RAPPORT ANNUEL 2022

Service Général du Renseignement et de la Sécurité
SGRS - ADIV
Algemene Dienst Inlichting en Veiligheid

Quaero et tego

Décryptage
du Renseignement, de la Sécurité et de la Cyber défense militaire belge

DEFENSIE
LA DÉFENSE

.be

SGRS

Service Général du
Renseignement et
de la Sécurité

TABLE DES MATIÈRES

4 Le Monde change mais notre mission reste identique
6 Naissance du Cyber Command
7 Le SGRS dans le giron de la Défense
8 Notre Mission, notre Vision et nos Valeurs
9 Notre Histoire
11 Notre Structure
11 La principale loi qui nous régit
12 Nos engagements
14 Notre Direction Renseignement est la première et la dernière défense avant le chaos
16 Tout commence et finit avec notre Direction Sécurité
18 Notre Cyber Défense est la première et la dernière frontière virtuelle du champ de bataille
20 Notre Direction « Plans & Policy » assure la planification, la coopération et l'évaluation des défis quotidiens
22 Notre Direction Support assure la stratégie et les ambitions du Service
24 Notre Service des Attachés de Défense
25 Nos chiffres
26 Notre recrutement, c'est innover dans le Capital humain
27 Notre collaboration avec la Sûreté de l'Etat : le Plan Stratégique National du Renseignement
29 Nos partenaires
30 Notre rétrospective dans les médias
32 Nos perspectives d'aujourd'hui sur les menaces de demain
35 Nous faisons le travail
36 Notre petit lexique

Editeur responsable : Vice-Amiral Wim Robberecht
Quartier Reine Elisabeth – rue d'Evere 1 à 1140 Evere

Photographies : Patrick Bouillon, DG StratCom et personnel SGRS
Graphisme : 2SeeDesign

Vice-Amiral Wim Robberecht © Patrick Bouillon

LE MONDE CHANGE, MAIS NOTRE MISSION RESTE IDENTIQUE

Quaero et Tego est notre devise ; **Protéger** notre pays, nos entreprises et nos expatriés par nos **Renseignements** est notre mission première ; **Conseiller** judicieusement les autorités est notre devoir envers notre pays, la société et nos concitoyens.

Il ne fait aucun doute que l'année 2022 restera dans les mémoires du SGRS comme l'année du changement.

Le 19 octobre dernier, le SGRS s'est doté d'une nouvelle structure avec, comme intention principale de pouvoir mieux appréhender les défis actuels et futurs dans le domaine du Renseignement, de la Sécurité mais également du Cyberespace. La finalité de notre Service demeure inchangée: protéger notre pays et nos concitoyens, tant sur le sol national qu'à l'étranger, contre toutes les formes de menaces possibles et envisageables, mais également formuler le meilleur conseil possible à nos autorités, à nos partenaires et à nos industries.

Cette adaptation était rendue nécessaire par les mutations profondes en cours dans le monde et en Belgique.

Une évidence interpelle en effet toutes les personnes intéressées par le Renseignement, la Sécurité ou le traitement de l'information de manière générale : le monde d'aujourd'hui est fondamentalement différent de celui du début du XXI siècle. Les mécanismes qui étaient en usage, il y a à peine 22 ans, sont déjà obsolètes face aux menaces actuelles. Notre monde est devenu numérique - dans toutes les strates de la société - et nous impose de traiter une quantité d'informations de plus en plus importante, à une vitesse sans cesse croissante.

Si le monde change, l'Information reste bel et bien la matière première essentielle au fonctionnement des services de Renseignement et de Sécurité.

NOUS TRAVAILLONS POUR VOUS, POUR NOTRE PAYS, POUR LA PAIX

En parallèle, le monde émerge de la pandémie mondiale, panse ses plaies et découvre les conséquences d'une nouvelle réalité sociétale. De profondes modifications ont eu lieu et impactent nos comportements et habitudes dans quasi toutes les facettes de nos vies et de notre société.

Il était donc impératif que le SGRS tire les bonnes leçons de ces mutations et s'adapte en conséquence dans ses domaines de compétence. De ces mutations naissent en effet de nouvelles menaces, qui deviennent des sujets majeurs de préoccupation au sein de la population. Parmi ces préoccupations, nous pouvons citer un sentiment d'insécurité croissant dû à une poussée des extrêmes et une augmentation des fraudes à l'encontre des internautes dans le cyberespace.

Chacun d'entre nous doit être conscient que les menaces suivent le cycle de mutation du monde et s'adaptent perpétuellement aux nouvelles réalités de nos vies quotidiennes. Le sentiment d'instabilité latente et l'impression d'une dégradation sociétale belge irréversible offrent aux personnes mal intentionnées des conditions idéales pour élargir leur terrain de jeu et exploiter cette situation, d'autant plus que la manipulation et la désinformation sont devenues monnaie courante. En tant que Service nous participons à l'information de nos concitoyens face à ces menaces et, avec l'aide de nos partenaires, nous tentons d'éradiquer ou de minimiser l'impact de ces fléaux.

Au moment d'écrire ces lignes nous faisons le constat que les activités d'espionnage et d'ingérence étrangère ont atteint des niveaux qui n'avaient plus été atteints depuis la guerre froide. Les principales menaces qui pèsent sur la sécurité nationale sont, outre cette ingérence, l'extrémisme violent, le terrorisme et les activités cyber malveillantes. A cela s'ajoute le retour de la guerre aux confins de l'Europe. D'autres conflits plus lointains font peser un impact sur notre modèle sociétal. Force est de constater que le rythme des menaces ne fait que s'accroître ; leurs effets touchent notre population, de près ou de loin. Au final, ces menaces font peser un danger direct sur notre régime démocratique.

En tant que Chef, je suis particulièrement fier des membres de mon personnel, militaires et civils. Souvent acteurs de l'ombre, ils travaillent sans relâche et dans des conditions parfois très difficiles pour que notre pays soit protégé le mieux possible contre les menaces qui pèsent sur la sécurité nationale, nos concitoyens – ici ou à l'étranger – ainsi que sur les secteurs vulnérables et critiques de l'économie belge.

Avec nos partenaires nationaux et acteurs de la sécurité, nous sommes les yeux et les oreilles de notre Nation. Nous recherchons ce que nos adversaires veulent garder secret. Nous agissons partout où ils se réfugient, le plus souvent dans l'ombre et avec un maximum de discrétion. Nous enquêtons sur les puissances hostiles afin d'anticiper les nouvelles menaces et nous veillons à la sécurité de nos secrets, de nos opérations militaires et de nos connaissances.

Nous conseillons nos dirigeants politiques et militaires afin qu'ils puissent faire les meilleurs choix, de façon indépendante et souveraine, pour protéger au mieux notre pays et ses concitoyens. Nous opérons partout dans le monde où nos intérêts le demandent. Car aujourd'hui les menaces à l'encontre de notre société sont devenues encore plus complexes, imprévisibles et multiples.

Nous sommes présents en appui des opérations militaires, dans la lutte contre l'espionnage et l'ingérence, la cyber sécurité, la lutte antiterroriste, la lutte contre les extrémismes, la protection de nos ressortissants, la lutte contre la prolifération d'armes de destruction massive, la lutte contre les organisations sectaires ou criminelles ainsi que dans les domaines de la protection du potentiel économique et scientifique et des infrastructures vitales.

Nous travaillons pour vous, pour notre pays et pour la Paix.

NAISSANCE DU CYBER COMMAND

LE CYBERESPACE EST DEVENU UN NOUVEAU CHAMP DE BATAILLE

Le 19 octobre 2022, nous avons officiellement lancé le Cyber Command lors d'une cérémonie d'investiture en présence de nombreux partenaires et journalistes.

Le Cyber Command est donc devenu une réalité, non seulement au sein de la communauté militaire, de la communauté du renseignement et de la sécurité mais aussi vis-à-vis de la société civile, du monde académique et de l'industrie.

Et conformément aux orientations politiques de notre Ministre de la Défense, le Cyber Command jouera un rôle sociétal de plus en plus important, non seulement au sein du microcosme régalien de la cyber sécurité mais aussi vis-à-vis de la société en général. L'acquisition de capacités « duales » correspond à cette volonté de nous déployer aussi bien en milieu militaire que civil.

GMJ Van Strythem

Ce Cyber Command est appelé à grandir tout en restant dans le giron de la famille du renseignement et de la sécurité dont elle partage les missions mais aussi le cadre légal. Pour permettre au Cyber Command de croître, le défi du personnel est naturellement notre première préoccupation. Nous ne manquons pas d'atouts, que ce soit nos trajets de formation, notre spécificité militaire ou encore la diversité de nos missions. Mais pour attirer de possibles candidats, nous devons trouver un équilibre entre une communication ouverte et le respect de nos impératifs de sécurité.

Outre la communication, la clé de la réussite du Cyber Command se situe dans notre capacité à établir des partenariats sur le long terme avec nos partenaires opérationnels mais aussi avec les acteurs de la société civile. Ces partenariats sont au centre de notre projet et ils prennent forme avec le milieu des entreprises, du monde académique et de la recherche, sans oublier le monde associatif et de la formation.

Ces partenariats sont d'une importance stratégique pour plusieurs raisons. Tout d'abord ils nous permettront de conserver et de développer l'expertise nécessaire afin de faire face à des menaces de plus en plus sophistiquées dans un environnement en perpétuelle évolution. Mais ils nous permettront aussi d'anticiper nos besoins futurs car il nous est indispensable d'établir une vision à long terme en adéquation avec la société de demain. Enfin, ils concrétisent des possibilités de recrutement en constituant des relais indispensables avec le monde associatif dans des milieux qui ne sont pas familiers avec la Défense.

C'est avec une grande fierté que je continuerai à m'engager et à mettre les compétences de mon personnel au service du développement du Cyber Command en une nouvelle Composante Cyber à la Défense. Le défi est de taille, tant au niveau du personnel que des missions actuelles et futures. Mais je suis persuadé que nous disposons de suffisamment d'atouts pour les relever tous ensemble.

LE SGRS DANS LE GIRON DE LA DÉFENSE

Vice-amiral Wim Robberecht,
Chef du SGRS

Adjudant-major Frédéric Charlot,
l'Adjudant de Corps

1er Caporal-chef Bruno Wilmart,
le Caporal de Corps

Le Service Général du Renseignement et de la Sécurité se trouve dans le giron de la Défense belge. Il est le service belge de référence en matière de **renseignement extérieur** et de **renseignement de défense**. Ses membres sont majoritairement militaires, bien qu'il y ait dans ses rangs de plus en plus de civils.

En égard à son appartenance militaire, certaines fonctions emblématiques sont exercées en son sein sous la dénomination de Chef de Corps, d'Adjudant de Corps et de Caporal de Corps.

Leurs fonctions sont principalement axées sur la réglementation interne du service, la discipline et le bien-être du personnel dans son ensemble.

L'Adjudant de Corps et le Caporal de Corps sont également responsables de l'organisation et de l'exécution des traditions militaires et des visites officielles au sein de l'organisation.

Les fêtes militaires traditionnelles sont :

07 Avril
Journée des Vétérans

21 Juillet
La Fête nationale

11 Novembre
L'Armistice

15 Novembre
La fête du Roi

© SFRS

MISSION

QUAERO ET TEGO
JE CHERCHE ET JE PROTÈGE

Le SGRS est le service de renseignement et de sécurité militaire belge.

Il a pour mission de rechercher, d'analyser et de traiter le **renseignement** relatif à toute activité qui pourrait menacer l'intégrité du territoire national ou la population, les plans de défense militaires, le potentiel scientifique et économique lié au secteur Défense, les missions des Forces armées et la sécurité des ressortissants belges à l'étranger ainsi que le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge.

Il veille au maintien de la **sécurité** militaire du personnel de la Défense et des installations militaires, armes, munitions, documents et systèmes informatiques, et protège le secret y attachant.

Le SGRS a la tâche d'effectuer des enquêtes et des vérifications de sécurité et de délivrer des habilitations, des avis et des attestations de sécurité.

Dans le cadre de l'exercice de ses missions, le SGRS fournit, dans un contexte national et international, du renseignement aux autorités politiques et militaires afin de les aider à la prise de décision.

VISION

SAVOIR ET FAIRE SAVOIR

Le SGRS contribue à protéger les intérêts de la Nation, la Défense et la population grâce à une **approche intégrée** de la sécurité alliant les dimensions Renseignement, Contre-Ingérence, Sécurité et Cyber, tant sur le territoire national qu'à l'étranger.

Il est le service belge de référence en matière de **renseignement extérieur** et de **renseignement de défense**.

Il participe avec ses partenaires nationaux au maintien et au renforcement de la **sécurité intérieure.**

VALEURS

NOS 10 COMMANDEMENTS

1. Nous cherchons et trouvons ce qui échappe à d'autres
2. Nous avons confiance en nous et en chacun
3. Nous avons les bonnes personnes au bon endroit
4. Nous sommes unis
5. Nous travaillons de façon intelligente et sans relâche
6. Nous apportons la bonne information, à la bonne personne, de la bonne façon, au bon moment
7. Nous regardons vers l'avenir
8. Nous entretenons d'excellentes relations
9. Nous saisissons la culture de renseignement
10. Nous travaillons dans l'ombre

Kathleen Van Acker

NOTRE HISTOIRE

Après l'indépendance de la Belgique en 1830, l'une des premières actions du gouvernement provisoire fut de lever une armée. Comme cette armée ne disposait aucun département chargé de la collecte de l'information et de l'analyse du renseignement, en 1831, on créa à cette fin la « Police militaire du Département de la Guerre ». Ce nouveau corps travaillait de manière non régulière avec des informateurs supervisés par des officiers et était chargé principalement de détecter et de surveiller les orangistes et les éléments républicains au sein de l'Armée.

L'arrêté royal du 26 juin 1910 promulgua un Etat-major général de l'Armée. Ce dernier était composé de quatre bureaux, dont le 2e bureau en charge du Renseignement.

Au début de l'année 1911, le 2e Bureau « Renseignement » mit en place un service de surveillance et de renseignements aux frontières, où furent employés 300 gendarmes locaux, douaniers et gardes forestiers.

La Sûreté militaire belge fut quant à elle créée le 1er avril 1915. Son rôle principal consistait à contrecarrer les activités d'espionnage de l'ennemi. Pour ce faire, le Service disposait de pouvoirs étendus dont l'éloignement et l'internement de délinquants et de personnes soupçonnées de collaboration et d'espionnage ; le pouvoir d'effectuer des fouilles (corporelles), des recherches et la confiscation d'armes et d'empêcher les réunions subversives et d'intercepter les correspondances privées.

Après l'armistice, le Service fut également chargé de la sécurité des troupes belges participant à l'occupation de la Ruhr.

En 1929, le Service fut dissous en raison d'un scandale lié à la falsification de plans militaires contre l'Allemagne. Ces plans militaires en tombant entre les mains de la presse néerlandaise provoquèrent un scandale international appelé « Le faux d'Utrecht ».

En 1937, le Service ressuscita de ses cendres dans le plus grand secret pour faire face à l'espionnage allemand grandissant.

Après la campagne de Belgique de 1940, le Gouvernement belge en exil à Londres souhaita rétablir au plus vite les liens avec la patrie occupée. Deux services de renseignement belges coexistaient et travaillaient chacun depuis Londres. Par manque de clarté sur les compétences attribuées aux deux Services par le Gouvernement, une querelle d'autorités éclata nuisant non seulement aux

relations entre les deux services mais aussi à la coopération avec les services de renseignement britanniques. Le problème persista jusqu'en octobre 1942, date à laquelle un accord définissant les compétences des deux services fut signé par les nouveaux ministres de la Défense nationale et de la Justice.

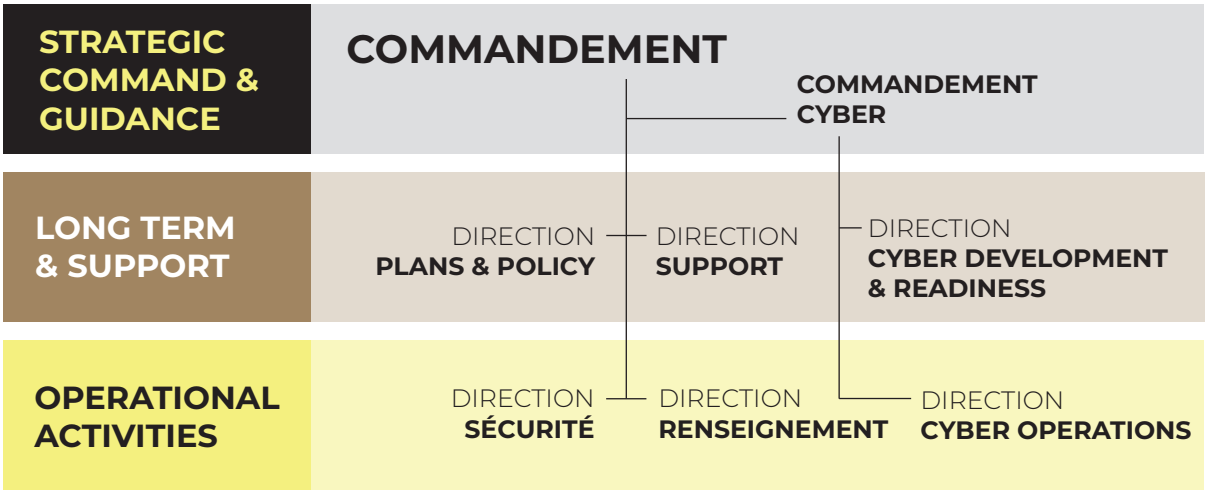
Après la Seconde Guerre mondiale, on créa, à côté du Service de Renseignement militaire, un service spécifique appelé « Service de Documentation de Renseignement et d'Action VIII » (SDRA VIII) . Son objectif premier était, en cas de conflit, l'évacuation du Gouvernement belge vers un lieu sûr et le maintien de contacts avec la mère patrie. Dans ce cadre, le SGRA VIII collectait des renseignements, se préparait à des tâches d'évasion y compris l'exfiltration de pilotes abattus ou d'agents découverts par l'ennemi, s'entraînait aux actions de sabotage d'objectifs militaires, organisait une structure pour résister à l'adversaire et s'impliquait dans la contre-information.

Le 3 août 1990, à la suite d'une enquête parlementaire sur le terrorisme en Italie, le Premier ministre Giulio Andreotti dut reconnaitre l'existence du réseau italien « Stay-behind ». Ce dernier faisait partie de l'opération « Gladio » qui couvrait toute l'Europe et qui consistait en la création par chaque pays européen d'un réseau « Stay-behind » dans le but de résister à l'ennemi sur le territoire national.

Le ministre belge de la Défense de l'époque, Monsieur Guy Coëme, dut s'expliquer sur le sujet lors d'une réunion internationale de ces réseaux qui se déroula à Bruxelles fin octobre 1990. Le même jour, le ministre convoqua le Chef du Service de Renseignement militaire et le Chef du SDRA VIII afin d'obtenir de plus amples informations.

Alors que personne n'avait jamais entendu parler de Gladio avant novembre 1990 et que le réseau belge « Stay-behind » exerçait ses activités en toute indépendance, le SDRA VIII se retrouva au cœur d'une tempête médiatique et de théories du complot reliant le réseau secret belge aux attentats sanglants perpétrés en Belgique dans les années 1980, notamment par les dossiers des tueurs du Brabant ou les Cellules Communistes Combattantes. Le 20 décembre 1990, le Gouvernement décida de dissoudre le réseau clandestin et d'ouvrir une enquête parlementaire. Le lien avec d'éventuels attentats terroristes ne fut jamais prouvé et l'identité des agents ne fut jamais révélée.

NOTRE STRUCTURE



LA PRINCIPALE LOI QUI NOUS RÉGIT

Les missions du SGRS sont décrites dans l'article 11 de la loi du 30 novembre 1998 réglementant les services de renseignement et de sécurité. Pour que ces missions puissent être menées à bien, le législateur a prévu dans la loi différentes méthodes de collecte de données dont notamment les « méthodes de recueil de données ». Les différentes méthodes de collecte sont assorties de conditions et d'un contrôle juridique spécifique, afin d'établir un équilibre entre les impératifs de sécurité nationale et les principes et les valeurs d'un État de droit démocratique. Lors de l'utilisation de ces méthodes, les responsables opérationnels du SGRS accordent beaucoup d'attention au respect des conditions légales.

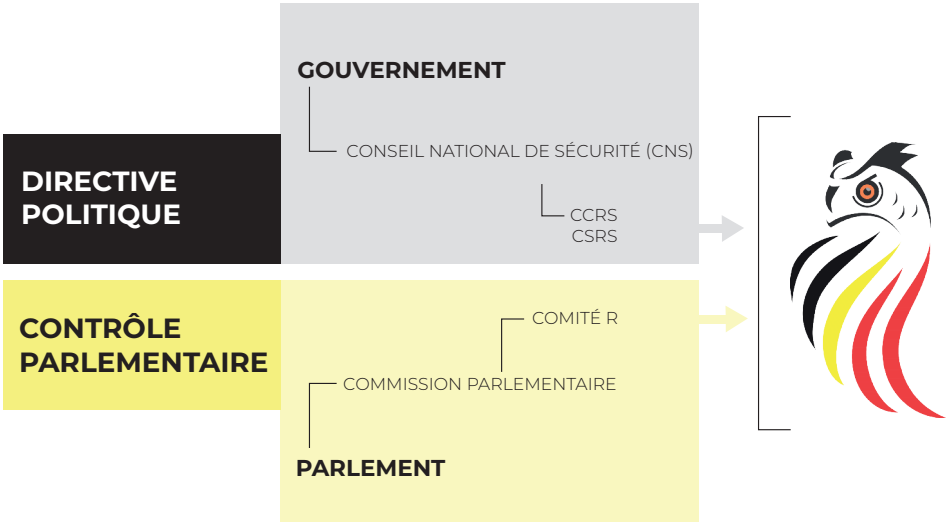
L'émergence de nouvelles menaces et le développement de nouvelles technologies entraînent toujours un risque résiduel d'agir illégalement (non intentionnellement). Un contrôle indépendant de ce risque résiduel et des actions quotidiennes du SGRS est garanti avant, pendant et après ces actions par le Comité permanent de contrôle des services de renseignement et de sécurité et la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité.

En partie sur la base des recommandations de la Commission d'enquête parlementaire « Attentats terroristes du 22 mars 2016 », des modifications ont été apportées à la loi du 30 novembre 1998 par le législateur en 2022. Pour les agents des services de renseignement et de sécurité, il a été prévu de donner la possibilité de s'infiltrer dans les mondes virtuel et réel et d'élargir les possibilités de commettre des infractions, avec les mesures de contrôle correspondantes. En outre, en ce qui concerne les sources humaines, la possibilité est donnée de commettre des infractions, mais sous conditions très strictes. Enfin et plus particulièrement pour le SGRS, une compétence supplémentaire a été ajoutée en cas de crise nationale de cybersécurité. La mise en œuvre de ces nouvelles compétences légales et les recommandations du Comité permanent de surveillance suite à l'affaire « Jürgen Conings » sont considérées comme prioritaires, bien que le travail opérationnel quotidien du SGRS se poursuit.

Au cours de l'année 2022, les premières initiatives ont été entamées pour préparer également des propositions de modification à la loi relative à la classification et aux habilitations, attestations et avis de sécurité (loi du 11 décembre 1998) et à la loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (loi du 30 juillet 2018).

NOS ENGAGEMENTS

L'engagement politique :



Le Conseil National de Sécurité établit la politique générale du renseignement et de la sécurité, en assure la coordination et détermine les priorités des services de renseignement et de la sécurité. Le Conseil est également compétent pour la coordination de la lutte contre le financement du terrorisme et la prolifération des armes de destruction massive. Le Conseil définit en outre la politique en matière de protection des informations sensibles. Il est présidé par le Premier Ministre et comprend les Ministres ayant dans leurs attributions la Justice, la Défense nationale, l'Intérieur et les Affaires étrangères. Ainsi que les Vice-Premiers Ministres qui n'ont pas ces matières dans leurs compétences.

Les Membres du Gouvernement qui ne font pas partie du Conseil peuvent être invités par le Premier Ministre à y participer pour l'examen des dossiers qui les concernent particulièrement. Lorsque leur présence est requise par l'ordre du jour, seront également invités :

Le Chef du Service Général du Renseignement et de la Sécurité,
L'Administrateur général de la Sûreté de l'Etat,
Le Commissaire général de la Police fédérale,
Le Directeur de l'Organe de coordination pour l'analyse de la menace,
Le Président du Comité de direction du Service public fédéral Intérieur,
Un représentant du Collège des procureurs généraux,
Le Procureur fédéral.

Le Comité de Coordination du Renseignement et de la Sécurité (CCRS) est composé des dirigeants des autorités et des services concernés par la politique du renseignement et de la sécurité. Il élabore des propositions stratégiques, assure le suivi de la mise en œuvre des priorités établies par le Conseil national de sécurité et garantit une collaboration efficace et un échange d'informations entre les services et les autorités.

Le Comité Stratégique du Renseignement et de la Sécurité (CSRS) se charge tant de la préparation que de la mise en œuvre de la politique et est constitué des représentants des membres du Conseil national de sécurité et du président du Comité de coordination. Le secrétariat du Comité stratégique est assuré par le SPF Chancellerie du Premier Ministre.

Les contrôles :

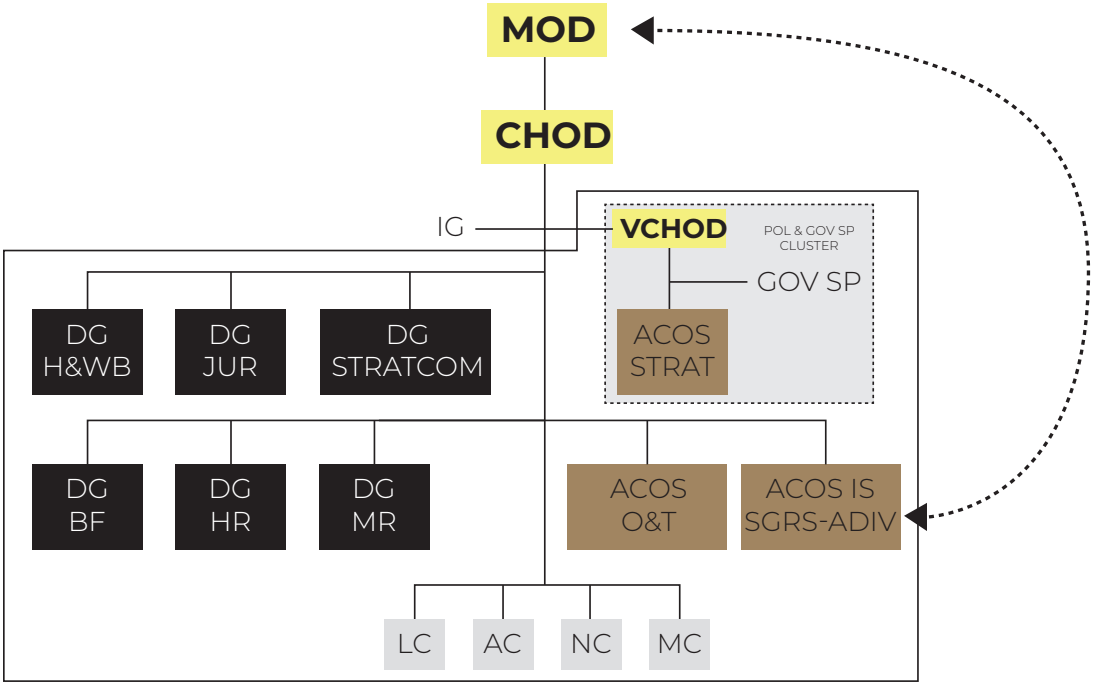
Le Comité permanent R est chargé de contrôler les activités et le fonctionnement de la Sûreté de l'État et du Service Général du Renseignement et de la Sécurité. Le contrôle porte aussi bien sur la légitimité (le contrôle du respect des lois qui réglementent la matière) que sur l'efficacité et la coordination des services de renseignement (la coordination mutuelle de leur fonctionnement).

Les commissions parlementaires et le Parlement peuvent non seulement, lors de leurs séances respectives demander des explications aux ministres et / ou poser des questions spécifiques, mais aussi demander la convocation d'un ou plusieurs membres d'un service de renseignement et de sécurité. Toutefois, si les questions et la convocation d'une personne font aussi partie intégrante du contrôle démocratique, pour des raisons de classification du contenu des réponses, le huis-clos peut être demandé.

L'engagement militaire :

L'histoire du SGRS est liée aux opérations militaires. Aujourd'hui encore, une partie non négligeable de son travail est destinée à la Défense belge et en particulier aux opérations militaires. Ce lien avec la Défense se remarque par le fait que la gestion de son personnel, de son infrastructure et de son budget est assurée par des directions générales militaires. C'est également la raison pour laquelle le SGRS dépend hiérarchiquement du Chef de la Défense sous le nom d'ACOS IS (sous-département de la Défense Intelligence Service).

Au cours de ces dernières années, le travail du SGRS s'est élargi et touche également des domaines civils-militaires spécifiques comme la lutte contre le terrorisme ou l'extrémisme. C'est la raison pour laquelle le SGRS dépend directement du ministre de la Défense.



DIRECTION RENSEIGNEMENT

La Direction Renseignement fournit des analyses de haute qualité sur base de différents types d'informations et d'origines pour conseiller notre Gouvernement et nos partenaires.

La Direction du Renseignement est chargée, d'une part, de la collecte et de l'exploitation d'informations et, d'autre part, de leur transformation sous forme de renseignements. Les informations sont soit collectées par des agents, soit par du matériel technique spécifique appartenant au Pilier Collecte. Ensuite, elles sont transmises aux analystes du Pilier Exploitation pour y être traitées. Il existe plusieurs types d'approches de traitement des informations en fonction du produit final souhaité. L'analyste peut mettre davantage l'accent sur l'axe militaire, sécuritaire, politique, économique, social… La richesse de notre Renseignement réside précisément dans la possibilité d'offrir différents rapports finaux en fonction des besoins du demandeur.

Le Pilier Collecte

Le Pilier « Collecte » de la Direction du Renseignement se compose d'un certain nombre de services différents qui rassemblent des informations provenant soit des agents de terrain, soit des techniciens utilisant du matériel spécifique, soit des deux à la fois. Ces services sont appelés dans le jargon « des services de collecte ».

Lorsqu'on parle de « source humaine » ou de « contact » en langage Renseignement, on désigne une personne qui fournit des informations. Elle peut résider soit à l'étranger, tant en zone opérationnelle militaire que dans un pays cible, soit sur le territoire national. Le Service chargé des sources et contacts nationaux intervient aussi dans les enquêtes liées à une menace T.E.S.S.OC. Ces enquêtes dites de contre-ingérence sont liées à une menace dans le domaine du Terrorisme, de l'extrémisme de gauche comme de droite, de l'Espionnage, du Sabotage, de la Subversion et de la criminalité organisée (« Organised Crime ») dirigée contre les intérêts du pays et en particulier de la Défense.

NOTRE DIRECTION RENSEIGNEMENT EST LA PREMIÈRE ET LA DERNIÈRE DÉFENSE AVANT LE CHAOS

Lorsqu'on parle de « matériel », on désigne les signaux électromagnétiques comme l'écoute électronique ou les informations géographiques comme les images satellitaires. On désigne également les informations provenant de sources dites « ouvertes » telles que la presse écrite, la presse radiophonique ou télévisuelle et toutes celles disponibles sur internet.

L'évolution du Renseignement demande aujourd'hui de regrouper les moyens humains et matériels dans un souci de performance. Lorsqu'on parle d'une opération de filature physique par exemple, on utilise un ou plusieurs agents de terrain et divers moyens techniques appropriés pour pallier à toute éventualité ou déjouer les contre-mesures mises en place par la personne surveillée.

> **Le Pilier Collecte dispose également d'un service jouant le rôle d'entrée et de sortie de tout le flux d'informations en provenance de l'OTAN afin de garantir la coopération militaire entre Alliés.**

Le Pilier Exploitation

Le Pilier Exploitation de la Direction du Renseignement se compose de différentes Plateformes organisées par zones géographiques ou par thèmes dont l'objectif final est de fournir des produits de renseignement sur différents sujets. Par exemple sur les menaces pesant sur une opération militaire à l'étranger, l'extrémisme dans une région donnée, la situation politique en Ukraine ou sur des sujets reliés à une analyse prévisionnelle comme la sécurité dans l'Est du Congo.

Les Plateformes sont composées d'analystes spécialisés, d'une part, en espionnage et, d'autre part, en contre-ingérence. Les principales zones géographiques couvertes sont l'Europe, l'Afrique, l'Asie et le Moyen-Orient. Les principaux thèmes sont le terrorisme, l'extrémisme, l'espionnage, le sabotage, la subversion et la criminalité organisée (T.E.S.S.OC.).

> **Afin d'assurer la qualité des produits finis, le Pilier Exploitation dispose d'un service de « Quality control ».**

Le Centre de Coordination

La Direction du Renseignement dispose d'un La Direction du Renseignement dispose d'un Centre de Coordination qui se compose de représentants des piliers Collecte et Exploitation et de la Direction Cyber Operations.

Le Centre de Coordination distribue toutes les informations ou requêtes entrantes vers les personnes concernées et toutes les informations ou requêtes sortantes vers les clients ou services partenaires appropriés.

Le centre dispose également d'un service de gestion de la collecte qui aligne les efforts de collecte sur les besoins d'analyse et coordonne les efforts de contre-ingérence entre les Plateformes, d'une part, et le personnel travaillant sur le terrain en Belgique, d'autre part.

Afin de se conformer à la loi, le Centre de Coordination dispose d'un service qui introduit toutes les demandes d'utilisation de méthodes spécifiques et exceptionnelles auprès de la Commission administrative chargée du contrôle de ces méthodes de recueil des données. Avec cette autorisation, le SGRS peut, par exemple, entreprendre d'effectuer des écoutes téléphoniques ou d'installer des dispositifs d'écoute.

DIRECTION SÉCURITÉ

La Direction de la Sécurité est responsable du maintien de la sécurité militaire et industrielle. Cette compétence couvre le personnel, les installations, les systèmes d'armes, les équipements et les opérations de la Défense, en Belgique comme à l'étranger. Elle est également responsable de la protection des informations classifiées de la Défense et du maintien du secret, y compris au niveau de l'archivage. Elle mène des enquêtes de sécurité pour les employés de la Défense et les industries qui y sont liées.

Sécurité militaire et industrielle

Ce département est chargé de maintenir la sécurité militaire et industrielle de l'ensemble de la Défense et de l'industrie liée à la Défense.

Premièrement, elle a un rôle de régulation vis-à-vis de l'ensemble de la Défense et des entreprises civiles qui fournissent des services ou des systèmes d'armes.

Les agents de sécurité conseilleront les unités de défense ou les entreprises sur la manière d'appliquer correctement ces directives. Les inspections annoncées ou les visites de contrôle inopinées font également partie des tâches des agents. Lorsque les choses tournent mal, ils mènent des enquêtes sur les incidents de sécurité ou aident les forces de police.

Enfin, ce service dispose de spécialistes de la détection des équipements d'espionnage afin de préserver nos propres installations des écoutes.

Service d'enquête de sécurité

Ce service mène des enquêtes conformément à la loi sur la classification et les habilitations de sécurité, les certificats de sécurité et les avis de sécurité (loi sur la classification 11 déc. 98). Cette loi réglemente la protection du secret nécessaire à la sauvegarde de la sécurité nationale, des plans de défense militaire et des intérêts fondamentaux de notre pays. Une utilisation non autorisée ou incorrecte des informations et systèmes d'armes classifiés pourrait potentiellement causer des dommages non seulement à la Défense, mais aussi au pays tout entier.

Par conséquent, tous les futurs membres du personnel de la Défense, civils et militaires, sont soumis à une vérification de leurs antécédents au cours du processus de recrutement afin d'évaluer leur intégrité et leur fiabilité. En outre, la grande majorité du personnel entre en contact avec des informations, des procédures et des systèmes d'armes classifiés dans l'exercice de ses fonctions au sein de notre organisation. Pour cela, ces membres du personnel doivent disposer d'une habilitation de sécurité du niveau requis : confidentiel, classifié ou secret

La profondeur de l'enquête dépend du niveau et de la fonction exercée. Pour mener à bien ces enquêtes, les enquêteurs en sécurité font appel, entre autres, à la coopération des forces de police, du pouvoir judiciaire, du Registre national, des autorités fiscales et même des services partenaires étrangers. Une habilitation de sécurité n'est accordée que si le candidat fait preuve d'intégrité, de loyauté et de discrétion suffisantes. Une enquête portant sur l'entourage du demandeur, un contrôle numérique ou un entretien avec ce dernier font partie des méthodes d'investigation possibles pour vérifier ces trois critères.

Lorsqu'un refus de délivrer une habilitation de sécurité est communiqué, le demandeur a la possibilité de faire appel de cette décision auprès de la Commission d'appel des habilitations de sécurité.

Les archives classées

Ce service est la mémoire de la Défense en ce qui concerne l'ensemble des informations classifiéesqui ont été archivées. Le service préserve et gère toutes les archives classifiées ainsi que les archives historiques de la Défense tant qu'elles ont une utilité administrative. La préservation se fait à la fois sous forme physique et numérique. Toutes les archives entrantes sont inventoriées, préservées et conservées de manière à pouvoir être facilement exploitées. Les archives classées sont fréquemment consultées par les différents services du SGRS comme base de données. Les recherches historiques scientifiques, les enquêtes parlementaires, les questions des familles de prisonniers de guerre ou encore les enquêtes judiciaires font appel à notre service. À l'occasion des anniversaires importants des unités de la Défense, nos archives permettent de se souvenir de la rédaction d'un livre ou d'une brochure. Lorsque l'utilité administrative de la conservation à la Défense expire, les archives sont déclassées avant d'être transférées aux Archives générales de l'État.

RÉGULATION
CONTRÔLE
MÉMOIRE

CYBER COMMAND

Le Cyber Command belge construit une Cyber Force au travers de partenariats pour protéger, défendre, collecter et combattre dans le cyberespace et l'environnement électromagnétique.

Au sein du Cyberespace et de l'environnement électromagnétique, le Cyber Command est chargé de conduire les missions de renseignement et de sécurité du SGRS, de garantir la liberté de manœuvre de la Défense et de générer des effets militaires à l'appui de ces opérations.

Le Cyber Command assure l'exploitation du cyberespace au profit de l'ensemble de la Nation, ainsi que du SGRS et de la Défense. Acteur clé de la résilience nationale, il occupe une position centrale dans la cyber architecture de notre pays et constitue un partenaire international fiable ainsi qu'une référence nationale en matière de cryptographie. Le Cyber Command développe son processus d'innovation et de nouvelles capacités militaires. Il met en œuvre ces capacités sur les couches physiques, logiques et virtuelles de l'espace cybernétique et électromagnétique. Il entretient une relation privilégiée avec l'industrie, le monde universitaire et associatif. Sa véritable force repose sur son capital humain.

Afin de réaliser ses missions, le Cyber Command mène quatre tâches distinctes :

- Premièrement, il soutient ses composantes sœurs et les autres départements de la Défense en développant un ensemble d'outils de cybercapacité cohérent et intégré.
- Deuxièmement, il assure le développement des capacités cybernétiques spécialisées du SGRS.

NOTRE CYBER FORCE EST LA PREMIÈRE ET LA DERNIÈRE FRONTIÈRE VIRTUELLE DU CHAMP DE BATAILLE

- Troisièmement, il mène des opérations de sécurité et de renseignement dans le cyberespace et l'environnement électromagnétique (Protect, Defend, Collect and Fight).
- Quatrièmement, il dispose de capacités spécialisées dans le cadre de l'aide à la Nation et des situations de cyber-crise nationale.

> Le Cyber Command dispose des attributions d'une 5ème composante (Terre, Marine, Air, Médical et Cyber) au sein de la Défense et de celles d'une direction au sein du SGRS. En fonction de sa mission, il est soumis à deux cadres juridiques distincts : la loi organique relative aux services de renseignement et de sécurité, ou le cadre juridique régissant l'engagement des forces armées belges.

LE CYBER COMMANDEMENT EST ORGANISÉ AUTOUR DE DEUX DIRECTIONS :

La Direction « Cyber Operations » est constituée de quatre unités primaires subordonnées.

- Tout d'abord, l'Unité des cyber opérations défensives (UCD) qui est responsable de la protection et de la défense des réseaux militaires et des systèmes d'armes de la Belgique. Cette unité homologue nos systèmes de communication, d'information et d'armes, effectue des évaluations de vulnérabilité et héberge le Centre d'excellence cryptographique des Forces armées. Il effectue des analyses de logiciels malveillants, surveille les réseaux de la Défense depuis son Centre opérationnel de cyber sécurité (CSOC) et se tient prêt à défendre nos réseaux contre tout acteur étranger ou malveillant.
- Deuxièmement, l'unité de collecte Cyber-SIGINT (CSCU) est responsable de toutes les opérations de collecte intrusives et non-intrusives et de la génération d'effets militaires dans le cyberespace et l'environnement électromagnétique.
- Troisièmement, l'unité de collecte d'influence numérique (DICU) est responsable de la collecte de données de sources ouvertes et de médias sociaux (OSINT et SOCMINT). Elle est aussi en charge de l'analyse de l'influence et des opérations de guerre de l'information adverses.
- Enfin, la plate-forme Cyber(space) Threat Intelligence effectue des analyses de renseignement sur les cyber activités néfastes contre les intérêts militaires belges.

La Direction « Cyber Development & Readiness » est chargée du développement des capacités de cyberdéfense à l'appui du SGRS et des Forces Armées.

Elle se concentre donc sur l'établissement de partenariats avec le monde universitaire, l'industrie et la société civile afin de stimuler l'innovation dans le domaine de la cyberdéfense. Elle est aussi responsable de l'éducation et de la formation du personnel, de l'établissement d'une base doctrinale pour les opérations cybernétiques et du développement d'une force de réserve cybernétique civile. Enfin, la liaison avec les partenaires structurels et les organisations internationales fait également partie de ses attributions.

DIRECTION « PLANS & POLICY »

LES TÂCHES DE LA DIRECTION PLANS & POLICY S'ARTICULENT AUTOUR DE **TROIS AXES** PRINCIPAUX :

1. La planification dans tous les domaines de responsabilité du SGRS, tant au niveau du renseignement, de la sécurité, du Cyber qu'au niveau du fonctionnement (personnel, matériel, infrastructure, budget, ...),

2. L'encadrement, la coordination et le développement de synergies avec les partenaires nationaux et internationaux du Service,

3. La mise en place d'un système de maîtrise de l'organisation.

PLANIFIER, COOPÉRER, SYNCHRONISER ET ÉVALUER SONT LES DÉFIS QUOTIDIENS DE NOTRE DIRECTION « PLANS & POLICY »

La section « Plans »

Cette section s'occupe de la planification dans tous les domaines de responsabilité du SGRS. Elle est chargée de rédiger, en coopération avec toutes les autres directions, les différents plans du Service, comme le Plan de restructuration implémenté le 19 octobre 2022, le Plan Directeur fixant les priorités du SGRS, le Plan Stratégique National du Renseignement, un Plan de gestion de crises, ...

Cette section est également chargée de la documentation de tous les accords signés par le Service mais aussi et surtout de celle décrivant tous les processus du SGRS. Elle exerce également le suivi de la doctrine OTAN en lien avec le renseignement, la sécurité et le Cyber.

Plan Directeur (PDSGRS)

Fin 2021, le SGRS a déterminé son Plan Directeur pour l'année 2022 avec pour objectif de déterminer les tâches à exécuter en priorité eu égard aux ressources disponibles. Dans le courant de l'année 2022, le SGRS a établi son Plan Directeur pour les années 2023 à 2027. Ce Plan vise à améliorer la capacité du SGRS à mieux appréhender les évolutions futures en termes de menaces et de risques.

Il comporte trois volets complémentaires :

- Son volet **«OPÉRATIONNEL»** détermine les activités planifiées à court et moyen termes, dans le respect du cadre légal, des engagements internationaux et des directives supérieures. L'évolution de ces activités prend en compte l'arrivée attendue de ressources supplémentaires.
- Son volet **«RESSOURCES»** fait le point sur les moyens dont devra disposer le Service et leur évolution dans le temps
- Son volet «**FONCTIONNEMENT»** s'attache à fixer les lignes de force des projets les plus importants pour l'amélioration et le maintien de l'opérationnalité du SGRS.

L'équilibre entre les moyens et les tâches est le moteur de cette planification.

La section « Relations »

Cette section a pour tâche de tenir à jour un inventaire de toutes les synergies existantes entre le SGRS et les partenaires nationaux et internationaux et d'identifier les partenariats qui doivent encore être développés. Elle détermine les lignes directrices en termes de synergies et les règles à respecter en présence de partenaires. Elle est le point d'entrée et de sortie pour tous les contacts avec les services de renseignement étrangers. Elle fournit également les officiers de liaison avec nos partenaires nationaux.

La section « Ressources et Capacités »

Cette section est en charge de la planification des tâches de support au SGRS. Cela porte sur la planification en termes de gestion du personnel, du matériel et de l'infrastructure. Mais aussi sur le développement d'un projet de digitalisation visant à, notamment, améliorer le travail des analystes et la documentation en automatisant certains processus.

La section « Contrôle interne »

Cette section a pour objectif d'implémenter un système de maitrise de l'organisation efficace. Il s'agit d'un système de bonnes pratiques de gestion permettant d'assurer l'atteinte des objectifs en appliquant le cycle « Plan Do Check Act ». Une attention particulière est portée sur la gestion des processus et la gestion des risques. Cette section est chargée de la détermination, en coopération avec les différents directeurs, des objectifs stratégiques et opérationnels du SGRS. Elle assure également le suivi des recommandations de nos organes de contrôle. Enfin, elle tire des leçons de l'issue d'une crise et produit un rapport annuel.

À côté de ces sections, il existe un **Officier de Projet Culture** dont l'objectif est de promouvoir la culture organisationnelle, la culture de sécurité et la culture du renseignement. Le but étant de fédérer les agents autour de valeurs et comportements communs et de développer auprès de chacun d'entre-eux un sentiment d'appartenance au SGRS.

DIRECTION SUPPORT

La Direction Support du SGRS a comme mission principale de fournir conseils et appuis au Chef du SGRS et à toutes les directions du SGRS dans les domaines du personnel, de la sécurité, du matériel, de l'infrastructure, de la formation, du training et du budget. La Direction Support est également responsable du suivi des attachés de Défense par l'entremise du **Defense Attaché Office** (DAO).

CONSEILS, APPUIS ET GESTION DES RESSOURCES SONT LES SERVICES INDISPENSABLES FOURNIS PAR NOTRE DIRECTION SUPPORT POUR ASSURER LA STRATÉGIE ET LES AMBITIONS DU SERVICE

LA DIRECTION SUPPORT SE SUBDIVISE EN SIX SECTIONS, CHACUNE RESPONSABLE DANS DES DOMAINES SPÉCIFIQUES

La gestion du personnel

Cette section conseille le Chef du SGRS pour toutes les questions liées au personnel du SGRS. Elle tient à jour les effectifs, planifie et assure sa mise en place dans le cadre des différents plans de mutation ou de l'appui aux opérations du SGRS. Elle coordonne et implémente également les différentes directives de la Défense en cette matière.

Elle est également responsable de la gestion du personnel de réserve du SGRS.

La sécurité

Cette section est chargée des problèmes de sécurité interne au SGRS. Ce domaine couvre la protection des personnes, des installations, des équipements et des informations du SGRS.

Elle assure la fonction d'Officier de Sécurité au sens de la loi dans le cadre des habilitations de sécurité pour l'ensemble du personnel du SGRS. Elle tient à jour une liste des incidents de sécurité, effectue les enquêtes et propose les mesures correctives si nécessaire.

La gestion du matériel et de l'infrastructure

Dans le cadre du matériel, cette section veille au ravitaillement, à l'évacuation, et à l'administration de tout le matériel du SGRS à l'exception du matériel de transmission, du matériel informatique et du matériel Crypto. Elle est responsable de la coordination et de l'émission de l'expression des besoins pour ce matériel avec les gestionnaires de la Direction Générale Material Ressources. Cette section gère également l'ensemble des véhicules du SGRS et les demandes de transport.

Enfin, elle est responsable de l'entretien de l'infrastructure occupée par les services du SGRS avec le support du casernement quartier.

La gestion des systèmes de communication et d'information

Cette section conseille le Chef du SGRS dans le domaine des systèmes d'information et de gestion de l'information au sein du SGRS. Elle donne un avis d'opportunité pour des besoins en matériel de transmission, en matériel informatique et en matériel Crypto. Elle fournit l'appui logistique et technique pour les réseaux internes du SGRS et implémente les droits et les accès déterminés par les autorités fonctionnelles. Elle garantit le support à l'Information Management au sein de l'unité.

La formation et l'entrainement

Ce service analyse les besoins et les offres en formation et entrainement pour l'ensemble du personnel du SGRS, tant en interne qu'en externe. Il coordonne et dispense des périodes de formation et d'entrainement. Enfin, il évalue les formations et fait évoluer l'offre en fonction de l'évolution des besoins.

La gestion des budgets

Cette section conseille le Chef du SGRS pour ce qui concerne l'utilisation des budgets attribués au SGRS. Elle établit un planning budgétaire et fixe les priorités en fonction des moyens disponibles. Elle coordonne avec le sous-département Opération & Entraînements tous les aspects pécuniaires des missions pour le personnel. Ce service assure également le soutien financier et la comptabilité des Attachés de Défense belges à l'étranger. Enfin, il est responsable de la gestion des visas et passeports de service.

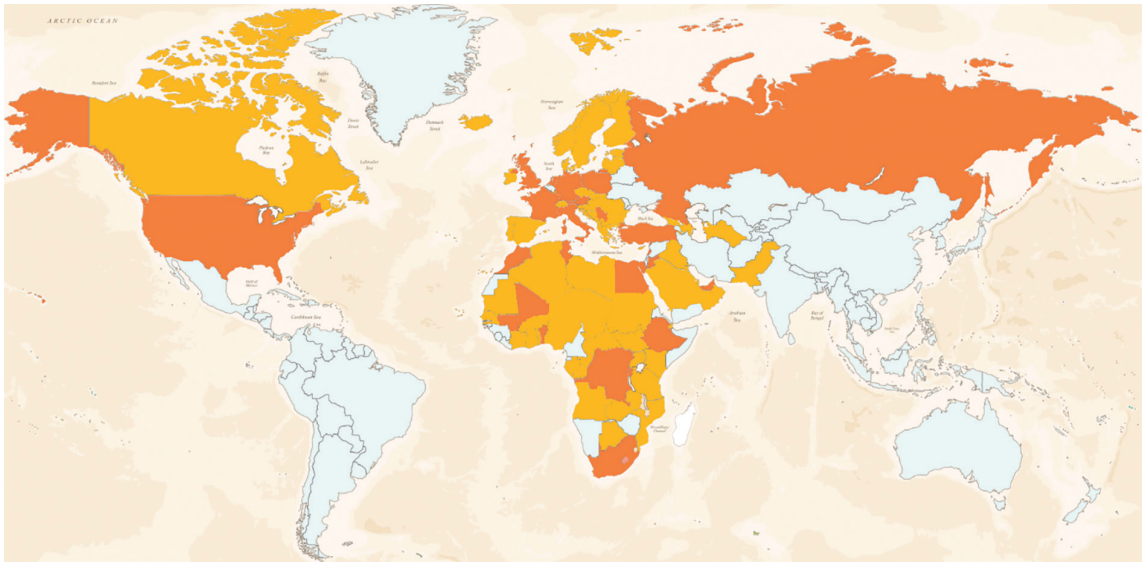
NOTRE SERVICE DES ATTACHÉS DE DÉFENSE

Le Service des Attachés de Défense est responsable de la liaison tant avec les Attachés de Défense belges et étrangers, que les Conseillers militaires et les Attachés de Sécurité belges en poste à l'étranger.

Il est en charge de la mise en place de la procédure de sélection des Attachés de Défense, des Conseillers militaires, des Attachés de Sécurité belges et leurs assistants belges qui sont désignés pour occuper un poste à l'étranger. Il établit leur programme de formation spécifique. Il joue le rôle d'intermédiaire auprès des différentes sections de la Direction Support du SGRS dans les domaines logistique, financier et administratif. En coordination avec différents services du SGRS, il organise les évaluations de tous les postes suivant un calendrier précis.

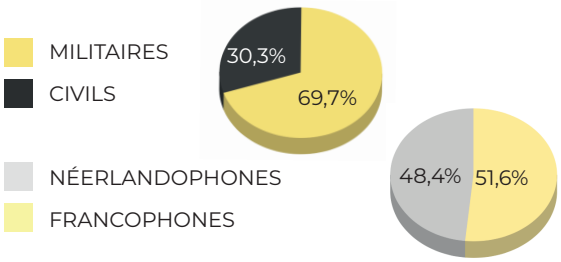
Le service des Attachés de Défense est également en charge des attachés de Défense étrangers accrédités pour la Belgique et il intervient dans la finalisation du processus d'accréditation sur le territoire belge. Le Service responsable des Attachés de Défense étrangers est le Bureau désigné comme point de contact unique pour la Défense. Il centralise toute la correspondance (demandes de renseignements, demandes de visites, demandes d'entrevues, invitations, offres de cours, etc...) qui émanent des Attachés de Défense étrangers accrédités pour la Belgique. Chaque année, le Service responsable des Attachés de Défense étrangers établit, au profit des Attachés de Défense étrangers, un programme d'activités qui comprend des visites dans les unités de la Défense et dans le secteur de l'industrie de défense belge. Une session d'information présidée par le Chef de la Défense est aussi prévue annuellement.

La carte ci-dessous donne un aperçu de tous les pays où les Attachés de Défense belges sont en poste (orange) et les pays pour lesquels ils sont accrédités (orange et jaune).



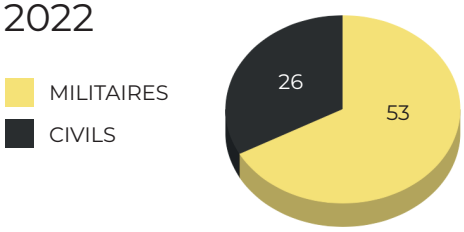
NOS CHIFFRES

PERSONNEL



PERSONNES RECRUTÉES

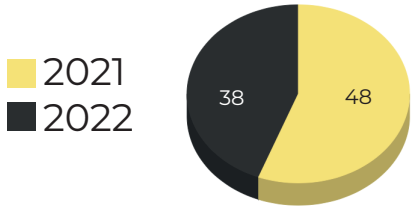
2022



RÉPERCUSSIONS DANS LES MEDIAS

NOMBRE DE FOIS CITÉS DANS LES MÉDIAS ÉCRITS NATIONAUX	**219**
NOMBRE DE FOIS CITÉS DANS LES MÉDIAS ÉLECTRONIQUES NATIONAUX	**294**
NOMBRE D'HEURES CUMULÉES DE PASSAGE SUR LES CHAINES DE TÉLÉVISION ET RADIO NATIONALES	**27H**

NOMBRE DE THÈMES FAISANT L'OBJET DE QUESTIONS PARLEMENTAIRES



NOMBRE DE PAPERS PRODUITS

	2021	2022
Demandes d'informations venant de nos clients et partenaires	5350	6982
	30,50% d'évolution par rapport à 2021	
Volume de l'input	65323	69748
	6,77% d'évolution par rapport à 2021	
Volume de l'ouput		
Demandes d'informations envoyées vers des partenaires (nationaux et internationaux)	60	320
	433,33% d'évolution par rapport à 2021	
Nombre de productions SGRS	486	591
	21,60% d'évolution par rapport à 2021	

NOTRE RECRUTEMENT CYBER

Le capital humain, notre première richesse :

Les recrutements IT sont étroitement liés à la transformation numérique de nos sociétés. Plus spécifiquement, dans les domaines de la cyber-sécurité et de la cyberdéfense, l'évolution, tant quantitative que qualitative des besoins en capital humain va de pair avec l'évolution rapide et disruptive des risques et des menaces cyber sécuritaires. Dans le cadre de ce que nous appelons communément la défense collective, notre cyber résilience étatique en est l'enjeu directement lié à notre capacité de recrutement.

Protect-Defend-Collect-Fight, ... & recruit with agility :

Le Cyber Command regroupe déjà pas moins de 40 métiers, 'STEM' (Science, Technology, Engineering and Mathematics) et 'non-STEM', en lien avec ses quatre domaines d'activité. L'objectif d'affirmation de notre souveraineté dans le cyberespace a donc clairement pour corollaire des objectifs de recrutement soutenus durant les dix prochaines années et bien au-delà. La réflexion autour des métiers d'avenir se mène dès aujourd'hui.

La Défense, jamais un simple job, toujours une MISSION... à haute valeur ajoutée sociétale :

En termes de séduction, parmi une foison d'offres d'emploi Cyber-IT émanant d'autres secteurs, le Cyber Command peut compter sur un position-nement peu commun en lien avec la spécificité des Forces armées et les missions exclusivement dévolues à notre Défense. Comme employeur, la Défense investit massivement dans la formation et la mise à jour permanente des compétences de ses collaborateurs, civils comme militaires.

INNOVER DANS LE CAPITAL HUMAIN : UN DÉFI DE TAILLE ET UNE FORMIDABLE OPPORTUNITÉ

Des projets exploratoires et innovants :

L'indisponibilité de profils de compétence adéquats sur le marché de l'emploi est notoirement criante. Certaines compétences indispensables visant à répondre aux besoins de demain ne sont toujours pas hissées au rang de compétences transversales dans nos écoles. En outre, il est évident que, ni nos concurrents directs sur le marché de l'emploi, ni nos adversaires auto-déclarés dans le cyberespace ne s'embarrassent de certaines lourdeurs administratives dans le cadre de leurs propres démarches de séduction et d'embauche. Le Cyber Command n'a aucunement pour objectif de provoquer une guerre des talents. Mais plutôt de fédérer de nombreuses parties prenantes autour d'un projet de société commun : permettre à tout citoyen cyber-compétent de mettre son temps et son talent au service d'un nouveau type de réserve. Pour cela, les profils 'junior', pas nécessairement diplômés, mais bourrés de talents, et certifiés par des organismes extérieurs constituent des pistes intéressantes. C'est dans ce sens que le Cyber Command a développé une série de partenariats dans le monde associatif avec des ASBL comme « Molengeek » ou « BeCode ».

NOTRE COLLABORATION AVEC LA SÛRETÉ DE L'ÉTAT : LE PLAN STRATÉGIQUE NATIONAL DU RENSEIGNEMENT

En 2018, la Sûreté de l'Etat et le SGRS se sont engagés dans une coopération étroite et dans la mise en commun de certaines tâches ou capacités. Ainsi, du personnel des deux services se sont rassemblés pour constituer une plateforme commune visant à lutter contre le terrorisme. Les équipes de surveillance ont également été mises en commun. D'autres synergies ont été renforcées, dont notamment dans la gestion des sources humaines. Cela a été formalisé dans un Plan Stratégique National du Renseignement (PSNR 2018).

En 2022, les deux services ont décidé d'aller encore plus loin en termes de coopération.

QUATRE DOMAINES ONT ÉTÉ IDENTIFIÉS COMME PRIORITAIRES :

1. La lutte contre l'extrémisme et le terrorisme

2. La lutte contre l'espionnage et l'ingérence

3. Le renseignement Cyber

4. L'interconnexion des environnements Information and Communication Technologies (ICT)

Chacun des deux services de renseignement et de sécurité a des missions propres et des capacités spécifiques, tout en étant complémentaires. Le partage de données, l'échange de savoirs, l'harmonisation de processus, la mise en commun de tâches ou la centralisation de ressources sont des moyens permettant de renforcer l'efficacité des deux services et donc de contribuer à assurer la sécurité nationale.

La lutte contre le terrorisme et l'extrémisme

Dans la lignée de la création de la plateforme commune contre-terrorisme, la Sûreté de l'Etat et le SGRS vont également mettre en commun leurs tâches et leurs moyens afin de lutter contre l'extrémisme. Cela se matérialisera par la transformation de la plateforme contre-terrorisme existante en plateforme commune contre-extrémisme et contre-terrorisme confessionnels et la création d'une deuxième plateforme contre-extrémisme et contre-terrorisme idéologiques.

La lutte contre l'espionnage et l'ingérence

Pour lutter contre l'espionnage et l'ingérence, la coopération prendra la forme de 'Houses' au sein desquelles les différentes menaces émanant de pays ou d'entités seront priorisées en commun. Les tâches y seront réparties de la manière la plus optimale possible et pour traiter de certains dossiers, des équipes mixtes pourront être constituées.

Le renseignement Cyber

Le Cyber Intelligence a pour objectif de collecter des informations portant sur les menaces dans le cyber espace et de les analyser pour en faire du renseignement. La collecte dans le cyber espace peut se faire par différents moyens, intrusifs ou non. Le SGRS développe une capacité cyber importante, par le biais de son Cyber Command. La coopération dans ce domaine vise à faire bénéficier la Sûreté de l'Etat des capacités du SGRS en les mettant en contact avec les niches spécifiques développées au sein de la Sûreté de l'Etat.

L'interconnexion des environnements ICT

Afin de soutenir structurellement la coopération et les échanges entre les deux services de renseignement et de sécurité, une interconnexion poussée des environnements ICT des deux services est indispensable. Pour ce faire, les développements ICT respectifs doivent être synchronisés. Cela permettra, entre autres, l'échange rapide et efficace d'informations classifiées, l'harmonisation, quand cela s'avère nécessaire, des processus informatiques et l'utilisation d'outils communs.

D'autres synergies sont également renforcées, notamment dans le domaine de la formation et de l'entraînement.

La Sûreté de l'Etat et le SGRS mettent tout en œuvre pour implémenter les différentes synergies prévues dans le Plan Stratégique National du Renseignement 2022.

NOS PARTENAIRES

DÉFENSE
SÛRETÉ DE L'ÉTAT
POLICE
DOUANES
SPF ÉCONOMIE
SPF AFFAIRES ÉTRANGÈRES
CENTRE DE CRISE NATIONAL
CTIF
MP
OCAM
EUROPE
OTAN
CCB
COMITÉ R
SPF JUSTICE

Le SGRS fait partie de différentes communautés :

- La Communauté du Renseignement, tant au niveau national avec la Sûreté de l'Etat et l'OCAM, qu'au niveau international avec les services de renseignement étrangers.
- La Communauté de la Sécurité, raison pour laquelle il a des liens étroits avec la Police intégrée, le Ministère public, les Douanes, le CCB, le Centre de crise, ... Il est membre de l'Autorité Nationale de Sécurité.
- Les organisations internationales dont les principales sont l'Union européenne et l'OTAN.
- En tant que service principalement axé vers l'extérieur, il entretient des relations étroites avec le SPF Affaires étrangères.

De par ses compétences très diverses, le SGRS entretient de plus des liens avec de nombreuses autres institutions belges qu'il serait fastidieux de citer exhaustivement: Office des étrangers, CGRA, CTIF, CIAOSN, AFCN.....

Il est primordial pour un service de renseignement d'entretenir des relations de confiance avec ses partenaires et d'échanger des informations. Les synergies avec la Police fédérale doivent également être renforcées, notamment en matière de formations et de Cyber. Un nouvel Officier de liaison a été désigné par le SGRS pour favoriser ces contacts et des coopérations plus poussées avec les Affaires étrangères.

Le Centre Belge de la Cyber Sécurité (CCB) coordonne la mise en œuvre de la stratégie nationale de Cyber sécurité dont le SGRS et en particulier son Cyber Command est un partenaire actif. Nous assistons le CCB techniquement lors de son intervention sur des incidents, nous fournissons une expertise d'analyse de logiciels malveillants et de part de notre position renseignement unique, nous livrons nos analyses approfondies de la menace cyber venant d'acteurs étatiques.

Au niveau international, le SGRS travaille, avec la Sûreté de l'Etat, sur une mise à jour de la Directive approuvée par le Conseil National de Sécurité portant sur les relations avec les services de renseignement étrangers.

NOTRE RETROSPECTIVE 2022 DANS LES MÉDIAS

Janvier - Février - Mars

- Le Plan Directeur du SGRS pour l'année 2022 est approuvé par la ministre de la Défense.
- La loi introduisant des mesures de sécurité supplémentaires pour la fourniture de services mobiles 5G est adoptée par la Chambre le 10 février. Elle prescrit que les opérateurs mobiles qui désirent utiliser des composants 5G devront obtenir une autorisation préalable. Elle émanera d'un groupe composé du Premier Ministre et des ministres des Télécoms, de la Défense, de la Justice, de l'Intérieur et des Affaires étrangères. Pour déterminer le profil de risque du fournisseur, les ministres s'appuieront sur un avis des services de renseignement et de sécurité et de l'IBPT (le régulateur des télécoms).
- Le SGRS est entendu au Kern concernant la guerre en Ukraine.
- L'invasion de l'Ukraine par la Russie s'accompagne d'une vague de cyber opérations russes, tant en Ukraine qu'à l'étranger. Sous la direction du Centre de la Sécurité Informatique, plusieurs initiatives ont été prises au niveau national et des consultations ont été organisées avec des représentants de la Direction Cyber. Nos équipes étaient chargées de surveiller les cyber activités suspectes en étroite collaboration avec l'OTAN et d'autres partenaires internationaux.
- Le SGRS lance un avertissement au personnel de la Défense pour augmenter la vigilance quant aux incidents qui pourraient être liés à l'invasion russe en Ukraine.
- La Belgique expulse 21 diplomates russes.
- La ministre de la Défense expose en commission de la Défense, à huis clos, un plan pour améliorer le fonctionnement du SGRS (Plan Directeur 22).
- Le 30 mars est diffusé l'interview de la ministre de la Défense et du Vice-amiral Wim Robberecht dans De Standaard et La Libre concernant le Plan Directeur.

Avril - Mai - Juin

- Le 7 avril paraissent dans la presse néerlandophone des accusations sur l'achat et l'emploi par le SGRS de routeurs wifi de la marque Huawei. Cette tentative de désinformation est démentie par le Vice-amiral Wim Robberecht dans plusieurs interviews.
- Le cabinet du ministre de la Justice souhaite que les dispositions relatives aux marchés publics prévoient la possibilité de refuser un appel d'offres s'il existe un risque d'espionnage.

  Le 29 mai est diffusé l'interview du Vice-amiral Wim Robberecht dans De Tijd et l'Echo concernant l'évolution structurelle du SGRS.
- Le ministre de la Justice Vincent Vanquickenborne et la ministre de la Défense Ludivine Dedonder déposent au Parlement un projet de loi visant à donner plus de marge de manœuvre aux services de renseignement belges.
- Des articles paraissent à l'occasion du premier anniversaire de la crise de « Jürgen Conings ».
- Les différents gouvernements de notre pays concluent un accord de coopération au sein du Comité consultatif. Il porte sur un mécanisme de filtrage des investissements étrangers dans les secteurs importants pour l'ordre et la sécurité publics ou d'importance stratégique.
- L'opération Cerberus est un succès. La Belgique a rapatrié d'un camp du Nord-Est syrien sous contrôle kurde 16 enfants de djihadistes et six mères de nationalité belge dans un avion de la Défense.
- La commission de l'Économie de la Chambre approuve en deuxième lecture la nouvelle version de la loi sur la rétention des données, qui impose aux opérateurs télécoms de conserver les métadonnées de leurs clients.
- Le SGRS adopte son nouveau « Mission Statement » : mission, vision et valeurs.
- Le gouvernement dépose en urgence un projet de loi au Parlement concernant cinq traités d'entraide judiciaire.

Juillet - Août - Septembre

- La loi modifiant celle du 30 novembre 1998 réglementant les services de renseignement et de sécurité est adoptée.
- Le SGRS et la VSSE signent un nouvel accord de coopération : le Plan Stratégique National de Renseignement 2.0 (PSNR22).
- Lors d'une conférence de presse des Affaires Etrangères, la cyber attaque à l'encontre de la Défense est attribuée à des acteurs chinois. Au cours du premier semestre 2022, des travaux ont été entrepris pour remettre tous les systèmes attaqués en état d'exploitation et supprimer tous les logiciels malveillants. Un rapport de traitement de l'incident et un rapport de renseignement contenant les conclusions techniques ont été fournis.
- Le personnel de la Défense (civils et militaires) sera screené tous les 5 ans.
- Selon un rapport de l'OCAM, environ 500 combattants djihadistes font l'objet d'un suivi prioritaire en Belgique.
- En septembre, la loi instaurant un règlement général de déclassification des documents classifiés est publiée au Moniteur belge. Cette loi garantit que les documents classifiés ne peuvent plus le rester indéfiniment. La loi prévoit qu'après une période de 20 ans (pour les documents confidentiels), 30 ans (pour les documents confidentiels) ou 50 ans (pour les documents hautement secrets), le gouvernement d'origine est tenu de décider si un document classifié peut être déclassifié. Si l'autorité d'origine estime qu'il ne peut être classifié à ce moment-là, cela doit être justifié de manière approfondie. Un document ne peut jamais rester classifié plus de 100 ans. Ensuite, la classification expire automatiquement.
- Des articles font état que, suite à une enquête du SGRS, un militaire belge est suspendu de ses fonctions pour ses sympathies marquées pour l'extrémisme de droite.

Octobre - Novembre - Décembre

- La nouvelle structure du SGRS est implémentée.
- L'inauguration du Cyber Command se tient à Evere en présence de la ministre de la Défense : celui-ci assurera l'exploitation du cyberespace au profit de l'ensemble de la Nation, de la Défense et du SGRS. Il a pour ambition de devenir une référence nationale en matière de cryptographie et d'occuper une position centrale dans l'écosystème fédéral de la cyber sécurité. Grâce à son réseau de partenaires dans le monde économique, universitaire et associatif, il assurera la croissance de la future cinquième Composante.
- Le Chinois Yanjun Xu est reconnu coupable d'espionnage industriel aux États-Unis et condamné à 20 ans de prison.
- Les investissements de la Chine dans les ports d'Anvers et de Zeebrugge comportent un risque d'ingérence ou d'influence dans nos processus de décision, selon le ministre de la Justice en commission de justice dans la Chambre.
- Le Plan Directeur pour les années 2023 à 2027 (PD SGRS 23-27) est finalisé.
- Il transparaît dans l'interview de Noël du Vice-amiral Wim Robberecht par Belga que, globalement, le SGRS est davantage écouté par les responsables politiques.
- Le puzzle du SGRS est dévoilé. Ce jeu vise à susciter l'intérêt du grand public au monde du Renseignement.

NOS PERSPECTIVES D'AUJOURD'HUI SUR LES MENACES DE DEMAIN

Par la Direction Renseignement et par thèmes :

Terrorisme

Le nombre d'incidents, qui de par la nature de leur motivation peuvent être qualifiés d'attaques terroristes religieuses, devrait être stable en 2023 par rapport à 2022.

En 2022, plusieurs hauts cadres des deux principaux mouvements djihadistes internationaux, Al Qaeda et l'Etat islamique, ont été éliminés. Contrairement à ce qui a été observé dans le passé, les deux organisations n'ont pas communiqué sur la mise en place de successeurs.

Par ailleurs, il n'y a actuellement aucune information confirmée concernant la réactivation d'une structure dédiée à l'organisation d'opérations extérieures centrée sur les pays occidentaux et/ou la Belgique au sein de ces deux mouvances.

Cependant, si la capacité fait actuellement probablement défaut, l'intention terroriste de ces groupes persiste. En outre, des attaques et/ou revendications d'opportunité ne peuvent être exclues de même qu'un passage à l'acte d'une personne auto-radicalisée. Une attaque perpétrée par une personne isolée représente d'ailleurs le scénario le plus probable.

Extrémisme

La menace posée par l'extrémisme non-religieux ne devrait pas décroître en 2023.

La crise économique, aggravée par la crise énergétique et la guerre en Ukraine, se marquera par la persistance d'une forte inflation qui continuera à peser sur le pouvoir d'achat, notamment des catégories les plus fragiles. Cette crise favorisera dès lors l'émergence de mouvements de contestation que les groupes extrémistes, tant de gauche que de droite, chercheront à récupérer.

La persistance de la pression migratoire vers l'Europe continuera à nourrir la propagande extrémiste de droite.

La fragmentation structurelle de la scène politique dans de nombreuses démocraties occidentales et la polarisation favorisée par l'usage des réseaux sociaux continueront à susciter l'attrait des groupes et personnes tenant un discours extrémiste. L'émergence de nouvelles formes d'extrémisme ne répondant qu'imparfaitement aux critères définissant les extrémismes de gauche et de droite mais caractérisées par l'adhésion à des thèses complotistes devrait se poursuivre. La survenance d'une nouvelle crise sanitaire constituerait un catalyseur à cet égard.

Prolifération

Globalement, l'architecture de non-prolifération des Armes de Destruction Massive continue de s'éroder.

Cette tendance mine les relations internationales, favorise la course à l'armement avec comme conséquence l'augmentation du risque d'escalade et d'erreur de calcul.

Dans cette perspective, la Russie constitue la menace principale et la plus directe pour la paix euro-atlantique, en particulier dans le contexte actuel de son invasion de l'Ukraine.

Au Moyen-Orient, le comportement de l'Iran (développements balistiques et nucléaires, ingérence) constitue un important potentiel de déstabilisation dans une région d'intérêt majeur pour l'économie mondiale. Le régime syrien, avec le support de la Russie, demeure un défi pour le désarmement chimique.

En Asie, les relations conflictuelles entre les puissances nucléaires pakistanaises et indiennes, l'essor de la Chine, et les développements nucléaires de la Corée du Nord demeurent préoccupants.

En Occident, la menace terroriste CBRN reste d'actualité.

Par la Direction Renseignement et par pays :

Russie

Plusieurs expulsions ont entraîné une réduction temporaire des capacités de renseignement russe sur le territoire belge. Celle de 21 diplomates russes attachés à l'ambassade de Russie en Belgique et au consulat à Anvers le 29 mars. Mais aussi celle de 19 diplomates russes travaillant à la mission russe auprès de l'UE le 5 avril. L'image détériorée de la Russie dans la société belge en raison de la guerre renforce cette tendance.

Toutefois, les services de renseignement russes s'adapteront à l'évolution de la situation pour répondre à leurs besoins en matière de renseignement.

Chine

XI Jinping ayant obtenu son troisième mandat, les besoins en renseignements du Parti communiste chinois (PCC) se concentrent de plus en plus sur l'étranger.

Pour la première fois, un chef du renseignement fait partie du Politburo, ce qui se traduira par une augmentation des ressources pour les agences de renseignement. Celles-ci doivent fournir des renseignements qui permettront à la Chine de devenir technologiquement autonome, de se positionner dans les conflits avec l'Occident et de garantir les intérêts économiques de la Chine à l'échelle mondiale.

Avec la collecte de renseignements et l'influence vers l'UE et l'OTAN, l'importance de la Belgique dans le travail de renseignement chinois ne fera qu'augmenter.

Pays africains

Les prochaines échéances législatives en RDC et au Rwanda devraient renforcer la volonté des différentes autorités africaines de persévérer dans des activités qui soutiennent leurs intérêts nationaux.

Il y a fort à parier que l'invasion de l'Ukraine par la Russie aura aussi des conséquences pour le continent africain en 2023. Les états révisionnistes tels que la Chine ou la Russie pourraient chercher à utiliser des proxys africains comme instruments pour atteindre ou consolider une position avantageuse, voire dominante, face à des rivaux politiques, militaires ou économiques. De telles tensions pourront avoir des conséquences en Belgique ou pour les intérêts et personnes belges en Afrique.

Le SGRS restera donc attentif à l'évolution de la situation internationale et à des conséquences éventuelles sur les activités des services de renseignement africains.

Par la Direction Cyber Operations :

Généralités

Les acteurs de la cyber menace s'intéressent de plus en plus aux attaques de la chaîne d'approvisionnement informatique et à celles menées contre les fournisseurs de services cloud et informatiques.

Ces attaques permettent à ces acteurs de prendre pied sur les entités qu'ils ciblent. La perturbation des communications par satellite est probablement une tendance qui va gagner en importance à court et à moyen terme. La perturbation des câbles de fibre optique a fait la une des journaux en 2022 et il est probable que ce type d'attaques cyber-physiques se multiplient à court et à moyen terme.

Russie

À court terme, le service de renseignement militaire russe GRU sera très préoccupé par l'Ukraine, tandis que le service de renseignement extérieur russe SVR continue de cibler des gouvernements, des ONG et des groupes de réflexion avec de nouveaux logiciels malveillants. Les sanctions économiques qui limitent l'accès de la Russie à la technologie pourraient entraîner une augmentation du cyber-espionnage économique.

Après avoir mené des attaques perturbatrices contre l'Ukraine avec pas moins de 9 effaceurs de données au premier semestre 2022, les acteurs

liés au GRU ont continué à cibler l'Ukraine avec de nouveaux logiciels malveillants d'effacement de données au second semestre 2022.

En 2022, de nouveaux types de logiciels malveillants russes visant les systèmes de contrôle industriel et les technologies opérationnelles ont été découverts. Une attaque russe sur le réseau électrique en Ukraine pourrait perturber la distribution électrique. Des acteurs étatiques russes ont également été observés en train de mener une cyber-reconnaissance contre des infrastructures critiques dans des pays occidentaux. Les analystes s'inquiètent d'une éventuelle attaque contre les infrastructures critiques occidentales si la guerre en Ukraine s'étend au-delà du théâtre ukrainien.

Les hacktivistes pro-russes ont mené un nombre croissant de cyber-attaques perturbatrices contre presque tous les pays de l'OTAN (et même au-delà), souvent en réaction aux mesures prises par ces pays que la Russie perçoit comme menaçantes. Les États baltes auraient été les plus durement touchés par les hacktivistes, permettant à la Russie de mener des cyberopérations et des opérations de désinformation.

Ces cyber-attaques perturbatrices se poursuivront en 2023 et sont souvent une réaction russe à une déclaration politique forte ou à la livraison d'équipements militaires à l'Ukraine.

La cybercriminalité sous forme d'attaques par ransomware est de plus en plus utilisée comme une arme géopolitique depuis le second semestre 2022, non seulement contre des entités ukrainiennes mais aussi contre des services gouvernementaux de membres de l'OTAN (exemple : Monténégro).

En plus de fournir à la Russie une dénégation plausible, les attaques par ransomware lui permettent de mener des attaques destructrices contre des membres de l'OTAN tout en restant sous le seuil de l'article 5. Nous pensons donc que cette tendance à utiliser les ransomwares comme une arme géopolitique va se poursuivre.

Chine

Le cyber ciblage continuera probablement à servir des intérêts économiques et militaires, avec une attention particulière pour les pays qui jouent un rôle important dans les initiatives « Belt and Road » de la Chine et dans les objectifs stratégiques de la Chine en mer de Chine méridionale.

Les attaques perturbatrices menées par des hacktivistes chinois sur Taïwan lors de la visite de Madame Nancy PELOSI à Taipei en août 22 seront probablement répétées si la Chine perçoit les actions d'autres pays à l'égard de Taïwan comme allant à l'encontre du principe de la « Chine unique » de la Chine.

Reste du monde

Des cyber opérations perturbatrices contre les services gouvernementaux d'un partenaire de l'OTAN (Albanie) ont été attribuées à l'Iran, ce qui laisse présager une moindre retenue à l'avenir dans l'attaque de cibles de l'UE/OTAN. Un groupe mandataire iranien basé en Irak a visé des cibles ukrainiennes à deux reprises, ce qui pourrait indiquer une collaboration croissante entre l'Iran et la Russie en termes de cyber opérations.

Alors que certains cyber acteurs offensifs du secteur privé, comme le groupe israélien NSO (Pegasus), font l'objet d'un examen minutieux de la part de divers gouvernements, des articles de presse annoncent néanmoins que le business des cyber mercenaires est en plein essor. Leur offre de «surveillance en tant que service» permet à leurs clients de pénétrer les réseaux, les ordinateurs et les smartphones de leurs cibles (souvent des dissidents, des journalistes, des militants des droits de l'homme).

Une tendance à surveiller est la collaboration de cyber acteurs offensifs du secteur privé avec des sociétés militaires privées (exemple : le groupe Wagner).

NOUS FAISONS LE TRAVAIL

Nous sommes les yeux et les oreilles de notre Nation. Nous recherchons ce que nos ennemis veulent garder secret. Nous agissons partout où nos adversaires se réfugient et toujours dans l'ombre et avec un maximum de discrétion. Nous enquêtons sur nos adversaires afin d'anticiper les nouvelles menaces et nous veillons à la sécurité de nos secrets militaires et de nos connaissances technologiques.

Nous conseillons nos dirigeants politiques et militaires afin qu'ils puissent faire les meilleurs choix, de façon indépendante et souveraine, pour protéger au mieux notre pays et ses concitoyens. Nous opérons partout dans le monde où nos intérêts le demandent. Car aujourd'hui les menaces à l'encontre de notre société sont devenues encore plus complexes, imprévisibles et multiples.

Nous sommes présents en appui des opérations militaires, dans la lutte contre l'espionnage et l'ingérence, la cyber sécurité, la lutte antiterroriste, la lutte contre les extrémismes, la lutte contre la prolifération d'armes de destruction massive. Sans oublier la lutte contre les organisations sectaires ou criminelles ainsi que dans les domaines scientifiques et économiques comme la protection des entreprises et les infrastructures vitales.

NOTRE PETIT LEXIQUE

SGRS : Service Général du Renseignement et de la Sécurité

VSSE : Sûreté de l'État

OCAM : Organe de Coordination pour l'Analyse de la Menace

GRU : Service de renseignement militaire russe

SVR : Service des renseignements extérieurs de Russie

OTAN : Organisation du traité de l'Atlantique nord

UE : Union européenne

ONG : organisation non gouvernementale

CBRN : agent ou matériel chimique, biologique, radiologique et nucléaire

PSNR : plan stratégique nationale du renseignement

PDSGRS : plan directeur du SGRS

CGRA : Commissariat général aux réfugiés et aux apatrides

AFCN : Agence fédérale de Contrôle nucléaire

CTIF : Cellule de Traitement des Informations Financières

CIAOSN : le centre d'information et d'avis sur les organisations sectaires nuisibles

CCB : Centre Belge de la Cyber Sécurité

DAO : Bureau des Attachés de Défense

UCD : Unité des cyber opérations défensives

CSOC : Centre opérationnel de cyber sécurité

CSCU : Unité de collecte Cyber-SIGINT

DICU : Unité de collecte d'influence numérique

OSINT : la collecte de données de sources ouvertes et de médias sociaux

T.E.S.S.OC : Terrorisme – Espionnage – Subversion – Sabotage – « Organised Crime »