ESPIONNAGE POLITIQUE ET ECONOMIQUE

Recommandation - Enquête de contrôle PRISM (2013)

Le Comité permanent R estime que les deux services de renseignement doivent s'intéresser aux éventuels risques inhérents aux nouveaux moyens technologiques en matière de captation massive de données et d'espionnage économique et politique, même s'ils émanent de pays amis. À cet égard, des analyses de risques devraient être effectuées, en prenant également en considération la présence d'institutions internationales sur le territoire belge.

L'attention portée à ce phénomène est nécessaire, en ce qui concerne la VSSE et le SGRS, pour se forger une bonne position d'information afin de connaître les moyens et le *modus operandi* d'autres services. Cela permet non seulement d'en informer, le cas échéant, les autorités, ou de prendre des mesures de rétorsion, mais aussi d'évaluer leurs propres techniques de collecte.

En ce qui concerne la VSSE, il est évidemment nécessaire de s'intéresser à la captation massive de données parce que ce phénomène présente une réelle menace pour au moins deux intérêts qu'elle doit défendre en vertu de la loi, à savoir les libertés et droits fondamentaux et la souveraineté de l'État. On retrouve déjà, par exemple, un grand nombre d'informations dans des sources ouvertes. Des informations peuvent aussi être demandées au service de renseignement militaire. Sur la base de ces éléments, il est déjà possible de se faire une idée globale du phénomène et des risques. Cela pourrait se traduire par une analyse du phénomène[1] à envoyer à intervalles réguliers aux autorités concernées. Les citoyens et les entreprises devraient eux aussi être davantage encore sensibilisés à la problématique.

À l'estime du Comité permanent R, l'intérêt accordé par la VSSE et le SGRS à la captation massive de données et à l'espionnage économique est nécessaire. En effet, les deux services sont obligés d'établir une bonne position d'information pour connaître les capacités et les pratiques des autres services étrangers.

Cet intérêt est non seulement nécessaire pour, le cas échéant, informer les autorités belges ou prendre des mesures de rétorsion, mais aussi pour évaluer ses propres techniques de collecte.

---

[1] Le Comité permanent R a déjà attiré l'attention précédemment sur les atouts de ce que la VSSE appelle une « analyse du phénomène » : « *L'analyse du phénomène expose un thème actuel qui relève des sphères d'intérêt et des missions dévolues à un service de renseignement et qui représente un défi politique et social majeur, tant aujourd'hui que pour les années à venir. Elle s'attache à décrire ce problème tant au niveau de ses origines historiques, qu'au plan de l'idéologie, de l'organisation, de la structure et des activités y relatives. Elle contextualise les défis et les risques, établit une « évaluation du risque » à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique.* » (cf. la première analyse de phénomène de la VSSE). Aussi parce que de telles analyses sont destinées à une diffusion plus large, elles se prêtent bien à la problématique de la captation de données.

Quant à la VSSE

La VSSE considère qu'il est manifestement nécessaire de prêter attention à la captation massive de données car ce phénomène constitue une menace réelle pour au moins deux intérêts juridiquement protégeables, à savoir (1) les droits et libertés fondamentaux et (2) la souveraineté des États.

Selon la VSSE, l'image globale que l'on se fait de la captation massive de données pourrait se traduire par une analyse du phénomène[2] à envoyer à intervalles réguliers aux autorités concernées. Les citoyens et les entreprises devraient, eux aussi, être davantage sensibilisés à la problématique.

Quant au SGRS

Le SGRS reconnaît l'existence de la menace, mais ne voit pas immédiatement l'intérêt de préparer une analyse à ce sujet. Le SGRS est manifestement confronté à un manque de personnel pour assurer un suivi complet de la captation massive de données par les services étrangers dans toute la mesure du possible.

ÉVALUATION DU COMITÉ PERMANENT R

Le Comité permanent R constate qu'une telle analyse du phénomène - destinée à identifier la menace que représentent les systèmes d'interception étrangers pour le PES et les infrastructures critiques de la Belgique - n'a pas été réalisée à ce jour.

Le Comité permanent R constate que les deux services disent ne pas disposer des moyens de traiter correctement le phénomène de captation massive de données. Le Comité estime cependant que les services doivent continuer à investir dans la protection contre de telles pratiques massives d'écoute.

À compter du 19 octobre 2022, le *Cyber Command* de la Défense belge, en étroite collaboration avec le SGRS, sera officiellement opérationnel. Il sera chargé de la mise en œuvre de la stratégie de cybersécurité et de la fourniture des moyens appropriés pour atteindre les objectifs y énoncés.

---

[2] Le Comité permanent R avait déjà souligné les atouts de ce que la VSSE appelle une 'analyse du phénomène' : *'L'analyse du phénomène expose un thème actuel qui relève des sphères d'intérêt et des missions dévolues à un service de renseignement et qui représente un défi politique et social majeur, tant aujourd'hui que pour les années à venir. Elle s'attache à décrire ce problème tant au niveau de ses origines historiques, qu'au plan de l'idéologie, de l'organisation, de la structure et des activités y relatives. Elle contextualise les défis et les risques, établit une « évaluation du risque » à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique'* (cf. la première analyse du phénomène de la VSSE). Aussi parce que de telles analyses sont destinées à être diffusées plus largement, elles se prêtent bien à la problématique de la captation de données.

II.2. DEUXIÈME RECOMMANDATION : LA CONCEPTION DE LA NOTION DE « SERVICES AMIS »

Recommandation - Enquête de contrôle PRISM (2013)
Il apparaît que tant la VSSE que le SGRS se montrent « plus prudents » dans leurs contacts avec les services amis ou les services de pays amis. Bien que le Comité puisse se montrer compréhensif jusqu'à un certain point, il recommande aux services de renseignement belges de prendre *chaque* menace au sérieux, même si elle provient de services amis ou de services de pays amis. Le Comité permanent R rejoint la VSSE sur le fait qu'il est indiqué de parler de « partenaires stratégiques » au lieu de « services amis ».

Le 26 septembre 2016, le Conseil national de sécurité a édicté une directive en cette matière. Il s'agit de la *« Directive concernant les relations des services de renseignement belges avec les services de renseignement étrangers »*.[3] Cette directive définit le mécanisme que la VSSE et le SGRS doivent mettre en œuvre.

Le but est d'objectiver de manière structurée le choix de leurs partenaires internationaux en vue de déterminer la mesure et la nature de la collaboration avec ces partenaires et d'évaluer cette collaboration sur une base régulière. La directive fournit également des orientations concernant la fourniture de données à caractère personnel à des services étrangers.

Le mécanisme décrit dans la directive comprend une série de critères d'évaluation. Ces critères doivent être pris en compte et concernent, d'une part, d'éventuels obstacles à une collaboration avec un partenaire étranger et, d'autre part, les éventuelles occasions ou possibilités de collaboration avec ces partenaires. Sur la base de ces critères d'évaluation, la directive prévoit une évaluation biennale de la collaboration de chaque service étranger avec lequel une collaboration est menée. Une fiche de synthèse doit être établie concernant chaque service partenaire étranger. Ces services partenaires sont également regroupés en catégories, qui déterminent le mode de collaboration.

Dans le cadre de cette enquête, les deux services ont été interrogés pour définir dans quelle mesure cette directive était appliquée de manière systématique, et dans quelle mesure encore, lors de l'évaluation de la collaboration avec un service étranger, il était tenu compte d'une captation éventuelle de données par ce service.

Quant à la VSSE

La VSSE a déclaré s'efforcer d'intégrer toujours plus le mécanisme d'évaluation des services de renseignement étrangers dans le fonctionnement quotidien du service.

---

[3] Pour ce qui a trait à l'obtention d'une vue d'ensemble de l'historique de cette directive, et les recommandations formulées à cet égard par le Comité permanent R, voir COMITÉ PERMANENT R, « Enquête de contrôle concernant le Memorandum of Understanding (MoU) conclu en octobre par le SGRS et les services de renseignement rwandais », 30 juin 2020, p. 4-6.

Quant au SGRS

Le SGRS a simplement déclaré que, selon lui, la directive devrait être revue. Le SGRS n'a pas précisé dans quel sens cette révision devrait aller.[4]

ÉVALUATION DU COMITÉ PERMANENT R

Le Comité permanent R estime que la menace que représente l'utilisation de systèmes de captation massive par un partenaire stratégique doit être incluse dans l'évaluation que le service de renseignement fait de sa relation avec un service partenaire.

Le Comité permanent R estime que les services de renseignement doivent s'équiper de tous les moyens humains et techniques possibles pour déceler de telles menaces, éventuellement par l'entremise du *Cyber Command* de la Défense belge. Selon le Comité permanent R, les services de renseignement doivent accorder une attention constante à la possibilité d'une captation massive de données par des partenaires stratégiques ou des services « amis ».

[4] Note 21.50057672 du 23 mars 2021, SGRS, p.3.

II.3. TROISIÈME RECOMMANDATION : COLLABORATION PLUS ÉTROITE ENTRE LES DEUX SERVICES DE RENSEIGNEMENT

Recommandation - Enquête de contrôle PRISM (2013)

Le Comité a dû constater qu'avant les révélations d'E. Snowden, la VSSE et le SGRS ne se sont jamais échangés d'informations sur les menaces que représentent les captations massives de données et l'espionnage politique et économique. Par la suite, les services ont échangé des informations, mais ces échanges sont restés limités. Le Comité pose ce constat en premier lieu en regard de l'obligation légale qu'ont les services d'échanger des informations (art. 19 L.R&S). En outre, le Comité signale l'existence d'un accord de coopération mutuelle (Protocole d'accord du 12 novembre 2004), qui vise justement la transmission spontanée d'informations appartenant à la sphère de compétence de l'autre service. Au moins après les révélations, les mécanismes décrits dans ce Protocole d'accord auraient dû être utilisés pour consolider la position d'information des deux services. Le Comité attire particulièrement l'attention sur le fait que ce Protocole offre la possibilité de créer une « plateforme de collaboration *ad hoc* », au sein de laquelle des analyses conjointes peuvent être réalisées. Le contraste mis en lumière dans le présent dossier (à savoir que le SGRS possède des connaissances certaines, mais qu'avant les révélations, le service n'était pas compétent pour le suivi des captations massives de données, contrairement à la VSSE qui était certes compétente mais disposaient de peu d'informations spécifiques sur le phénomène) pourrait être soulevé dans un tel cadre.

Le protocole de coopération de 2004 prévoit la possibilité de mettre en place une plateforme de collaboration ad hoc concernant la captation de données en matière d'espionnage économique. Le Comité permanent R constate qu'après l'enquête de contrôle de 2013, ni la VSSE, ni le SGRS n'y ont eu recours.

Quelque 10 ans plus tard, d'autres plateformes de coordination ont certes été établies. L'une des plateformes a été chargée d'accorder une attention particulière à la préservation du PES, sous la présidence de la VSSE. En 2018, la VSSE et le SGRS ont présenté à ce sujet une proposition de Plan Stratégique National du Renseignement (PSNR). Il s'agit d'un document donnant notamment un aperçu des coopérations et synergies déjà existantes entre les deux services de renseignement, ainsi que des propositions de coopération futures.

Il est important de noter que, dans ce PSNR, les services attirent l'attention sur le fait que l'architecture du renseignement en Belgique est limitée en comparaison avec nos pays voisins. L'activité de renseignement est en effet habituellement divisée en (au moins) 4 services, parmi lesquels un service de renseignement stratégique et externe ainsi qu'un service d'interception de communications ou service technique. En Belgique, il n'existe pas de véritable service de renseignement externe consacré spécifiquement à la sécurité, ni aux intérêts vitaux et essentiels de l'État fédéral à l'appui de la politique économique du pays. Par défaut, le SGRS remplit en partie ce rôle, mais seulement dans le domaine de la sécurité au sens large du terme.

En décembre 2020, le Centre pour la Cybersécurité Belgique (CCB) a également été invité pour la première fois à la session plénière virtuelle de la plateforme PES.

ÉVALUATION DU COMITÉ PERMANENT R

Le Comité permanent R constate que la question de la protection du PES ne figure pas au premier rang de la liste des priorités des services de renseignement. Les initiatives prises en ce domaine sont toujours contrées par l'actualité. Depuis 2014, les services ont été confrontés successivement à la « filière syrienne », aux attentats de Paris et de Bruxelles, à la montée de l'extrémisme et, enfin, à un retour marqué et saisissant de la guerre froide. Ces différentes menaces ont contraint les services à se réorienter en permanence, ce qui a considérablement réduit l'attention accordée au PES. De l'avis du Comité permanent R, les moyens supplémentaires promis en termes de personnel et de matériel doivent également être affectés - de façon permanente - à la protection du PES. Le Comité permanent R estime également que la protection du PES pourrait faire l'objet d'un suivi par l'intermédiaire d'une plateforme commune entre les deux services de renseignement.

II.4. QUATRIÈME RECOMMANDATION : DIRECTIVES EN MATIÈRE DE COLLABORATION AVEC DES SERVICES DE RENSEIGNEMENT ÉTRANGERS

Recommandation - Enquête de contrôle PRISM (2013)

En 2012, la VSSE a rédigé l'« Instruction en vue d'une collaboration bilatérale avec les correspondants », qui est détaillée. Le Comité permanent R considérait cette directive comme particulièrement précieuse. Il a néanmoins fait remarquer que certaines options prises par la VSSE devaient être endossées par les responsables politiques, c'est-à-dire les membres du Comité ministériel du renseignement et de la sécurité. De plus, un des aspects les plus importants de cette collaboration – quels renseignements peuvent être communiqués à des services extérieurs ? – n'a été abordé que de manière sommaire. Le Comité permanent R réitère sa recommandation selon laquelle la VSSE doit transmettre sans délai sa directive – qu'elle aura complétée avec des règles plus précises en matière d'échange d'informations – au Comité ministériel.[5]

La même recommandation vaut pour le SGRS, certainement maintenant que le Comité permanent R a pu constater dans le cadre de la présente enquête l'existence d'une collaboration étroite avec des sections SIGINT étrangères. À l'instar de la VSSE, le SGRS prépare une note similaire avec des « critères d'évaluation » dans le cadre de la collaboration avec des services de renseignement étrangers (au sens large). Cette note serait finalisée dans le courant de l'année 2014. Le Comité insiste sur l'importance d'une telle directive pour le SGRS parce que – aussi après l'approbation du Comité ministériel – elle peut offrir un cadre légitime aux accords de coopération que le service de renseignement militaire conclut dès aujourd'hui.

En outre, le Comité recommande que les directives soient, dans la mesure du possible, au même niveau pour le SGRS *et* la VSSE. Selon le Comité, le SGRS peut dès lors s'inspirer des éléments suivants, qui ont été repris par la VSSE dans son instruction confidentielle ci-dessus :

- il faut tenir compte des facteurs susceptibles de peser sur la collaboration (tels que des problèmes d'ingérence, des intérêts opposés, le respect des droits fondamentaux, ...) ;

- les propres missions légales doivent toujours être sauvegardées, certainement dans des matières telles que le terrorisme et l'extrémisme qui prennent très vite une dimension judiciaire ;

- la collaboration avec des services étrangers doit être tout à fait transparente et traçable (ce qui permet notamment un contrôle par le Comité permanent R) ;

- une évaluation périodique de la collaboration doit être réalisée.

Par ailleurs, le Comité recommande une évaluation effective et régulière de la collaboration sur la base des critères prédéfinis. Les récentes révélations en démontrent la nécessité.

Le Comité permanent R ne veut néanmoins laisser subsister aucun malentendu : il est convaincu que les services de renseignement belges doivent continuer d'investir dans une bonne collaboration avec les services étrangers, et ce tant sur le plan bilatéral que multilatéral.

Pour ce qui concerne le suivi donné à cette recommandation, on peut simplement se référer à ce qui est indiqué dans le cadre de la deuxième recommandation (« la conception de la notion de services amis »).

ÉVALUATION DU COMITÉ PERMANENT R

Depuis 2012, la VSSE a pris l'initiative d'élaborer une directive pour l'évaluation de ses relations bilatérales avec les partenaires stratégiques. Le ministre de la Défense de l'époque a également signé la directive, de sorte qu'elle s'appliquait également au SGRS.

---

[5] COMITÉ PERMANENT R, Rapport d'activités 2012, p. 95.

Lors de l'enquête du Comité permanent R sur le *Memorandum of Understanding* (MoU) entre le SGRS et le service de renseignement rwandais, le National Intelligence and Security Services (NISS), le Comité a évalué le memorandum et a formulé une série de recommandations pour le rendre plus efficace. Depuis, les services sont tenus de procéder à des évaluations conjointes de leurs partenaires stratégiques communs. Ils sont également tenus d'évaluer ces relations tous les deux ans.

II.5. CINQUIÈME RECOMMANDATION : LA NÉCESSITE D'UNE COUVERTURE POLITIQUE POUR LES ACCORDS DE COOPÉRATION

Recommandation - Enquête de contrôle PRISM (2013)
Le Comité estime que les services doivent faire preuve d'un plus grand esprit d'ouverture concernant les accords de coopération existants aux niveaux bilatéral et multilatéral, et ce en premier lieu à l'égard des ministres compétents. En effet, dans le cadre de tels accords de coopération, des engagements peuvent être pris ou des choix opérés, qui dépassent le niveau de décision d'un service de renseignement et qui nécessitent une évaluation et une couverture politiques. En d'autres termes, les ministres compétents doivent être suffisamment informés, de telle sorte qu'il leur soit toujours possible d'assumer leur responsabilité politique. Ce qui est « politiquement pertinent » peut toutefois évoluer avec le temps.

La « *Directive concernant les relations des services de renseignement belges avec les services de renseignement étrangers* » (voir supra - deuxième recommandation) prévoit la possibilité de conclure un accord de coopération formel ou informel avec un service étranger.

Cette directive ne précise pas clairement si la VSSE et le SGRS doivent obtenir ou non une autorisation ministérielle préalable ou l'autorisation d'une autre instance. Aux yeux du Comité permanent R, une telle autorisation semble essentielle, étant donné que tout accord de coopération doit être couvert politiquement.[6]

Il convient de noter qu'outre cette recommandation de 2013, une nouvelle recommandation a été formulée en 2017 par le Comité permanent R. Cette nouvelle recommandation confirmait la recommandation de 2013 : « *Dans le cadre des liens de coopération établis par le SGRS (mais aussi par la VSSE) au niveau international, des engagements ou des choix nécessitant une évaluation et une couverture politiques peuvent être posés. En tant que principe général, le Comité avait précédemment recommandé que les ministres compétents soient correctement informés afin d'être en mesure d'assumer leurs responsabilités politiques vis-à-vis du parlement.* »

La recommandation de 2013 a été cependant quelque peu affinée en 2017 : « *Le Comité réitère cette recommandation et la rend plus concrète, en avançant des éléments susceptibles de constituer des critères permettant d'apprécier l'opportunité et le moment adéquat pour le service d'informer le ministre. Entre autres éléments : le bureau qui mènera l'opération, le lieu de l'opération (dans une zone de conflit ? Dans un domaine d'opération militaire belge ?) ; l'ampleur des risques stratégico-politiques (listés de manière structurée et formelle), le contexte international, la question de savoir s'il existe ou non un lien avec une enquête judiciaire, le danger de compromission de l'opération... Cette énumération n'est pas exhaustive. Il appartient au service et au ministre de compléter la liste et d'en développer les éléments si nécessaire.* »[7]

---

[6] Voir en ce sens : Proposition de loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité en vue d'instaurer des notes d'évaluation pour la collaboration avec les services de renseignement et de sécurité étrangers, Doc. parl. Chambre 2019-20, n° 55- 956/001 (23 janvier 2020).

[7] COMITÉ PERMANENT R, Rapport d'activités 2017, 107 (XII. Couverture politique des accords de coopération.)

ÉVALUATION DU COMITÉ PERMANENT R

À l'occasion de l'enquête sur le MoU Rwanda (voir supra - quatrième recommandation), le Comité permanent R a instauré l'obligation que les accords bilatéraux entre les services et leurs partenaires stratégiques soient approuvés ou couverts par le ministre compétent.

À ce jour, le Comité permanent R renvoie à sa recommandation prise en 2017 et relative à la coopération avec un partenaire étranger. De l'avis du Comité permanent R, l'assentiment politique demeure en effet toujours nécessaire avant la conclusion d'accords bilatéraux ou internationaux.

II.6. SIXIÈME RECOMMANDATION : LA NÉCESSITE QUE LE COMITÉ MINISTERIEL DU RENSEIGNEMENT ET DE LA SÉCURITÉ DONNE UNE ORIENTATION POLITIQUE

Recommandation - Enquête de contrôle PRISM (2013)

Le Comité ministériel du renseignement et de la sécurité a été créé comme un organe d'orientation politique du travail de renseignement. Il a pour tâche, de définir, par le biais de directives, la politique générale en matière de renseignement, de fixer les priorités des deux services de renseignement, de veiller à une coordination entre les services et de fixer les règles en matière de collaboration internationale et d'échange de données. Le Comité ministériel ne s'est toutefois pas réuni après les révélations.

Le Comité estime souhaitable que le Comité ministériel remplisse son rôle de « pilote » - aussi sur les conseils des deux services de renseignement qui font en outre partie du Collège du renseignement et de la sécurité - concernant le phénomène de captations massive de données et de l'espionnage politique et économique. Le Comité estime que de cette manière, la Belgique pourrait, du moins en partie, satisfaire à l'obligation positive reprise à l'article 8 CEDH de protéger la vie privée de ses citoyens.[8]

Par ailleurs, le Comité attire l'attention sur l'absence d'approbation formelle par le Comité ministériel de la liste proposée à la fin 2012, reprenant les entreprises dont le SGRS doit protéger le PSE.

Le Comité ministériel du renseignement et de la sécurité a entretemps été transformé en Conseil National de Sécurité (CNS).

Pour autant que le Comité permanent R a pu le vérifier, le CNS n'a, après l'enquête PRISM de 2013, pas accordé d'attention spécifique au phénomène de la captation massive de données.

ÉVALUATION DU COMITÉ PERMANENT R

Le Comité permanent R estime qu'il appartient au CNS de définir la politique générale en matière de renseignement et les priorités qui en découlent. Cependant, le Comité permanent R attend toujours du CNS une implication plus active en la matière.

---

8 Voir dans la même veine la recommandation de la Commission LIBE : « exhorte les États membres à satisfaire immédiatement à l'obligation positive, qui leur incombe au titre de la convention européenne des droits de l'homme, de protéger leurs citoyens des activités de surveillance contraires aux dispositions de la convention, y compris lorsque ces activités visent à garantir la sécurité nationale, réalisées par des pays tiers et à veiller à ce que l'état de droit ne soit pas affaibli par l'application extraterritoriale du droit d'un pays tiers », dans: PARLEMENT EUROPÉEN, Commission des libertés civiles, justice et affaires intérieures, Projet de rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI), PR/1014703FR.doc, PE526.085v02-00, 8 janvier 2014).

II.7. SEPTIÈME RECOMMANDATION : COLLABORATION INTERDÉPARTEMENTALE EN MATIÈRE DE *CYBERSECURITY, ICT-SECURITY* ET *CYBERINTELLIGENCE*

Recommandation - Enquête de contrôle PRISM (2013)

Certains aspects des révélations d'E. Snowden pointaient des faiblesses dans les systèmes de sécurité des réseaux IT des acteurs privés *et* des institutions publiques. Par conséquent, le Comité insiste à nouveau sur la nécessité d'accorder davantage d'attention à la *cybersecurity et à la ICT-Security* (INFOSEC) et sur le fait que ces problématiques – qui ne font pas uniquement partie des tâches des services de renseignement – requièrent une collaboration interdépartementale. Ainsi, par exemple, un rôle crucial est dévolu à l'Autorité nationale de sécurité en la matière.

Par ailleurs, le Comité se réfère à cet égard à l'approbation d'un projet d'arrêté par le Conseil des ministres du 19 décembre 2013, qui doit mener à la création d'un « Centre pour la Cybersécurité Belgique » à la Chancellerie du Premier ministre. En outre, des moyens supplémentaires ont été alloués pour mettre en œuvre la stratégie en matière de cybersécurité, comme approuvé à la fin 2012. Une partie de ces moyens serait destinée au SGRS[9], ce qui doit permettre à ce service d'accroître sa capacité et d'accorder davantage d'attention à la *cyberintelligence*. Le Comité permanent R est toutefois convaincu que la *cybersecurity* et la *cyberintelligence* continueront de nécessiter des investissements dans les décennies à venir.

Le Comité permanent R constate que le CCB a été créé le 10 octobre 2014. Cependant, le CCB prend part, depuis décembre 2020, aux discussions plénières de la plateforme PES, sous la présidence de la VSSE.

Le CCB ne participe toutefois pas systématiquement aux réunions du Comité stratégique, ni à celles du Comité de coordination du renseignement et de la sécurité, ni à celles encore du CNS.

Le CCB n'a pas non plus pour mission de détecter les cybermenaces, ni la responsabilité directe de protéger le PES.

ÉVALUATION DU COMITÉ PERMANENT R

Depuis les révélations de l'affaire Snowden, d'importants développements ont été observés dans le paysage de la sécurité belge et le Comité permanent R ne peut que s'en féliciter. Ainsi, la future structure de l'Autorité Nationale de Sécurité (ANS), actuellement toujours en cours d'élaboration, et le *Cyber Command* de la Défense belge vont changer radicalement le paysage actuel du renseignement et de la sécurité. Le Comité permanent R estime que ces deux nouvelles entités devront travailler à la protection des intérêts vitaux de la Belgique sous la surveillance collégiale du CNS. Des efforts plus importants devront être déployés dans le domaine de l'homologation des systèmes informatiques et du développement d'une cryptographie propre. Néanmoins, le Comité permanent R estime nécessaire de souligner, qu'outre les investissements matériels, le maillon faible dans ce contexte est le « facteur humain ». Des efforts doivent être consentis afin de sensibiliser régulièrement le personnel aux menaces que constituent les technologies de captation massive.

---

9 Recrutement de cinq personnes en 2014 et encore cinq en 2016.

II.8. HUITIÈME RECOMMANDATION : LES CONSÉQUENCES NÉGATIVES DU COMPARTIMENTAGE ET DU SECRET AU SEIN DU SGRS

Recommandation - Enquête de contrôle PRISM (2013)
Le nombre très restreint de personnes, au sein du SGRS, qui ont un accès direct aux informations SIGINT et la stricte confidentialité autour de ce thème font qu'il peut être difficile d'avoir une vue d'ensemble. Aussi le Comité est-il d'avis que le SGRS devrait réfléchir à la question de savoir s'il est possible de mieux concilier les principes de *need to know* et de *need to share*.

Spécifiquement interrogé à ce sujet, le SGRS a fait savoir que la situation n'avait guère évolué.

ÉVALUATION DU COMITÉ PERMANENT R

Compte tenu des constatations faites à l'occasion d'une enquête postérieure[10] à l'enquête de contrôle PRISM de 2013 et des informations fournies en juin 2022, le Comité permanent R estime qu'en ce qui concerne cette recommandation, des progrès insuffisants ont été engrangés et qu'il est encore question d'un compartimentage inacceptable au SGRS. La raison, entre autres, est l'absence d'un système informatique intégral unique au sein de ce service.

Le Comité permanent R estime que le SGRS doit maximiser davantage la disponibilité de l'information. Pour y parvenir, des investissements doivent être consentis dans des bâtiments adéquats et dans une infrastructure informatique performante. Le Comité estime que le SGRS doit fournir les efforts nécessaires pour amener les décideurs politiques à ces nécessaires investissements.

[10] Voir en particulier l'« *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* ».

II.9. NEUVIÈME RECOMMANDATION : LE CHAMP D'APPLICATION TERRITORIAL DE LA LOI MRD

Recommandation - Enquête de contrôle PRISM (2013)
Les évolutions technologiques rendent indispensable une précision du champ d'application territorial de la Loi MRD. Dans l'attente d'une éventuelle initiative législative, le Comité donne une interprétation plus prudente de l'actuelle réglementation, dans le sens où la méthode MRD ne peut être mise en œuvre pour des communications qu'au moment où le signal d'une communication à capter se trouve sur le territoire belge.

La Loi modifiant la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et l'article 259*bis* du Code pénal (*MB* du 28 avril 2017 ; ci-après la loi d'actualisation MRD - Méthodes de recueil de données) a apporté d'importantes modifications au champ d'application territorial des méthodes spécifiques et exceptionnelles, désignées méthodes MRD. La modification législative a une incidence sur le fonctionnement géographique des méthodes MRD étudiées dans le cadre de cette enquête de contrôle, à savoir l'interception de (télé)communications (*cf.* art. 18/17 de la loi sur les services de renseignement et de sécurité (L.R&S)) et l'intrusion dans des systèmes informatiques (*cf.* art. 18/16 L.R&S).

Quant à la VSSE

Avant la modification législative précitée, une méthode MRD ne pouvait être mise en œuvre que *sur le territoire du Royaume*. La loi stipule, à ce jour, que le service de renseignement exerce les méthodes MRD *« sur ou à partir du territoire du Royaume »* (*cf.* art. 18/1, 1° L.R&S).

L'exposé des motifs [11] de la loi d'actualisation MRD précise à cet égard que la VSSE doit désormais « mettre en œuvre » les méthodes MRD « sur » le territoire belge, ce qui signifie que les agents de la VSSE ne peuvent pas se rendre à l'étranger pour, par exemple, inspecter une habitation, installer un micro ou une caméra, voire encore scanner un téléphone. L'exposé des motifs indique que la collecte d'informations, elle-même, peut en revanche se dérouler à l'étranger.[12]

Quant au SGRS

Pour ce qui concerne le SGRS également, la loi d'actualisation MRD a apporté des changements dans le champ d'application territorial des méthodes MRD. À cet égard, le législateur a encore franchi un pas supplémentaire pour le SGRS en ne liant plus aucune restriction territoriale à l'exercice des méthodes MRD (*cf.* art. 18/1, 2° L.R&S).

L'exposé des motifs[13] de la loi d'actualisation MRD précise à cet égard que cette modification se justifie par le fait que la majorité des missions du SGRS sont exécutées à l'étranger, comme par exemple la protection des missions des Forces armées ou la protection des ressortissants

---

[11] EdM, *Doc. parl.* Chambre 2015-16, n° 54-2043/001, pp. 46-47.

[12] Pour clarifier la chose, les exemples suivants sont donnés, lesquels sont également immédiatement pertinents pour la présente enquête de contrôle : (1) l'intrusion informatique exécutée à partir de la Belgique mais sur un réseau qui dépasse les frontières et (2) si une cible mise sur écoute reçoit un appel de l'étranger.

[13] EdM, *Doc. parl.* Chambre 2015-16, n° 54-2043/001, pp. 47-50.

belges à l'étranger. Il est également indiqué que, dans le cadre des opérations avec mandat donné par le Conseil de Sécurité des Nations unies, il est souvent attendu des services de renseignement de la coalition qu'ils mènent des enquêtes de renseignement nécessitant le recours à des méthodes spécifiques et exceptionnelles et que la limitation du champ d'application territorial empêche le SGRS de remplir adéquatement sa part de travail dans le cadre de la coopération [14] internationale.

L'exposé des motifs indique également que l'interdiction de mettre en œuvre des méthodes spécifiques et exceptionnelles à l'étranger pose actuellement de sérieux problèmes.

Les exemples suivants sont significatifs dans le cadre de la présente enquête de contrôle :

- « *Par exemple, lors d'une opération militaire à l'étranger, si le GSM d'un kamikaze est retrouvé, le SGRS ne peut pas collecter les données s'y trouvant et pouvant fournir des informations cruciales sur d'éventuelles nouvelles menaces. En effet, il s'agit d'une méthode exceptionnelle d'intrusion dans un système informatique (article 18/16 L.R&S) autorisée uniquement sur le territoire du Royaume.* » Ensuite, « *il est précisé que l'intrusion informatique sur base de l'article 44/1 L.R&S (voir infra) ne pourra pas avoir lieu si le kamikaze n'appartient pas à une organisation ou une institution listée dans le plan annuel d'intrusion. Par exemple, si un militaire belge se radicalise à l'étranger, le recours à la méthode exceptionnelle visée à l'article 18/16 L.R&S est indispensable car il va de soi que l'armée belge ne sera jamais dans la liste des institutions et organisations à surveiller et reprises dans le plan annuel d'intrusion informatique* » ;
- « *Art. 18/7 L.R&S : l'utilisation d'un IMSI catcher permet de localiser un individu menaçant dont on connait le numéro de téléphone. Cette localisation pourrait par exemple être indispensable lorsque le SGRS découvre qu'un militaire belge désaxé planifie, en opération, une vengeance contre ses propres collègues* » ;
- « *Art. 18/8 L.R&S : pour remonter des filières de passeurs (par exemple trafic de migrants), le travail de renseignement nécessite la prise de connaissance des contacts existant entre la cible à l'étranger et d'autres individus. La possibilité légale de se connecter, grâce à un moyen technique, à une antenne pour collecter les données d'appel d'un target dont l'organisation ne se trouve pas dans le plan d'écoute, rendrait ce travail beaucoup plus efficace* » ;
- « *Art. 18/16 L.R&S : le SGRS identifie un individu susceptible de présenter une cyber-menace contre un intérêt militaire : cet individu est localisé à l'étranger et ne fait pas partie d'une organisation ou d'une institution se trouvant sur le plan annuel d'intrusions informatiques visé à l'article 44/3 L.R&S. Le SGRS doit pouvoir procéder à une intrusion, à l'étranger, dans le système informatique de cet individu pour collecter les données permettant de prévenir une attaque, d'identifier l'ensemble des individus menaçants, ...* » ;

[14] EdM, *Doc. parl.* Chambre 2015-16, n° 54-2043/001, p. 6.

- « *Art. 18/17 L.R&S : le SGRS doit pouvoir mettre sur écoute un individu prenant en otage un navire belge dans les eaux internationales, même si celui-ci ne fait pas partie du plan d'écoute visé à l'article 44/3 L.R&S* ».

Enfin, il convient de noter que l'exposé des motifs précise que la mise en œuvre de méthodes spécifiques et exceptionnelles lors d'opérations à l'étranger n'est pas toujours praticable.[15]

ÉVALUATION DU COMITÉ PERMANENT R

De l'avais du Comité permanent R, dans le cadre de la modification de la loi sur les services de renseignement et de sécurité, menée en 2017, l'application territoriale de la loi MRD a été clarifiée.

Cette modification permet également au SGRS de prendre des images fixes ou animées et de procéder à l'intrusion dans un système informatique à l'étranger, dans le cadre de l'article 44 L.R&S. En conséquence, ces méthodes, qui sont équivalentes aux méthodes prévues aux articles 16/4 et 18/16 L.R&S, ne sont plus soumises à l'approbation de la Commission BIM, mais relèvent directement du contrôle du Comité permanent R.

De manière quelque peu surprenante, le Comité permanent R a dû constater, à la suite du contrôle qu'il a mené sur les méthodes MRD, que le SGRS n'avait jusqu'à présent jamais déployé pareilles méthodes à l'étranger.

[15] EdM, *Doc. parl.* Chambre 2015-16, n° 54-2043/001, 7, p. 84 et 86.

II.10. DIXIÈME RECOMMANDATION : UNE RÉGLEMENTATION INT PLUS PRÉCISE

Recommandation - Enquête de contrôle PRISM (2013)

La réglementation INT belge, qui autorise le SGRS à intercepter des communications à l'étranger, a été élaborée à une époque où les interceptions concernaient essentiellement des signaux radio. Depuis lors, la technologie a connu une telle évolution que cette réglementation devrait être réexaminée par le législateur. Les révélations d'E. Snowden n'ont fait que confirmer ce constat. Des éléments qui doivent en tous points être examinés lors d'une telle révision, sont dans quelle mesure les interceptions doivent ou non être ciblées, la portée exacte de la possibilité de « rechercher » des signaux, le degré de précision du Plan d'écoutes annuel, la possibilité de procéder à du *datamining* dans des informations en vrac et la question de savoir si les opérations SIGINT internationales doivent entrer dans le cadre d'un « mandat international » plus large.

Le SGRS dispose d'une compétence particulière pour intercepter des communications étrangères.

Cette compétence « SIGINT » (*Signals Intelligence*) a été instituée par la loi sur le renseignement du 30 novembre 1998 (L.R&S), et modifiée et étendue par la loi du 3 avril 2003. La modification législative de 2003 a fait en sorte que la compétence du SGRS ne s'est plus limitée exclusivement à l'interception de radiocommunications militaires, mais a été élargie à tous les types de communications émises à l'étranger.[16]

Un nombre limité de changements principalement législatifs ont été apportés par les lois du 4 février 2010[17] et du 5 mai 2014.

Une dernière modification (à ce jour[18]), substantielle dans son contenu, est intervenue par l'entremise de la loi d'actualisation MRD du 30 mars 2017 qui a apporté en la matière les modifications suivantes :

1. Les possibilités d'interception du SGRS ne concernent pas seulement les communications « émises à l'étranger ». Les possibilités sont étendues dans le sens où les communications « reçues à l'étranger » relèvent désormais également du champ d'application. Le SGRS a ainsi acquis la compétence d'intercepter toute forme de communication à l'étranger, indépendamment de la personne à l'origine de l'appel et de l'endroit où se trouve celle-ci, pour autant qu'une partie de la communication se déroule à l'étranger ;

2. Une obligation légale de coopérer a été créée dans le cadre de la mise en œuvre de la compétence d'interception dans le chef des opérateurs et fournisseurs de télécommunications. L'exposé des motifs précise que : « *[l]a manière la plus efficiente et la plus rapide de faire du cable taping est de solliciter la collaboration des opérateurs de réseau et des fournisseurs de services de télécommunications. La collaboration de*

---

16 EdM, *Doc. parl.* Chambre 2002-2003, n° 50-2059/001, pp. 4-6.

17 Via la loi MRD du 4 février 2010, il a été ajouté à la réglementation SIGINT - définie à l'époque notamment à l'article 259*bis*, §5 du Code pénal - que le SGRS, outre la captation, l'écoute, la prise de connaissance et l'enregistrement de communications étrangères, était compétent pour le repérage de telles communications.

18 L'exposé des motifs de la loi d'actualisation MRD indique qu'une évaluation devra intervenir dans les cinq ans suivant l'entrée en vigueur de la loi.

certains opérateurs actifs en Belgique, qui offrent des services de transmission par câble vers et de l'étranger, permettrait en effet plus facilement d'intercepter des flux de communications et de données émises à l'étranger. Ces flux seront filtrés par le SGRS sur la base du plan d'écoute afin de n'extraire que les communications et données émises à l'étranger et autorisées par ce plan et en lien avec les missions du SGRS. »[19]

Le *cable taping*, qui faisait déjà partie des possibilités légales du SGRS depuis la loi du 3 avril 2003 (*supra*), gagne ainsi en praticabilité ;

3. La réglementation SIGINT, à savoir l'interception de communications étrangères (*cf.* art. 44 L.R&S), a été élargie à une réglementation CYBER, à savoir l'intrusion dans les systèmes informatiques étrangers (*cf.* art. 44/1 L.R&S) et une réglementation pour l'enregistrement d'images à l'étranger (*cf.* art. 44/2 L.R&S). Tout comme il existe un plan d'écoute annuel approuvé par le ministre de la Défense, qui contient une liste des organisations et institutions qui feront l'objet des interceptions concernées, un plan annuel relatif aux intrusions et un plan annuel relatif à la prise d'images sont exigés. Ces derniers plans comprennent également une liste des organisations et institutions devant faire l'objet d'un suivi ;

4. Précisons que le SGRS peut mettre en œuvre ces compétences SIGINT, CYBER et de prise d'images dans toutes ses missions légales de renseignement et de sécurité, à l'exception de la réalisation des enquêtes de sécurité et de vérifications de sécurité ;

5. Ce qui est significatif dans ce contexte est que la mission de renseignement du SGRS a été considérablement élargie. Dans le cadre de sa mission de renseignement, le SGRS se doit désormais également : « *de rechercher, d'analyser et de traiter le 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 [...] et d'en informer sans délai les ministres compétents* » (cf. art. 11, §1, 1° *in limine* L.R&S). Cette composante de la mission de renseignement est appelée « soutien en renseignement aux opérations militaires ». Cette extension du champ d'application crée également logiquement un champ d'application plus large pour la compétence d'interception visée à l'article 44 L.R&S ;

6. Le contrôle a été renforcé notamment par une motivation plus élaborée de la liste annuelle et par la transmission mensuelle au Comité d'une liste motivée de pays ou d'organisations et d'institutions qui ont fait l'objet d'une écoute, d'une intrusion ou d'une prise d'images. De cette manière, le Comité est régulièrement tenu informé des écoutes, intrusions et prises d'images effectuées ;

---

[19] EdM, *Doc. parl.* Chambre 2002-2003, n° 50-2059/001, 89.

7. Enfin, la perspective d'une évaluation obligatoire a été instaurée. L'exposé des motifs de la loi d'actualisation MRD stipule notamment que, dans les cinq ans suivant l'entrée en vigueur de la loi, il sera procédé à une nouvelle évaluation de la situation pour voir si les prérogatives du SGRS sont praticables à l'étranger.

ÉVALUATION DU COMITÉ PERMANENT R

À cet égard, le Comité permanent R estime que la législation actuelle est suffisante.

II.11. ONZIÈME RECOMMANDATION : UN RESPECT STRICT DE L'ARTICLE 33 L.CONTRÔLE

Recommandation - Enquête de contrôle PRISM (2013)
Pour pouvoir exercer sa mission de contrôle, la Comité permanent R insiste sur l'obligation reprise à l'article 33 L.Contrôle de transmettre *« d'initiative au Comité permanent R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services »*. Cette obligation vaut également pour les conventions, MoU ou accords conclus au niveau international, que ce sur le plan bilatéral ou multilatéral.

Pour pouvoir exercer sa mission de contrôle, le Comité permanent R a insisté à plusieurs reprises[20] sur l'obligation de l'article 33 L.Contrôle visant le fait de transmettre *« d'initiative au Comité permanent R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services »*.

En 2020[21] encore, le strict respect de cet article a été spécifiquement recommandé au SGRS. Cette obligation valait également pour les conventions, MoU (et l'autorisation ministérielle correspondante ainsi que les approbations ministérielles dans le cas de collaborations informelles) ou accords conclus au niveau international, que ce soit sur le plan bilatéral ou multilatéral.

Quant à la VSSE

La VSSE est le seul service qui, de sa propre initiative, communique deux fois par an divers documents / notes au Comité. À chaque reprise, entre 20 et 40 documents sont envoyés. Seul un certain nombre de documents sont pertinents pour les missions de contrôle et autres du Comité. Les autres documents portent principalement sur des questions administratives et logistiques.[22]

Les appels internes à candidatures, les mouvements de personnel, les notes de service et les circulaires (par exemple la note de service sur les mandataires politiques, la circulaire sur la procédure de reconnaissance des communautés religieuses, la récente note de service sur la réorganisation de la Direction des opérations), les lettres d'information (par exemple celle sur l'introduction du nouveau modèle d'enquête), les communications et les rapports de réunion du comité de direction (qui fournissent souvent des explications sur des choix stratégiques), sont cependant intéressants et peuvent également être pertinents à cet égard.

---

[20] Des recherches ont déjà été effectuées à ce sujet : COMITÉ PERMANENT R, *Rapport d'activités 1996*, 28-32 (Rapport sur l'application par les services de renseignements de l'article 33 alinéa 2 L.Contrôle) ; *Rapport d'activités 2001*, 218-220 (Les informations indispensables dont le Comité permanent R estime devoir disposer afin d'accomplir sa mission efficacement) ; *Rapport d'activités 2002*, 27 (La transmission d'initiative par les services de renseignement de certains documents au Comité permanent R) ; *Rapport d'activités 2006*, 12 ; *Rapport d'activités 2013*, 116 ; *Rapport d'activités 2014*, 120.

[21] COMITE PERMANENT R, *Rapport d'activités 2020*, 174.

[22] Un certain nombre de documents transmis n'ont pas de réelle utilité pour le Comité ; il s'agit de « délégations de signature », d'annonces de réceptions, de permanences de Noël, ...

Le Comité a toutefois pu constater, de manière plutôt exceptionnelle certes, que tous les protocoles, directives, ... n'étaient pas transmis (par exemple le protocole BELPIU, certains MoU internationaux, ...).

Quant au SGRS

Toutes les directives sont réunies dans des *Standing Operating Procedures* (SOP), pas toujours actualisées. La *mise à jour* de ce recueil est depuis des années l'une des priorités des différents plans d'action du service de renseignement militaire. [23]

ÉVALUATION DU COMITÉ PERMANENT R

Le Comité permanent R doit souvent rappeler aux deux services de renseignement l'obligation découlant de l'article 33 de la loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace. La transmission de directives, de SOP et d'autres prescriptions n'est toujours pas automatique ni systématique. Le Comité R prie instamment les services de procéder à la transmission systématique de ces documents.

Selon le Comité permanent R, le respect de l'article 33 de la loi organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace demeure un point d'amélioration, certes bien davantage pour le SGRS que pour la VSSE.

[23] J5-DOC semble être chargé de ce processus : gestion centralisée des SOP, MOU, STANAG OTAN, etc.