DIFFUSION RESTREINTE
(A.R. 24.03.2000)

COMITE PERMANENT DE CONTROLE DES SERVICES
DE RENSEIGNEMENT ET DE SECURITE

Numéro de notice 2023.310

Enquête de contrôle concernant les actions menées par les services de renseignement pour détecter la menace d'ingérence de puissances étrangères par le financement de partis politiques, institutions politiques ou personnalités politiques en Belgique

DIFFUSION RESTREINTE
(A.R. 24.03.2000)

TABLE DES MATIERES

I. INTRODUCTION

I.1. ORIGINE DE L'ENQUETE

Le 17 avril 2023, la Présidente de la Chambre des représentants, qui préside également la Commission d'accompagnement Renseignement et Sécurité, a demandé au Comité permanent R d'ouvrir une enquête sur les actions menées par les services de renseignement pour détecter la menace d'ingérence de puissances étrangères par le financement de partis politiques, institutions politiques ou personnalités politiques en Belgique.

Dans un message daté du 28 avril 2023, la Chambre a précisé sa demande en indiquant souhaiter l'examen de quatre questions spécifiques.

I.2. COMPETENCE DU COMITE PERMANENT R ET PORTEE DE L'ENQUETE

L'article 33 de la loi du 18 juillet 1991 organique 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 permanent R enquête sur les activités et les méthodes des services de renseignement et la manière dont ils accomplissent leurs tâches (légalité, efficience, efficacité).
Les questions soulevées dans cette enquête portent exclusivement sur la légalité des activités de renseignement de la VSSE et du SGRS et sur l'adéquation de l'analyse des renseignements recueillis.

I.3. QUESTIONS DE FINALITE

L'article 8, 1°, g) de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) définit l'ingérence comme *« la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins*. »

L'objectif de l'enquête est d'analyser comment la VSSE et le SGRS détectent la menace d'ingérence de puissances étrangères par le financement de partis politiques, institutions politiques ou personnalités politiques en Belgique.
Les questions suivantes sont examinées en particulier :

- Quelles actions mènent-ils aujourd'hui ?
- Quelles actions devraient-ils mener ?
- Quelles sont les compétences et les moyens nécessaires pour mener à bien cette mission ?
- Quelles actions mèneront-ils à l'avenir, compte tenu de l'évolution de la situation, notamment en matière de cybersécurité, et de l'augmentation des effectifs de la VSSE ?

I.4. METHODOLOGIE D'ENQUETE

La décision d'enquête a été approuvée lors de la réunion plénière du Comité permanent R le 14 novembre 2023 ; le Service d'Enquêtes R (SEDE) a ensuite été chargé de conduire l'enquête.

Le SGRS et la VSSE ont été informés par une notification écrite de l'ouverture de l'enquête, respectivement les 14 et 16 novembre 2023. Cette notification écrite reprenait également les questions initiales.
Le Comité a reçu les réponses du SGRS et de la VSSE à ces premières questions, respectivement les 11 et 21 décembre 2023.

Après l'analyse des réponses, le Comité s'est concerté oralement avec des représentants de la VSSE le 8 janvier 2024 et avec des représentants du SGRS le 9 janvier 2024. Les réponses qui avaient été données par les deux services ont été expliquées et des informations complémentaires ont été fournies le cas échéant.

Le présent rapport a été établi sur la base de toutes les informations fournies par les services de renseignement au cours de l'enquête.

II. QU'ENTEND-ON PAR INGERENCE (FINANCIERE) ?

La menace d'« ingérence » est définie à l'article 8, 1°, g) de la L.R&S comme *« la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins*. »
L'ingérence contourne les processus politiques démocratiques et constitue donc une sérieuse menace pour les institutions démocratiques. Concernant la Belgique spécifiquement, en tant que *host nation* de plusieurs institutions internationales et de l'UE, cela porte également sur les processus politiques au sein des institutions européennes.

Le fait que d'autres pays tentent d'influencer la prise de décision en Belgique n'est pas un problème en soi, car cela se fait généralement de manière légitime : lobbying, diplomatie, etc. Cependant, lorsque des puissances étrangères cherchent à promouvoir leurs objectifs stratégiques, politiques, militaires ou économiques par des moyens clandestins, illicites ou trompeurs, nous considérons qu'il s'agit d'ingérence.

Pour faire basculer un processus décisionnel à son avantage, l'acteur de la menace dispose d'une palette de moyens, entre autres par l'intermédiaire de ses services de renseignement. L'un des modes opératoires consiste à contacter clandestinement des décideurs ou encore à financer des groupes de réflexion de manière non transparente afin d'introduire une voix particulière (subversive, incendiaire, disruptive...) dans le débat. Le but de l'ingérence ne doit pas toujours consister à influencer directement le résultat d'un processus décisionnel. Il peut également s'agir d'objectifs plus subtils, tels que présenter un pays sous un jour favorable, détourner l'attention ou simplement retarder des décisions qui pourraient avoir des conséquences préjudiciables pour le pays concerné.

L'acteur de la menace choisit une cible et consacre du temps et des moyens à la manipuler en vue d'atteindre l'objectif. Cette action est elle aussi très subtile et ne doit pas toujours revêtir un caractère financier. Il arrive souvent que des personnes ayant un intérêt connu pour un pays soient invitées à se rendre dans le pays en question. Cette démarche peut être suivie de visites d'étude, d'invitations à des conférences ou d'opportunités économiques pour la personne ciblée ou son entourage. Ces activités peuvent être totalement transparentes et donc légitimes, mais elles peuvent tout aussi bien être clandestines ou trompeuses, auquel cas il peut être question d'un processus de recrutement pouvant mener à de l'ingérence.

Il est clair que l'ingérence couvre une vaste zone grise entre le lobbying légitime et l'espionnage clandestin, la variante transactionnelle de l'ingérence qui implique des transactions financières n'étant qu'une manifestation parmi d'autres.

Le processus de recrutement (élicitation) pour l'ingérence ou l'espionnage se déroule de la même manière. La cible est d'abord abordée de manière très « douce », par exemple lors d'une réception ou d'une conférence. Les sujets de conversation sont d'abord très généraux. S'il existe un lien personnel entre la cible/victime et l'agent de renseignement, la relation peut se poursuivre par des invitations répétées à des dîners, des voyages d'étude, des conférences à l'étranger, etc. De cette manière, la cible/victime se rapproche de plus en plus de ce que veut l'agent de renseignements. Si la relation progresse, des questions plus spécifiques sont posées, qui peuvent aller dans le sens de l'espionnage ou de l'ingérence.

Que la cible de la tentative de recrutement soit consciente ou non d'être manipulée n'a aucune importance pour l'auteur de la menace. Contrairement à l'espionnage, où la cible est à un moment donné très consciente du franchissement d'une limite (déontologique ou juridique), l'ingérence est un jeu sophistiqué où la ligne rouge réside dans la manière dont les moyens sont utilisés et dans l'identité du donneur d'ordre. Le législateur a considéré, à juste titre, que l'ingérence, telle que définie par la L.R&S, pouvait constituer une menace sérieuse pour la sécurité intérieure et extérieure de l'Etat.

L'ingérence pouvant avoir des conséquences (très) néfastes pour les institutions démocratiques du pays, il est extrêmement important que les personnes susceptibles d'être la cible d'une ingérence par des acteurs de la menace en soient conscientes. Les services de renseignement et de sécurité sont les mieux placés, compte tenu de leur expertise et de leur expérience, pour proposer des campagnes de sensibilisation aux mandataires politiques, par exemple. La sensibilisation, la transparence et la déontologie sont des armes proactives de choix contre les menaces d'ingérence.

Dans le cadre de la lutte contre l'ingérence, les services s'efforceront de détecter et d'identifier les activités des agents d'influence étrangers. En d'autres termes, l'enquête de renseignement se concentrera sur l'acteur de la menace plutôt que sur les cibles potentielles des tentatives d'influence. Les services ont comme mission légale de suivre les menaces, pas de suivre les vulnérabilités.
Ainsi, si un mandataire politique apparaît dans le cadre de l'enquête, c'est principalement en raison d'une enquête sur les activités d'un acteur de la menace et non l'inverse.

Le transfert de faveurs matérielles est un moyen d'atteindre l'objectif consistant à influencer le processus décisionnel. Dans le cadre de l'ingérence financière, des fonds (en espèces, en cryptomonnaies ou par le biais de transferts de fonds) sont transférés directement ou par l'intermédiaire d'hommes de paille à la cible de l'opération d'ingérence. En contrepartie, le processus décisionnel dans lequel la cible est impliquée est poussé dans une direction favorable à l'acteur de la menace.

L'acteur de la menace qui engage des moyens financiers tentera de les dissimuler. Comme pour toutes les enquêtes sur les flux financiers, cela nécessite une expertise de la part des enquêteurs, en particulier lorsque des structures d'entreprise complexes (étrangères) ou des cryptomonnaies sont utilisées.

III. LE FINANCEMENT DES PARTIS POLITIQUES ET DES CAMPAGNES ELECTORALES EN BELGIQUE

En février 2023, le Comité permanent R a rédigé une note juridique portant sur la loi du 4 juillet 1989 relative au financement des partis politiques. Cette note examinait si la réglementation existante permet de détecter les financements étrangers illégaux visant à influencer les décideurs politiques belges.

En contrepartie de leur financement, les partis politiques doivent respecter des obligations bien définies : la limitation des dépenses de propagande électorale, la réglementation de l'utilisation de certaines ressources électorales, l'interdiction des dons de personnes morales et d'associations de fait ainsi que la limitation et l'identification des dons de personnes physiques, la transparence de la comptabilité des partis politiques et le respect des droits et libertés garantis par la Convention européenne des droits de l'homme.

Dans sa note juridique, le Comité permanent R déclarait que :

« L'actualité montre que les tentatives d'influences sont probablement réalisées au travers de flux d'argent liquide non déclaré. L'objectif principal est de provoquer un enrichissement personnel des candidats et la trésorerie destinée à la propagande électorale n'est fournie que marginalement. Il n'est toutefois pas impossible que des acteurs représentant une menace au sens de la loi organique coordonnent leurs efforts pour utiliser les possibilités légales de financer des partis ou des candidats. Dans ce cas se pose la question de la réponse à apporter à ce comportement qui pourrait constituer une menace (potentielle) à la pérennité de l'ordre démocratique et constitutionnel, en rapport avec l'ingérence.

À cet égard, il faut renvoyer aux possibilités de communication de renseignements que la loi et la réglementation autorisent aux services de renseignement et de sécurité à l'égard d'organismes publics belges. Dans son « Analyse juridique des possibilités légales dont disposent les deux services de renseignement en matière d'entrave », le Comité permanent R écrivait :

La communication des renseignements [...] est régie en ordre principal par l'article 19, alinéa 1er L.R&S. Cet article dispose que : « les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 73, deuxième alinéa, — en d'autres termes, les informations traitées ('renseignements' ou 'intelligence') relatives aux menaces pour la sécurité qui relèvent de la compétence matérielle de la VSSE — 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 [à l' article] 7 [...]. » Ces menaces comprennent le terrorisme, l'extrémisme, l'espionnage, l'ingérence, la prolifération des armes de destruction massive, les organisations criminelles et les sectes nuisibles.

Bien que les catégories de destinataires soient largement définies, il est néanmoins important que l'article 19, alinéa 1er L.R&S constitue une liste exhaustive de destinataires.

L'article 19, alinéa 1er L.R&S doit être lu conjointement avec l'article 20, g[...]3, L.R&S.

Ce dernier stipule que :

« §3. Le Comité ministériel définit les conditions de la communication prévue à l'article 19, alinéa 1er, et de la coopération prévue au § 1er du présent article. »

Le Comité constate qu'il n'existe pas de directives particulières du Conseil national de sécurité (CNS) réglementant la communication et la transmission de renseignements dans les actions « qui sont entreprises avec l'intention d'entraver et pour lesquelles l'entrave constitue la finalité » (cf. l'objectif spécifique d'une communication et d'une transmission de renseignements par la VSSE d'une instance tierce, telle que définie par l'Administrateur général de la VSSE dans la note de service interne de la VSSE n° 18-50 [...]. »

L'emploi des termes « toutes les instances et personnes compétentes conformément aux finalités de leurs missions » indique que les missions du destinataire des renseignements doivent avoir un lien avec les renseignements transmis et que ses compétences lui permettent d'agir à l'égard de la situation. En l'occurrence, les services de renseignement et de sécurité doivent donc garder cela à l'esprit en envisageant de transmettre des renseignements relatifs à un schéma de financement de candidats ou de partis conforme à la loi, mais procédant d'une tentative d'ingérence. La Commission étant un organe ressortissant du pouvoir législatif, on peut imaginer que la simple information selon laquelle des partis ou candidats sont financés dans le cadre d'une tentative d'ingérence est susceptible de déclencher au sein de la commission une multitude de réactions (questions et interpellations parlementaires, propositions législatives, etc.). »

Les conclusions de cette analyse juridique du Comité permanent R sont les suivantes :

« La Belgique dispose d'un cadre juridique relatif au financement des partis politiques et au contrôle des dépenses électorales. Ce cadre juridique a évolué avec le temps, notamment dans

le but de répondre aux recommandations du GRECO[1], qui considère qu'un certain nombre de ses recommandations n'ont pas été pleinement mises en œuvre.

Les règles applicables aux dons et sponsorings au bénéfice des partis politiques (et à leurs composantes), à des listes, à des candidats et à des mandataires politiques sont pertinentes dans le cadre de la détection et de la lutte contre l'ingérence étrangère dans les processus politiques nationaux. Il en est de même des obligations de rapportage financier auxquelles sont soumis les partis politiques.

La Commission de contrôle joue un rôle important dans le contrôle des dispositions et peut prendre des décisions significatives (privation d'une partie de la dotation ou amendes administratives).

Les autorités judiciaires sont également responsables du respect de certaines dispositions sanctionnées par des peines d'amendes (comme l'acceptation de dons non enregistrés par des mandataires politiques), éventuellement en concours avec d'autres infractions.

Enfin, dans le cadre de leurs missions, les services de renseignement sont libres de mettre en œuvre des méthodes de recueil de données afin de recueillir des informations produites sur la base de dispositions de la Loi de 1989, en ce compris, par exemple, les relevés de l'identité des donateurs.

Il n'appartient pas au Comité permanent R de formuler des recommandations quant aux compétences légales de la Commission de contrôle et à la manière dont elle pourrait réagir si elle était informée de tentatives d'ingérences. Le Comité permanent R souligne tout de même, comme il l'a fait dans l'analyse juridique citée ci-dessus, que le Conseil national de sécurité doit encore élaborer une directive qui devrait encadrer les communications des services de renseignement et de sécurité à l'égard d'autres autorités publiques. Pour le reste, l'opportunité d'une communication ayant pour finalité une entrave d'une tentative d'ingérence doit être examinée au cas par cas par les services de renseignement et de sécurité. »

IV. L'INGERENCE (FINANCIERE) DE LA RUSSIE

En décembre 2022, le Comité permanent R a publié le rapport 2022.297 intitulé *« Position d'information des services de renseignement quant au financement par des fondations ou autres organisations ainsi qu'à l'influence exercée par la Russie sur les « politiciens » en Belgique. »*

[1] Le Groupe d'États contre la Corruption (GRECO) a été créé en 1999 par le Conseil de l'Europe pour veiller au respect des normes anticorruption de l'organisation par les Etats membres.

La conclusion de ce rapport est la suivante :

« La vie politique en Belgique — lisez belge mais aussi européenne — peut faire l'objet de tentatives d'ingérence russes. Les services de renseignement sont conscients de la menace et opèrent un suivi de celle-ci selon des angles différents (tenant compte de leurs compétences respectives).

La VSSE considère posséder une position d'information solide sur l'ingérence russe et indique que le service a déployé à cette fin d'importants moyens et ressources en personnel. Toutefois, « la visibilité du financement effectif en provenance de Russie demeure un domaine d'investigation essentiel. En tout état de cause, notre service ne dispose pas d'éléments concrets qui démontrent que des partis politiques belges sont financés de manière structurelle par des puissances étrangères, » selon la VSSE.

La VSSE indique que la menace d'ingérence ne provient pas que de la Russie. D'autres puissances étrangères mènent des actions de ce type qui constituent une menace, notamment le Maroc, le Qatar et la Chine.

(…)

De même, suivant en cela ce que les deux services de renseignement soulignent, le Comité R estime que la menace d'ingérence de la Russie, comme d'autres États, ne peut en aucun cas être réduite à une problématique de simple et seul financement de « politiciens ». Enfin, le Comité rappelle que la menace d'ingérence peut également provenir d'acteurs privés, qu'ils soient ou non reliés de quelconque manière à un État. »

En février 2020, le Comité permanent R a finalisé un rapport d'enquête 2019.270 intitulé *« Enquête de contrôle sur la manière dont les services de renseignement suivent les risques liés à une éventuelle ingérence d'acteurs étrangers dans le processus électoral belge, sur la manière dont ils tentent de contrer les menaces potentielles et sur la manière dont ils font rapport aux autorités, en particulier en ce qui concerne le risque de cyber-ingérence ou de cyber-attaques ».*

Ce faisant, le Comité permanent R a constaté que les deux services de renseignement avaient largement pris les mesures nécessaires pour contrer les éventuelles menaces visant les élections belges et européennes de mai 2019. Ils ont procédé à la mise en place d'une *Joint Intelligence Task Force (task force conjointe sur le renseignement)* (JITF) pour enquêter sur cette éventuelle menace.

Les services ont ainsi fait les constatations suivantes :

- Aucune opération d'influence planifiée et coordonnée à grande échelle n'a été détectée lors des élections belges et européennes. Cependant, des campagnes de désinformation ont été menées sous la forme d'une diffusion de certains narratifs.
- Les tactiques de désinformation sont constamment affinées. La portée globale de ces campagnes diminue, mais elles deviennent plus ciblées et plus difficiles à détecter. Par conséquent, il convient d'accorder une plus grande attention à l'étude de financements de canaux de communication et au soutien de la diffusion de certains narratifs.
- Un lien a pu être établi entre certains comptes de médias sociaux et des comptes liés à certains narratifs visant à créer un sentiment nationaliste et anti-UE au sein de la population.

Dans de cadre de cette enquête, le Comité permanent R a formulé les recommandations suivantes :

- Le Comité permanent R recommande au Conseil national de sécurité et aux deux services de renseignement d'exécuter l'obligation énoncée à l'article 20 § 4 L.R&S (coopération sur la base d'une directive du CNS concernant la collecte, l'analyse et le traitement de renseignements relatifs aux activités de services de renseignement étrangers sur le territoire belge), respectivement d'établir une directive et de conclure un accord de coopération.
- Le Comité permanent R estime que le modèle de la *Joint Intelligence Task Force* est une initiative réussie. Cette méthode pourrait s'appliquer avec le même succès à d'autres problématiques à l'avenir.
- Dans son enquête, le Comité permanent R note que la surveillance des médias sociaux par les services de renseignement génère encore globalement beaucoup de travail. Les services ne disposaient pas de suffisamment d'outils automatisés pour permettre une approche plus efficace. Le Comité permanent R estime qu'il convient d'investir dans ce domaine à l'avenir, compte tenu de l'intérêt croissant des médias sociaux et alternatifs dans la diffusion de la propagande et de la désinformation pour influencer l'opinion publique.

V. ACTIVITES DES SERVICES DE RENSEIGNEMENT RELATIVES A LA MENACE D'INGERENCE

V.1. SUIVI DE L'INGERENCE PAR LA VSSE

La VSSE déclare ne pas mener d'enquêtes de renseignement sur les partis politiques, les institutions ou les personnalités en soi, mais seulement si des indications concrètes et crédibles apparaissent dans une enquête de renseignement sur l'ingérence qu'un parti politique, une institution ou une personnalité particulière serait approché ou risque d'être victime d'une tentative d'ingérence.

Concernant la priorisation d'enquêtes sur les ingérences, la VSSE établit une distinction entre les acteurs d'ingérence systémique et non systémique. Les acteurs d'ingérence systémique sont des pays fondamentalement opposés aux principes de base sur lesquels la Belgique et, par extension, les sociétés européennes et occidentales reposent : au niveau politique, un système politique démocratique avec une séparation des pouvoirs, des élections libres et équitables et une protection constitutionnelle des droits et libertés fondamentaux ; et au niveau économique, une économie de libre marché (socialement corrigée). Les acteurs systémiques se concentrent donc sur l'affaiblissement des pays démocratiques, et l'ingérence est l'un des moyens utilisés pour y parvenir.

Toutefois, la menace d'ingérence peut également provenir d'acteurs non systémiques. Il s'agit de pays qui ne considèrent pas les Etats démocratiques comme un adversaire de principe ou existentiel (comme c'est le cas des acteurs d'ingérence systémique), et qui sont même prêts à coopérer avec les pays démocratiques dans de nombreux domaines, mais qui déploient des

activités de renseignement autour de thèmes spécifiques que le pays en question considère comme cruciaux. L'ingérence est une méthode permettant à ces pays d'influencer certaines décisions politiques au niveau belge ou européen dans un sens qui leur est favorable.

Les acteurs d'ingérence systémique se livrent également à une ingérence opportuniste dans les dossiers qu'ils jugent importants.

Le financement de partis ou de personnalités politiques n'est qu'un des nombreux moyens pouvant être employés dans les tentatives d'ingérence. Lorsqu'elle se produit, c'est dans le contexte du financement (illégitime) des partis — soutien financier aux partis politiques censés soutenir les objectifs politiques de l'acteur de l'ingérence pour des raisons idéologiques ou pragmatiques — ou dans le contexte de la corruption active — faveurs financières accordées à un mandataire politique pour qu'il adopte une certaine position politique, qu'il montre un certain comportement de vote ou qu'il facilite l'accès à certains décideurs. Toutefois, il s'agit là d'une exception plutôt que de la règle. Plus souvent qu'une compensation purement financière, l'ingérence implique un jeu subtil d'élicitation pour faire aboutir l'influence.

V.1.1. Plan stratégique VSSE 2021-2024

Alors qu'au milieu des années 2010, à la suite des attentats de Paris et de Bruxelles, la VSSE se concentrait principalement sur la lutte contre le terrorisme, depuis le nouveau Plan stratégique 2021-2024, le service indique que les opérations de renseignement mettent tout autant l'accent sur l'espionnage et l'ingérence. Les opérations de renseignement s'articulent *de facto* autour de deux grands piliers : la lutte contre le terrorisme et l'extrémisme (CTE), d'une part, et la lutte contre l'espionnage et l'ingérence (CI), d'autre part. En fonction de la manifestation concrète des menaces, des membres du personnel sont déployés sur les deux menaces.

La lutte contre l'espionnage et l'ingérence est l'une des huit priorités définies par la VSSE dans son Plan stratégique 2021-2024.

Les objectifs de cette lutte sont décrits par la VSSE comme suit :

- Créer un environnement de travail hostile à l'espionnage et à l'ingérence contre les intérêts et la société belges ;
- Offrir des conseils et de la prévention aux acteurs belges (économiques, académiques, politiques, etc.) contre l'espionnage et l'ingérence ;
- Assurer le suivi de l'espionnage et de l'ingérence contre les institutions internationales sur le territoire belge ;
- Poursuivre la rationalisation de la coopération avec le SGRS dans ce domaine ;
- Renforcer le cadre juridique afin de permettre la lutte contre l'espionnage et l'ingérence.

V.1.2. Note de service VSSE Mandataires politiques

Si des mandataires politiques apparaissent, une procédure spécifique, connue sous le nom de procédure « d'obligation de notification pour les mandataires politiques », est suivie au sein de la VSSE. Cette procédure a été mise à jour en novembre 2023.

Ce n'est que lorsqu'il existe des *informations confirmées ou hautement probables* selon lesquelles un mandataire politique est *consciemment* impliqué dans l'émergence d'une menace que ces informations doivent être communiquées par note au ministre de la Justice et au Premier ministre. Une copie de la note est également transmise au Comité permanent R.
Il n'est donc pas du tout vrai qu'un rapport est établi chaque fois qu'un mandataire politique apparaît dans un dossier. Le ministre, le Premier ministre et le Comité permanent R seront informés uniquement en cas d'implication délibérée dans la menace.

La VSSE considère les fonctions suivantes comme des mandats politiques :

- Bourgmestres ;
- Ministres et secrétaires d'État des six gouvernements et eurocommissaires belges ;
- Membres de la Chambre et du Sénat, des parlements communautaires et régionaux et membres belges du Parlement européen ;
- Présidents de partis politiques (lorsqu'ils sont représentés au Parlement fédéral) ;
- Gouverneurs.

Il convient de noter que ces deux dernières catégories *ne* sont *pas* considérées comme des mandataires politiques par le SGRS (*infra*).

Depuis 2020, selon la VSSE, des mandataires politiques sont régulièrement apparus dans ses dossiers de menace actuels. Lorsque le mandataire politique lui-même est intervenu consciemment en tant qu'acteur, la procédure de notification a toujours été suivie.

L'expérience montre que les mandataires politiques apparaissent principalement dans les dossiers d'« espionnage et d'ingérence ». Mais on a également dénombré des cas individuels de mandataires politiques impliqués dans des dossiers d'extrémisme.

La procédure prévoit en outre la possibilité de donner un briefing de sensibilisation *(awareness)* à un mandataire politique lorsqu'on estime que celui-ci est inconsciemment impliqué dans la survenue d'une menace.

V.1.3. Enquêtes de la VSSE sur les flux financiers

En 2023, la VSSE a mis en place un pool d'experts FININT afin de développer une plus grande expertise en matière d'informations et de techniques financières, et d'améliorer l'échange d'informations avec les institutions financières publiques et privées. Les membres de cette cellule FININT sont formés au traitement des données financières dans le cadre des enquêtes de renseignement et à l'analyse des données financières avec une finalité de renseignement.

L'initiative FININT est née de la nécessité de traiter plus efficacement les informations relatives à la gestion financière d'une cible de la VSSE. Ainsi, la connaissance des renseignements pouvant être demandés au SPF Finances, entre autres, dans le cadre d'une enquête standard, n'était pas toujours claire au sein du service dans le passé.

Le pool d'experts FININT rassemble les connaissances existantes sur le traitement des informations financières, les approfondit et les partage avec ses collègues :
– Informations sur le cadastre (patrimoine) ;
– Informations fiscales ;
– Contact avec l'industrie (Febelfin, Banque Nationale), à l'exclusion des créances ;
– Enquêtes cryptographiques ;
– Contact avec la Cellule de traitement des informations financières (CTIF) ;
– Recherche et développement généraux et amélioration des processus (préparation de vade-mecum, etc.).

Dans la pratique, la cellule FININT existe depuis plus longtemps, mais elle n'a été officiellement reconnue comme pool d'experts qu'en 2023. Cette reconnaissance permet également à ses membres de suivre des formations plus ciblées afin de transmettre ces connaissances à leurs collègues. Les collaborateurs de FININT collaborent également avec les services de police pour pouvoir utiliser, par exemple, des logiciels financiers déjà acquis par les autorités fédérales (lorsque l'enquête le permet).

Le pool d'experts FININT fournit des connaissances de base en matière d'enquêtes financières aux collègues du groupe d'inspecteurs DATA (dont relève FININT) et offre une assistance pour les affaires très complexes, y compris les dossiers cryptographiques.
La VSSE indique que les capacités de FININT seront renforcées à l'avenir. Afin d'être mieux à même de cartographier les flux financiers, des efforts supplémentaires sont déployés pour développer cette spécialité :

- Une coopération encore plus étroite avec des partenaires tels que le SPF Finances, la CTIF, la BNB et d'autres ;
- Développement de méthodes spécifiques pour permettre au service d'appréhender l'utilisation des cryptomonnaies/ cryptoplateformes ;
- Achat de logiciels spécifiques. Ces logiciels sont extrêmement coûteux et doivent être refinancés chaque année. Ils sont dans un même temps nécessaires pour diverses missions du service (non seulement en fonction du suivi de l'ingérence et de l'espionnage, mais aussi en relation avec la prolifération des armes de destruction massive, le contrôle des investissements directs étrangers...).

La VSSE coopère avec d'autres partenaires belges pour surveiller des investissements étrangers spécifiques dans le cadre de la lutte contre la menace d'espionnage et d'ingérence. Dans le contexte des « investissements directs étrangers » (IDE), une méthodologie a notamment été définie réglementairement aux termes de laquelle les investissements d'un certain montant dans certains secteurs de la Belgique sont contrôlés par les services de renseignement et de sécurité. Le Comité de coordination du renseignement et de la sécurité (CCRS) émet un avis dans ces dossiers sur la base de l'apport des services, dont la VSSE.

Le CCRS regroupe les partenaires classiques de la VSSE en matière de sécurité dans la lutte contre l'ingérence financière. Des accords peuvent être conclus sur des thèmes de sécurité essentiels dans ce cadre. En ce qui concerne l'ingérence, il existe également dans ce contexte des plateformes qui s'occupent spécifiquement de la protection du web (activités en ligne), telles que la cellule Social Media Intelligence (Socmint) de la VSSE. En outre, le fonctionnement normal du service CI fournit régulièrement des informations sur les activités d'espionnage économique de certains pays. Les informations pertinentes sont partagées avec les acteurs fédéraux et régionaux.

V.2. SUIVI DE L'INGERENCE PAR LE SGRS

En réponse aux questions du Comité permanent R dans le cadre de cette enquête, le SGRS renvoie au Plan directeur 2023-2027, soumis au Conseil national de sécurité (CNS), et à la « Standing Operating Procedure (SOP) Mandataires politiques ».

Le SGRS n'enquête sur l'ingérence que dans la mesure où celle-ci porte atteinte à l'aspect militaire et aux intérêts de la Défense belge. Cela se produit, selon le service, lorsque la loyauté et l'intégrité des institutions et des entreprises liées à la Défense belge sont compromises ou lorsque des profils de risque au sein de la Défense peuvent être ciblés par des acteurs de la menace.

Le SGRS sensibilise activement ses propres membres du personnel à la détection des tentatives d'influence. Il met également à la disposition du personnel de la Défense et des Affaires étrangères, sur base volontaire, des briefings classifiés sur l'espionnage et l'ingérence, destinés aux titulaires d'une habilitation de sécurité qui se rendront à l'étranger pour des raisons professionnelles ou privées. Un briefing non classifié destiné à un groupe cible plus large est en cours d'élaboration.

L'ingérence, y compris sous la forme de flux financiers, peut faire partie de la guerre hybride. Il est question de guerre hybride lorsque les formes conventionnelles de la guerre sont complétées par une guerre non conventionnelle sous la forme de propagande, de désinformation, de cyberattaques, de sabotage, etc. Selon l'OTAN, la Russie et la Chine en particulier utilisent une telle stratégie de guerre hybride. Le SGRS suit l'influence dans le spectre cybernétique via des collaborations bilatérales avec des partenaires belges et autres.

Dans le cadre de cette stratégie, des actions très opportunistes peuvent être menées, notamment en concentrant l'influence sur des phénomènes susceptibles de perturber la

société démocratique belge. L'ingérence peut alors viser non seulement des membres de la Défense, mais aussi des chercheurs scientifiques, des membres de groupes de réflexion, des fonctionnaires, des personnalités issues du monde des affaires, des diplomates, les représentants d'organisations de la société civile et, bien entendu, des personnalités politiques et leurs proches collaborateurs.

On peut partir du principe que les services de renseignement étrangers cernent bien le processus de prise de décision démocratique en Belgique et qu'ils cibleront donc tout acteur potentiel qu'ils jugeront vulnérable à une approche.

Le SGRS précise que le service ne considère pas comme sa mission légale de mener des enquêtes ciblées sur des partis politiques, des institutions ou des personnalités. Lorsqu'une opération de renseignement révèle un lien avec le milieu politique, les autorités sont informées selon la procédure décrite dans la SOP Mandataires politiques. Le service souligne également qu'aucun indice de financement suspect n'a été relevé jusqu'à présent.

Le SGRS estime que si le suivi (du financement) des partis politiques devait faire partie de ses missions, une modification de la loi s'imposerait.

V.2.1. Plan directeur 2023-2027

Dans le Plan directeur du SGRS couvrant la période 2023-2027, on remarque que le service n'établit pas de distinction manifeste entre les menaces d'espionnage et d'ingérence. Selon le service, il est question d'un chevauchement thématique entre les deux menaces dans la pratique.

Pour comprendre la méthode utilisée par le SGRS pour assurer le suivi de la menace d'ingérence, il est nécessaire d'expliquer certains termes utilisés par le service.
Le SGRS établit une distinction entre ce que le service appelle le suivi « proactif » et le suivi « réactif ».

Le suivi « proactif » suppose que le SGRS mobilise son personnel et ses ressources pour détecter à un stade précoce les menaces qui pèsent sur la Défense. Il s'agit de mettre en place des opérations visant à identifier des groupes et des individus représentant une menace, à détecter l'implication éventuelle de membres de la Défense et à recruter des sources dans le milieu ciblé. Cette collecte et cette analyse permanentes visent à garantir une compréhension globale du milieu dans lequel la menace évolue et permettent des actions rapides et ciblées.

Le suivi « réactif » signifie que le personnel et les ressources ne sont déployés que lorsque le service entre en possession d'informations indiquant une menace pour la Défense. Le SGRS s'appuie au préalable sur les informations d'autres services de renseignement et de sécurité pour maintenir un certain niveau d'information sur les groupes actifs dans le cadre du phénomène bien défini.

En ce qui concerne l'espionnage et l'ingérence, certaines puissances étrangères et les activités de leurs services de renseignement font l'objet d'un suivi proactif, tandis que d'autres le sont

de manière réactive. Au cours de la période 2023-2025, le SGRS commencera à suivre de manière proactive les activités d'un certain nombre de services étrangers supplémentaires après l'allocation de moyens plus importants.

Le SGRS a également répondu que le Cyber Command n'effectue pas de recherches spécifiques d'influence par le biais du financement d'institutions politiques, mais qu'il réalise un suivi actif des médias sociaux par le biais de ses *Agile Task Force Information Operation*s (ATFIO), une forme permanente de surveillance des courants sur les médias sociaux, comme il l'a fait de manière ad hoc dans la période précédant les élections de 2019 avec la Joint Information Task Force.

V.2.2. Procédure Mandataires politiques

La SOP « Mandataires politiques », approuvée par la ministre de la Défense en décembre 2021 et entrée en vigueur le 1er janvier 2022, définit la procédure à suivre lorsque des mandataires politiques sont mentionnés dans des enquêtes de renseignement menées par le service, ou lorsqu'ils sont nommés dans des documents établis par le service. Elle définit également ce que l'on entend par mandataires politiques :

- ministres du gouvernement fédéral et des gouvernements régionaux ;
- membres du Parlement fédéral et des parlements régionaux, Parlement européen, membres belges de la Commission européenne, éventuellement président belge du Conseil européen.

Dans la SOP, il est également mentionné de manière explicite quelles sont les fonctions politiques qui ne relèvent pas de la définition du mandataire politique :

- présidents de parti (pour autant qu'ils soient pas députés ou membres d'un gouvernement) ;
- membres de la famille royale ;
- ministres d'Etat ;
- mandataires locaux ;
- gouverneurs de province et membres des conseils provinciaux ;
- anciens mandataires.

A noter que cette énumération est moins large que celle de la VSSE, pour laquelle les bourgmestres, les gouverneurs et les présidents de parti (des partis siégeant au Parlement fédéral, mais des présidents n'y siégeant pas eux-mêmes) sont également considérés comme des mandataires politiques.

Dans le cas où un mandataire politique, tel que défini dans la SOP, est impliqué – en tant que cible potentielle ou auteur présumé – dans une menace relevant des missions légales du SGRS, une note classifiée est adressée au ministre de la Défense et au Premier ministre, avec copie au Comité permanent R. Cette note comprend une description de l'implication du mandataire politique et une évaluation des conséquences possibles de la menace.

Il faut noter que la SOP Mandataires politiques diffère également de la Note de service VSSE Mandataires politiques en ce sens que le SGRS informe également son ministre, le Premier ministre et le Comité permanent R lorsqu'un mandataire politique est impliqué en tant que personne lésée, victime ou auteur présumé. Au sein de la VSSE, les notifications ne sont effectuées que lorsque le mandataire politique est *consciemment* impliqué dans l'émergence de la menace.

V.2.3 Ingérence financière

Le SGRS ne dispose pas d'un pool d'experts en renseignement financier, mais a des contacts avec, entre autres, la Cellule de traitement des informations financières.

VI. CONCLUSIONS ET RECOMMANDATIONS

VI.1. CONCLUSIONS

La VSSE et le SGRS sont tous deux conscients de la menace d'ingérence et mènent activement des enquêtes de renseignement pour y remédier. Ces enquêtes sont axées sur les menaces, à partir des activités des agents d'influence étrangers, et ne se concentrent donc pas sur les cibles potentielles de cette influence, parmi lesquelles les personnalités et les partis ou organisations politiques.

Les deux services ont mis en place une procédure de notification lorsque des mandataires politiques sont associés à une menace.

Tant la VSSE que le SGRS considèrent le financement clandestin comme une forme d'ingérence parmi d'autres et ne relèvent pas d'éléments indiquant que cette forme d'ingérence constitue un problème majeur ou croissant pour le milieu politique en Belgique. Néanmoins, la VSSE développe l'expertise nécessaire à la conduite d'enquêtes financières. Cette expertise est utile non seulement pour les enquêtes de renseignement concernant la menace d'ingérence, mais aussi pour d'autres menaces pour lesquelles le service est légalement compétent.

Pour assurer le suivi des menaces d'ingérence et autres dans le cadre des élections de 2024, les services du CCRS ont mis en place une « task force élections » comme en 2019. Y sont discutées les informations provenant des menaces liées aux élections ainsi que les mesures de suivi et de prévention.

VI.2. RECOMMANDATIONS

1/ Le Comité permanent R recommande au Conseil national de sécurité et aux deux services de renseignement de mettre en œuvre l'obligation énoncée à l'article 20 § 4 L.R&S, respectivement d'établir une directive et de conclure un accord de coopération.

2/ Le Comité permanent R recommande au ministre de la Justice d'adopter, conjointement avec la ministre de la Défense, une circulaire commune établissant les directives applicables aux services de renseignement et de sécurité concernant l'application de la disposition de l'article 19, alinéa 1er, de la loi organique des services de renseignement, qui dispose que : « *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.* »

3/ Le Comité permanent R recommande aux deux services de renseignement de poursuivre et, si possible, d'intensifier, de systématiser et de coordonner leurs efforts de sensibilisation aux menaces d'ingérence et d'espionnage à l'égard de cibles potentielles, y compris les mandataires politiques.

4/ Le Comité permanent R recommande que les deux services de renseignement coopèrent pour développer leur expertise en matière de renseignement financier (*'financial intelligence'*) et pour mener des enquêtes financières.

5/Le Comité permanent R recommande aux deux services de renseignement d'harmoniser leur procédure de notification concernant les mandataires politiques.

6/ Actuellement, la possibilité de sensibiliser les mandataires politiques *(awareness)* est déjà prévue de manière réactive dans la « procédure mandataires politiques » des services, ce que le Comité permanent R considère comme une bonne pratique.
Il est recommandé que les services de renseignement donnent des briefings de sécurité sur l'espionnage et l'ingérence aux mandataires politiques, tels que définis dans la « procédure mandataires politiques », sur une base préventive, systématique et régulière. Un briefing de sécurité annuel permettrait à ces mandataires politiques de prendre connaissance des renseignements du niveau de classification 'Restreint', tel que prévu dans la version adaptée de la L.C&HS du 11 décembre 1998.

7/ Le Comité permanent R demande que les recommandations énoncées ci-dessus soient mises en œuvre dans un délai de six mois maximum.