RAPPORT D'ENQUÊTE

La cybercapacité au sein du service de renseignement militaire

Numéro de notice 2025.317 – 5 février 2026

Comité R | I
Contrôle des services de renseignement
Toezicht op de inlichtingendiensten

EXECUTIVE SUMMARY

À la mi-octobre 2022, le Ministère de la Défense a créé le Commandement cyber. Celui-ci a été intégré au sein du Service Général du Renseignement et de la Sécurité des Forces armées (SGRS) afin de permettre à ce service d'exécuter ses missions dans le cyberespace. La présente enquête a montré que les structures de contrôle internes et les instruments de gestion confirment, dans la pratique, cette intégration légale du Commandement cyber au sein du SGRS.

La création du Commandement cyber a marqué une première étape dans l'approfondissement et l'élargissement des capacités cyber de la Défense, aboutissant finalement à la création, à partir de cette unité, d'une Force cyber à part entière, une des cinq forces de combat des forces armées belges.

La capacité cyber du Commandement cyber assure actuellement l'exploitation du cyberespace au profit du SGRS et de la Défense et apporte, dans certains cas, son soutien à la Nation. En fonction de sa mission, la capacité cyber relève d'un cadre juridique différent : la loi organique des services de renseignement et de sécurité (L.R&S) – dans ce cas, la responsabilité incombe au Commandement cyber du SGRS – ou bien l'Arrêté royal fixant la structure de la Défense et la Loi relative à la mise en œuvre et à la mise en condition de la Défense et son arrêté d'exécution, cas dans lequel la responsabilité incombe à la Force cyber. Bien que, d'un point de vue juridique, le Commandement cyber et la Force cyber soient deux entités distinctes au sein des forces de combat, ce n'est pas le cas sur le plan organisationnel. Le Commandant du Commandement cyber est également le Commandant de la Force cyber, et il existe une seule organisation au sein de laquelle tous les membres du personnel, le cas échéant, sont (doivent être) au service des deux entités. Alors que les missions et les compétences du Commandement cyber sont définies légalement dans la L.R&S, ce n'est pas le cas pour les missions de la Force cyber. D'autre part, les lignes hiérarchiques diffèrent selon que l'Unité cyber agit en tant qu'organe d'exécution du SGRS (Chef du SGRS) ou en tant que Force cyber (Chef de la Défense).

Cette dualité dans la structure juridique, bien que compréhensible et justifiée, comporte un risque d'ambiguïté dans l'exécution des missions et l'exercice des compétences, et risque de générer des discussions sur la compétence du Comité R/I en tant qu'organe de contrôle des activités de l'Unité cyber. Le Comité formule donc des recommandations concernant (1) la clarification des missions de la Force cyber, (2) l'intégration plus poussée du Commandement cyber au sein du SGRS et (3) l'octroi à la Commission parlementaire de suivi des missions militaires du pouvoir de charger le Comité d'effectuer un contrôle de la capacité cyber agissant en tant que Force cyber. Les autres recommandations portent sur la nécessité d'accorder une attention suffisante aux ressources financières consacrées à la capacité cyber, au soutien à la Sûreté de l'État (VSSE) et à une éventuelle révision de la compétence de « contre-attaque » du SGRS dans le cyberespace.

1.
PREAMBULE

1.1. ORIGINE DE L'ENQUETE

1. Le 19 octobre 2022, le Ministère de la Défense a mis en place son « Cyber Command », déjà présenté comme « *une première étape vers la création d'une cinquième composante dans l'armée belge, la composante CYBER* »[1], en plus des composantes Terre, Air, Médicale et de la Marine.[2]

2. Ce nouveau commandement (« Commandement cyber ») a été intégré au SGRS[3], si bien que le Comité R/I est compétent pour exercer son pouvoir de contrôle légal. Afin de garantir l'exercice efficace et efficient de ce contrôle, il était primordial pour le Comité R/I de se familiariser pleinement avec ce nouveau commandement dans tous ses aspects. Le Comité a constaté dès le départ que l'objectif était de faire évoluer le Commandement cyber, dans le giron du SGRS, vers une véritable Composante cyber / Force cyber (Cyber force). A cet égard, la ministre de la Défense de l'époque expliquait dans sa déclaration de politique générale du 4 novembre 2020 que : « *[à] partir de cette cybercapacité renforcée au sein du SGRS, une composante cyber de la Défense peut être développée à un horizon de cinq ans, sans affaiblir la capacité de cyber-renseignement du SGRS. Les opérations de la future composante Cyber pourront aller au-delà de la cyberdéfense et nécessitent un cadre juridique qui sera créé au cours de cette législature* ».[4]

---

1 MATRICHE, J., « Cyberespace, le nouveau champ de bataille de l'armée belge » , *Le Soir*, 18 octobre 2022 (*« une première étape vers la création d'une cinquième composante dans l'armée belge, la composante CYBER »*) .

2 L'Arrêté royal du 2 décembre 2018 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités (*M.B.* 8 janvier 2019), comme c'était le cas à ce moment-là, l'article 1er, 5° ne mentionnait que quatre composantes.

3 Fin décembre 2024, le SGRS a présenté la structure du service au Comité R/I. Lors de cette présentation, dans la partie consacrée au cyberespace, il a été expliqué que le Commandement cyber, dirigé par le Commandant Cyber Command (CyC), était intégré dans la structure du SGRS, et que ce Command cyber était responsable de l'exécution des missions reprises dans la L.R&S. Le SGRS décrit ces missions en utilisant les termes Cyber Intel et Cyber Security. Voir également le rapport de l'audition du Commandant du Commandement cyber par la Commission de la Défense nationale, *Doc. parl.*, Chambre, 2022-2023, DOC 55 3323/001.

4 *Doc. parl.*, Chambre, 2020-2021, DOC 55 1610/017, p. 25.

3. Cette évolution prévue vers une Composante cyber/Force cyber a également été confirmée dans les exposés d'orientation suivants relatifs à la Défense[5], ainsi que lors des premiers contacts entre le Comité R/I et le premier Commandant du Commandement cyber, le général-major Michel VAN STRYTHEM.[6] Dans une interview, le général-major VAN STRYTHEM a déclaré que le commandement du Commandement cyber resterait *« waarschijnlijk »* (sic) *(« probablement »* - traduction libre) au sein du SGRS.[7] Lors de la présentation qu'il a donnée au Comité R/I le 18 janvier 2023, il a également présenté une vision du Commandement cyber, qui fait certes partie du SGRS, mais qui doit également devenir une composante à part entière de la Défense, dans une dimension transversale d'appui comparable à celle de la Composante médicale. Le 2 mars 2023, le général-major VAN STRYTHEM a présenté, à l'Ecole royale militaire[8], la feuille de route du Commandement cyber qui doit finalement devenir une « Cybercomposante », qui, en tant que telle, relève, d'une part, de la loi organique des services de renseignement et de sécurité du 30 novembre 1998 (L.R&S) et, d'autre part, entre dans le cadre du 'CHOD Ops Order' et de ses règles d'engagement.[9]

4. Cette évolution du Commandement cyber, qui, d'une section du SGRS est devenu une Force cyber, pourrait avoir des conséquences évidentes sur l'exercice des missions du Comité et soulève plusieurs questions fondamentales, notamment en ce qui concerne l'exercice des missions du SGRS dans le cyberespace. Ceci a constitué une raison supplémentaire d'ouvrir une enquête de contrôle sur le Commandement cyber.

5. Dans l'Accord de gouvernement fédéral 2025-2029, la création de la Composante cyber n'est pas mentionnée. Les passages suivants portent sur la Défense et la problématique

---

5 *Doc. parl.*, Chambre, 2021-2022, DOC 55 2294/008, p. 31 ; *Doc. parl.*, Chambre, 2022-2023, DOC 55 2934/020, p. 42 et *Doc. parl.*, Chambre, 2023-2024, DOC 55 3649/022, p. 45.

6 Par l'A.R. du 23 octobre 2022, le général-major Michel VAN STRYTHEM a été désigné pour exercer la fonction de Commandant du Commandement cyber. Michel VAN STRYTHEM a été désigné au grade de lieutenant-général (*M.B.*, 18 août 2025).

7 CLEVERS, A., « L'armée belge se dote d'un Cyber Command », La Libre Belgique, 19 octobre 2022.

8 Institut Royal Supérieur de Défense , Conférence du soir « Pourquoi la Belgique a-telle besoin d'un Cyber Command ? », 2 mars 2023. *« Quelles sont les mission de ce Commandement cyber ? La première mission [= Intelligence, Security & military operations in Cyberspace] est de mener des opérations. Et cela peut se faire, cela doit se faire dans deux cadres juridiques distincts. Donc, tout d'abord, il y a le cadre juridique de la loi organique des services de renseignement et de sécurité où, en fait, les opérations effectuées dans le cadre des opérations de sécurité et les opérations de renseignement, sont menées en vertu de la loi organique du SGRS-ADIV. Les autres sont les opérations militaires menées sur mandat du gouvernement avec des règles d'engagement et un CHOD OP ORDER qui s'inscrit dans le cadre des procédures et du système connus dirigés par le Département Opérations de la Défense. [Il y a ?] les deux cadres dans lesquels cela s'inscrit. En temps de paix, ce sont l'accent, le volume et le pourcentage qui importent le plus pour le premier cadre juridique, mais il y a des exemples d'opérations dans le cadre de l'engagement de la force de combat, avec les règles d'engagement existantes* ». Traduction libre des propos tenus par le général-major VAN STRYTHEM.

9 Voir notamment la Loi Mise en œuvre et Mise en condition des Forces armées du 20 mai 1994 (*infra*).

cyber :

« La Défense joue également un rôle central dans la lutte contre les menaces hybrides et les menaces liées à la compétition entre grandes puissances (y compris les risques économiques) émanant d'acteurs étatiques et non étatiques. Pour jouer un rôle déterminant dans ce domaine, nous nous engageons à notamment poursuivre l'expansion de nos capacités de défense et notre cyberdéfense ***en investissant également dans des ressources de guerre électronique et dans l'intelligence artificielle. Ainsi, la poursuite du déploiement du cyber-commandement vise, entre autres, à accroître notre résilience face aux ingérences étrangères et à nous préparer à des opérations offensives si nécessaire.*** *Le renforcement de la coopération entre les différents acteurs devrait nous permettre d'améliorer nos capacités dans ce domaine. Nous investissons davantage dans les nouvelles technologies.*[10]

Nous déployons une approche multidimensionnelle fondée sur la sécurité militaire, la cybersécurité et la sécurité de l'information. Nous renforçons notre cyberprotection en investissant dans de ***nouvelles capacités pour notre Cyber Commandement*** *mais aussi via des coopérations avec des centres de connaissances et en renforçant davantage encore les* ***synergies entre les différents services de renseignement et en assurant une plus grande mobilité pour le personnel au sein des cadres légaux existants****. Ceci tout en respectant l'indépendance et l'individualité des différents services. Nous nous concentrons sur la poursuite de la réforme du SGRS, sans toutefois démilitariser sa fonction principale. Dans le cadre du Codex de la Défense, nous travaillons à la modernisation des lois relatives à la collecte de renseignements militaires, telles que la* ***loi sur le renseignement tactique****.*[11]

Nous renforçons la coopération avec les services de renseignement de nos partenaires au sein de l'OTAN et de l'UE. Dans le contexte de notre résilience sociétale, nous canalisons mieux les informations pertinentes vers d'autres acteurs. ***La collecte de renseignements à l'étranger est renforcée, tant dans le domaine de la défense et de la cybernétique que dans le domaine économique.***[12]

Le ***Service général du renseignement et de la sécurité dispose de ressources suffisantes pour remplir pleinement ses missions dans ce domaine*** *en respectant sa spécificité de service de renseignement militaire ».*[13]

6. Ces passages pourraient laisser entendre que le gouvernement fédéral a décidé de maintenir le Commandement cyber au sein des structures du SGRS pour les années à venir. Une confirmation explicite de ce choix figure à l'article 42 de l'Arrêté royal du 30 juin 2025 fixant la structure générale du Ministère de la Défense et les attributions de certaines

10 Accord de coalition fédérale 2025-2029, p. 189.

11 *Idem*, p. 190.

12 *Idem*, p. 190.

13 *Idem*, p. 190.

autorités [14], qui stipule que : *« [a]u sein du Service Général du Renseignement et de la Sécurité il existe un commandement cyber qui agit dans le domaine du cyberespace et qui exerce les missions visées à l'article 11 de la loi du 30 novembre 1998. Le commandement cyber est dirigé par le commandant cyber. Il est également le commandant de la force cyber».*

7. La note politique du ministre de la Défense du 17 avril 2025 indique que les composantes de la Défense seront à nouveau appelées « Forces » à compter du 21 juillet 2025, dont la Force cyber, *« [c]ette dernière n'ayant pas encore vu le jour »*[15], ce qui s'est produit peu après. L'article 1er de l'A.R. précité du 30 juin 2025 stipule que la Force cyber fait partie des Forces armées.[16]

1.2. COMPETENCE DU COMITE R/I

8. La compétence du Comité R/I dans le cadre de sa mission de contrôle générique n'est pas déterminée de manière fonctionnelle mais organique.[17] Le Comité contrôle le SGRS (et la VSSE) comme organisation. Le critère organique de délimitation des compétences implique que le Comité contrôle le SGRS (et la VSSE) en tant que structures distinctes, composées d'un ensemble de personnes et de ressources, d'un ensemble de missions et d'activités et d'une structure de contrôle hiérarchique propre. Le Comité contrôle toutes les activités des services soumis au contrôle, c'est-à-dire tant les activités opérationnelles que les missions de gestion.

9. Comme précisé dans le présent rapport, le SGRS mène diverses activités pour l'exécution de différents types de missions. Dans la Loi Contrôle, le législateur a clairement exprimé sa volonté de faire en sorte que toutes les activités exercées par une même organisation soient contrôlées par le Comité R/I. Le fait qu'un service, une unité ou une capacité, selon le type d'activité qu'il ou elle exerce, sous différentes autorités ou sous une dénomination différente, ne modifie pas la portée de la mission de contrôle légal du Comité. Sinon, cela reviendrait à défendre l'affirmation selon laquelle l'exécutif aurait la possibilité et le droit de contourner la loi par voie de règlement (arrêté royal, arrêté ministériel ou note de service interne).

10. La délimitation organique des compétences, telle que définie par le législateur, est importante pour le contrôle de l'Unité cyber. Comme cela a été précisé, cette unité, en tant qu'organisation, a été chargée de deux types de missions : les missions du Commandement

---

14 *M.B.*, 15 juillet 2025, p. 59443.

15 *Doc. parl.*, Chambre, 2024-2025, DOC 56 0856/022, p. 30. Précédemment (le 3 juin 2025), le Roi avait mentionné que *« l'histoire s'écrit au sein de la Défense en remettant le symbole de la Force cyber. Cette cérémonie a marqué le point culminant de la création de cette nouvelle force, indispensable compte tenu de la menace actuelle »* (traduction libre). (https://x.com/BECybercom/status/1930164947209629768).

16 *M.B.*, 15 juillet 2025.

17 *Cf.* art. 33, 34, 40, 48, 50 et 51 Loi Contrôle.

cyber (c'est-à-dire en exécution des missions du SGRS) et les missions de la Force cyber (c'est-à-dire en tant que force armée). Comme indiqué plus haut, ces activités sont menées par la même structure. Compte tenu du choix légal qui s'est porté sur le critère organique comme délimitation des compétences, le Comité est habilité à contrôler les activités menées dans le cadre de l'exécution des deux types de missions. Le fait que, dans l'exécution des ordres du Commandement cyber, l'Unité cyber soit placée sous l'autorité directe du Chef du SGRS, mais dans le cadre de l'exécution des missions de la Force cyber sous le commandement du Chef de la Défense, n'affecte pas le pouvoir de contrôle du Comité.

11. Pour la portée de la mission de contrôle légal du Comité, le fait que la cybercapacité militaire porte le nom de Commandement cyber ou de Force cyber n'a aucune importance.[18] Le Comité constate que le SGRS a un avis différent sur ce point.[19]

12. Toutefois, le Comité n'est pas habilité à vérifier les instructions données à l'Unité cyber par le ministre de la Défense, le Chef de la Défense ou, le cas échéant, le sous-chef d'état-major de mise en condition et opérations. Le Comité n'exerce aucun contrôle sur le gouvernement ni sur les autres autorités des organisations à contrôler.[20] En toute logique, le Comité a néanmoins un pouvoir de contrôle sur les instructions du Chef du SGRS à l'Unité cyber.

13. Enfin, le Comité rappelle que l'utilisation du budget de la Force cyber ne peut jamais avoir de répercussions sur les compétences légales. Si le budget de la Force cyber est utilisé pour placer des collaborateurs cyber au sein des autres forces (« modules de capacité décentralisés »), cela signifie que les acteurs concernés doivent avant tout se charger de l'exécution des missions de la Force cyber. D'autre part, cela ne signifie nullement que le

---

18 Cela n'a pas non plus d'importance que la capacité de renseignement militaire soit appelée SGRS ou ACOS IS.

19 Le SGRS n'était pas d'accord avec l'affirmation relative à la compétence de contrôle. Comme indiqué précédemment, le Comité estime que le fait qu'un service, une unité ou une capacité agisse sous différentes appellations, en fonction du type d'activités qu'il ou elle exerce, n'a aucune incidence sur la portée de la mission légale de contrôle du Comité. Affirmer le contraire reviendrait en effet à défendre la thèse selon laquelle le pouvoir exécutif peut et a le droit, en vertu du règlement (en l'occurrence l'AR Structure de la Défense du 30 juin 2025), de passer outre la loi (en l'occurrence la Loi Contrôle).

20 Dans le même ordre d'idées, le Comité n'est pas habilité à contrôler les activités du Chef du SGRS en sa qualité d'Aide de Camp du Roi. Les Aides de camp du Roi font en effet partie de la Maison Militaire, une organisation distincte qui assiste le Roi dans l'exercice de ses compétences constitutionnelles en matière de Défense. Le Comité n'est pas non plus habilité à exercer un contrôle sur les activités du ou des conseillers généraux du SGRS en sa/leur qualité de membre(s) du Conseil de direction du Ministère de la Défense. D'un point de vue organique, tant la Maison Militaire que le Conseil de direction constituent deux structures distinctes qui se distinguent juridiquement et factuellement de la structure unique SGRS & ACOS IS.

Comité est considéré de plein droit comme n'exerçant que de telles activités, ni que le Comité n'aurait aucun pouvoir de contrôle sur ces collaborateurs cyber.

1.3. FINALITE DE L'ENQUETE

14. La finalité de la présente enquête de contrôle est d'identifier et d'analyser l'organisation et les activités du Commandement cyber.[21] Il importe en particulier de clarifier la position exacte du Commandement cyber au sein du SGRS, en définissant les responsabilités précises et ce que cela implique pour la ligne de commandement. Il est au moins aussi important d'évaluer l'impact éventuel de la création de la Force cyber, dont le commandant est également le Commandant du Commandement cyber, sur l'exercice des missions du SGRS dans le cyberespace. A cet égard, il convient de se demander, entre autres, si certaines activités (de renseignement) réservées au SGRS risquent désormais d'être soustraites au contrôle du Comité R/I.

15. Ce risque de manque de contrôle constitue une menace potentielle pour la protection des droits des personnes au titre de la Constitution et de la loi, ainsi que pour la coordination et l'efficacité des services. La réalisation d'une enquête de contrôle permettra au Comité R/I d'informer le plus précisément possible les autorités compétentes des risques réels liés aux activités de renseignement qui échappent effectivement au contrôle démocratique et de formuler toutes les recommandations utiles pour circonscrire ces risques.

16. Récemment, le Premier ministre a donné un aperçu de la stratégie belge en matière de cybersécurité.[22] Il était notamment question de la coopération entre le Commandement cyber et le Centre pour la Cybersécurité Belgique (CCB), ou encore des interactions avec les représentants permanents belges de l'UE et de l'OTAN.[23] La Plateforme Cybersecurity du Comité de coordination du renseignement et de la sécurité (CCRS) a également examiné les possibilités offertes aux services de renseignement et de sécurité pour discuter de la politique de cybersécurité et échanger des informations sur la *situational awareness*.[24] Le présent rapport n'examine pas ces formes de coopération. Sur demande, ces thèmes

---

21 Le titre complet de l'enquête est: 'Enquête de contrôle sur l'organisation et les activités du Cyber Command du Service Général du Renseignement et de la Sécurité (SGRS)'.

22 *QRVA*, Chambre, 56 020, 29 juillet 2025 (Question n°61 de Monsieur le Député Kjell Vander Elst du 19 juin 2025 au Premier ministre sur « La stratégie belge en matière de cybersécurité ») (DO 2024202504357).

23 Outre cette coopération structurelle, le CCB et le Commandement cyber coopèrent également sur une base *ad hoc* sur des dossiers spécifiques tels que le NATO Cyber Defense Pledge, le EU Cyber Census et le EU Cyber Defence Coordination Centre (EU CDCC).

24 Les membres de la plateforme sont : le CCB, le SPF Affaires étrangères, la VSSE, l'OCAM, le Ministère public, le Collège des procureurs fédéraux, la Police fédérale, la Federal Computer Crime Unit, le Centre de crise National (NCCN), la Défense et le Commandement cyber.

pourront faire l'objet d'une enquête ultérieure.

17. Le projet de rapport de l’enquête de contrôle a été soumis au SGRS pour commentaires et demande de déclassification. Ces commentaires ont été prises en compte dans le présent rapport.

2.

FONDEMENT DE LA CREATION DU CYBER COMMAND (CYCOM)

18. Dans la Déclaration de politique du 4 novembre 2020, la ministre de la Défense de l'époque annonçait que la Défense allait considérablement renforcer sa capacité en matière de cyberdéfense, ce qui devait se traduire à terme par la création d'une composante à part entière. A cette fin, il conviendrait, dans un premier temps, de renforcer les capacités cyber au sein du SGRS, ce qui permettrait de mettre en place, à partir de cette capacité cyber, une véritable Composante cyber à un horizon de cinq ans, sans affaiblir la capacité de cyber-renseignement du SGRS.[25]

19. Une équipe de projet a été constituée à cet effet au sein de la Défense à la mi-2021. Cette équipe était chargée de mettre au point la nouvelle Composante cyber. Il en a résulté une cartographie de ce qui existait déjà en matière de capacité cyber au sein de la Défense belge et la mise en œuvre d'un *benchmark* international.[26]

20. Créé le 19 octobre 2022, le Commandement cyber du SGRS était à ce moment-là une fusion entre la direction Cyber du SGRS, le « Project Office Cyber & Influence », le service ELINT/SIGINT (anciennement « C3 »), le service OSINT/SOCMINT (anciennement « C5 ») et la plateforme « Information Warfare » (anciennement « PF10 »). Cet événement factuel n'a été formalisé que par la suite, à l'article 42 de l'A.R. du 30 juin 2025 fixant la structure générale du Ministère de la Défense et les attributions de certaines autorités.[27] Le seul document de base obtenu par le Comité R/I, datant de la création du Commandement cyber qui y faisait explicitement référence, est l'A.R. du 23 octobre 2022, déjà mentionné, portant nomination de l'ancien général-major VAN STYTHEM en tant que Commandant du Commandement cyber à compter du 19 octobre 2022.

21. Il ressort donc de la déclaration de politique susmentionnée que le développement d'un Commandement cyber au sein du SGRS poursuivait une double finalité. Premièrement, il

---

25 *Doc. parl.*, Chambre, 2020-2021, DOC 55 1610/017, p. 25.

26 *Doc. parl.*, Chambre, 2022-2023, DOC 55 3323/001, p. 4 (Audition du Commandant du Commandement cyber à la Commission de la Défense nationale le 1er mars 2023).

27 Voir *supra*. A cet égard, la ministre de la Défense déclarait dans son document de politique générale du 31 octobre 2022 : *« Les adaptations éventuelles à l'arrêté royal régissant l'organisation de la Défense et de son Etat-major suite à la mise en place du Cyber Command seront intégrées dans le cadre du projet de refonde de l'Etat-major»* (*Doc. parl.*, Chambre, 2022-2023, DOC 55 2934/020, p. 43).

devait renforcer la capacité cyber du SGRS afin de permettre à ce service de remplir ses missions dans le cyberespace, et, deuxièmement, il devait développer une véritable Composante cyber[28] sans compromettre la capacité (de renseignement) cyber du SGRS.

22. La note de politique de la Défense du 31 octobre 2023 indiquait que la création du Commandement cyber avait pour notamment pour objectif de contrôler le processus visant à atteindre les objectifs suivants : (1) renforcer la capacité cyber existante au sein du SGRS, (2) développer la recherche de talents et la formation, (3) initier l'innovation, la recherche et le développement technologique cyber, en lien avec la « Defense, Industry and Research Strategy (DIRS) », et accompagner le processus de développement de la nouvelle composante cyber. « *Le Cyber Command constitue dès lors le noyau de ce qui deviendra une Composante Cyber à part entière à la Défense* ».[29]

---

28 Voir également *Doc. parl.*, Chambre, 2022-2023, DOC 55 2934/020, p. 42 (note de politique de la Défense du 31 octobre 2022).

29 *Doc. parl.*, Chambre, 2023-2024, DOC55 3649/022, p. 45. Il est ressorti des entretiens menés au Comité que 2032 est la date butoir pour un « déploiement » complet.

3.
MISSION ET DOMAINES D'ACTIVITES DU CYBER COMMAND (CYCOM)

23. Les informations relatives à la mission et aux activités du Cyber Command (CyCom) sont disponibles dans plusieurs sources : les notes fournies par le Commandement cyber au Comité R/I, le site internet du Ministère de la Défense et du SGRS, les rapports des sessions parlementaires, la Stratégie Nationale Cyber, le *« SGRS – Rapport annuel 2024 »*, ainsi que quelques documents classifiés, parmi lesquels le *« Plan directeur 2023-2027 du SGRS*[30] *»*.

3.1. LES COMPETENCES DU COMMANDEMENT CYBER DANS LE PLAN DIRECTEUR 2023-2027

24. La partie opérationnelle du « Plan directeur du SGRS 2023-2027 » fait mention de la création d'un Commandement cyber et en décrit les compétences comme suit[31]:

« Le Cyber Command est investi d'une double responsabilité. D'une part, il assume les missions de renseignement et de sécurité du SGRS dans le cyberespace et le domaine électromagnétique. D'autre part, le Cyber Commander, en sa qualité de chef de la nouvelle composante cyber, endosse les rôles et les responsabilités d'une composante d'appui dans le domaine du cyberespace au profit des autres composantes et du reste de la Défense. A ce titre, la Cyber Composante est chargée de garantir la liberté de manœuvre des Forces Armées dans le cyberespace et de générer des cyber-effets militaires en appui des opérations de la Défense.

Ses tâches opérationnelles se résument en quatre points :

---

30 Le Plan directeur a été a été annoncé publiquement par la ministre de la Défense (*Doc. parl.*, Chambre, 2022-2023, DOC 55 2934/020, p. 32) : *« L'une des priorités identifiées était la préparation d'un Plan directeur pour le Service. Au début de cette année, le Plan directeur 2022 du SGRS a donc été mis en œuvre après avoir été présenté à la Chambre des représentants. Dans le prolongement de ce Plan, un Plan directeur pluriannuel pour la période est en cours de préparation et sera mis en œuvre au début 2023 »*.

31 La description des compétences a été reprise dans le Plan directeur classifié SECRET. A la demande du Comité R/I, le SGRS a accepté de le déclassifier.

- *« Conduct Cyber Operations » : Réaliser les missions du SGRS et appuyer celles des Forces Armées dans le cyberespace et le domaine électromagnétique. Celles-ci sont reprise dans les quatre volets du Cyber Operations Framework : Cyber Security Operations (PROTECT), Defensive Cyber Operations (DEFEND), Cyber Intelligence, Surveillance and Reconnaissance Operations (COLLECT & ANALYSE) and Cyber Offensive Operations (FIGHT).*

- *« Cyber readiness of the Forces » : Superviser la mise en condition et la préparation opérationnelle de l'ensemble de la Défense à pouvoir opérer dans le Cyberespace et le domaine électromagnétique ;*

- *« Readiness of the Cyber Forces » : Effectuer la mise en condition et la préparation opérationnelle des moyens cyber spécialisés du SGRS ; d'autres services, en dehors du Cyber Command, sont chargés de l'infiltration numérique par agents virtuels, de l'exploitation des données issues de l'interception téléphoniques sur le territoire national, des relations avec les opérateurs téléphoniques et de la collecte d'informations sur les réseaux sociaux à des fins d'enquêtes de sécurité ;*

- *« Homebase Support » : Conformément aux directives du Conseil National de Sécurité, se tenir prêt à mettre en œuvre les capacités Cyber du SGRS dans le cadre de missions d'aide à la Nation, notamment en cas de situation de crises nationales cyber. Le cas échéant, mettre ces capacités en œuvre. Cette tâche participe du renforcement de la résilience numérique de la Belgique et inclus, si nécessaire, l'appui aux opérateurs d'infrastructures critiques ».*

3.2. LES COMPETENCES DANS LE DETAIL

25. La capacité cyber du Commandement cyber permet l'exploitation du cyberespace au profit du SGRS et de la Défense et, dans certains cas, apporte un appui à la Nation. La capacité cyber relève, selon sa mission, de deux cadres juridiques différents : la loi organique des services de renseignement et de sécurité – dans ce cas, la responsabilité incombe au Commandement cyber du SGRS – ou au cadre juridique pour le déploiement des Forces armées belges – dans ce cas, c'est à la Force cyber que la responsabilité incombe.

26. Dans sa note de politique du 17 avril 2025, le ministre de la Défense a déclaré que le Commandement cyber continue de remplir ses missions de sécurité, notamment pour protéger le personnel de la Défense, les infrastructures de communication et les systèmes d'armes, ainsi que ses missions de renseignement (collecte et analyse) afin de maintenir une image précise des menaces étrangères ciblant la Belgique dans l'espace

électromagnétique, numérique et informationnel.[32]

27. En tant que Commandant du Commandement cyber, le lieutenant-général VAN STRYTHEM, qui était alors général-major, a énuméré les missions de son service à la Commission de la Défense nationale en ces termes : (1) exécuter des opérations dans le cyberespace (renseignement, sécurité, opérations défensives), (2) appuyer les autres composantes et activités (défensives ou offensives), et (3) renforcer la résilience nationale.[33]

28. Le Commandant du Commandement cyber a décrit les domaines d'activités comme suit : (1) action préventive[34], (2) surveillance active des réseaux, (3) collecte du renseignement, et (4) déploiement militaire (défensif et offensif, *cyber force protection*)[35].

29. Les missions du CyCom se basent dans une très large mesure sur la doctrine OTAN, qui est reprise dans la « *NATO Allied Joint Publication (AJP) – 3.20 Allied Joint Doctrine for Cyberspace Operation* ». Dans ce document, on retrouve notamment une définition du cyberespace, telle qu'utilisée par l'OTAN et donc aussi par le CyCom du SGRS. Cette définition s'énonce comme suit : *« Le domaine mondial constitué de tous les systèmes, réseaux et données de communication, d'information et autres systèmes électroniques interconnectés, y compris ceux qui sont séparés ou indépendants, qui traitent, stockent ou transmettent des données ».*[36]

30. Toujours selon la doctrine de l'OTAN, le cyberespace est constitué de trois « couches » : 1/ une couche physique, 2/ une couche logique, et 3/ une couche « cyber-persona » ou couche sociale, aussi appelée couche « virtuelle ».

    - La couche physique est liée à une localisation géographique et se compose d'éléments tangibles, tels que des ordinateurs, des serveurs, des routeurs, des hubs, des câbles et des équipements utilisés pour le stockage, le traitement et la transmission de données. La couche physique peut également inclure des systèmes d'armement et des infrastructures critiques.
    - La couche logique se compose d'éléments qui se manifestent sous la forme d'un code ou de données, tels que les systèmes d'exploitation, les protocoles ainsi que les composants logiciels et de données. La couche logique, avec la couche

---

32 *Doc. parl.*, Chambre, 2024-2025, DOC 56 0856/022, p. 11.

33 Notamment en ce qui concerne l'activation du plan de crise cyber du CCB et du Centre de crise National ; *Doc. parl.*, Chambre, 2022-2023, DOC 55 3323/001, p. 5 (audition par la Commission de la Défense nationale du 1er mars 2023 du Commandant du Commandement cyber).

34 Telles que l'homologation des réseaux, les directives relatives aux bonnes pratiques, la sensibilisation aux risques.

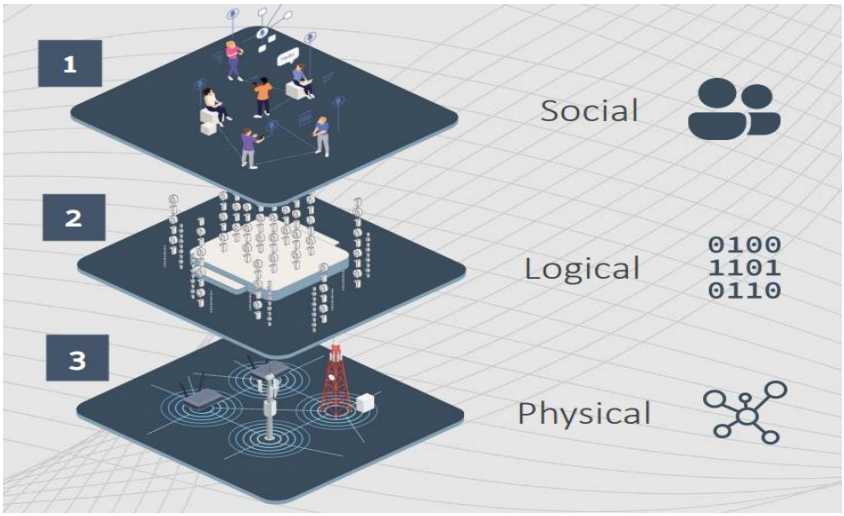
35 Notamment la protection des nouveaux systèmes d'armement interconnectés au travers des différentes composantes.

36 Traduction libre du « *NATO Allied Joint Publication (AJP) – 3.20 Allied Joint Doctrine for Cyberspace Operations* », p. 4.

physique, garantit la possibilité pour une personne cyber (cyber persona) de communiquer et d'agir.

- La couche « cyber-persona » ou couche sociale se compose d'éléments qui ne sont pas des personnes ou organisations réelles, mais une représentation de leur identité virtuelle. Une identité virtuelle peut consister en une adresse e-mail, une identification d'utilisateur, un compte sur les réseaux sociaux ou un pseudonyme. Une seule personne ou organisation peut donc avoir plusieurs « cyber-personas ». Inversement, plusieurs personnes ou organisations peuvent aussi créer une « cyber persona » partagée.

31. L'exécution d'opérations cyber se situe toujours dans la couche logique mais peut également se situer dans les deux autres couches.



32. Au sein des différentes « couches » du cyberespace, le Commandement cyber exerce les trois missions principales suivantes :[37]

    1/ PROTECT : afin de garantir la liberté d'action pendant les opérations militaires, la Défense doit protéger l'ensemble de ses communications et systèmes d'armement et d'information. L'optimisation de la sécurité et de la résilience de tous les systèmes nécessite une approche coordonnée à différents niveaux.

    2/ DEFEND : même la meilleure cybersécurité ne peut jamais exclure totalement le risque d'une cyberattaque réussie. La Défense doit disposer d'un ensemble de mesures robustes pour pouvoir réagir de manière adéquate aux incidents cyber et garantir la continuité de l'exécution des missions. C'est pourquoi la Défense développe en permanence ses capacités de détection, d'analyse et de remédiation, ainsi que d'attribution et de

[37] https://www.mil.be/fr/evolution-de-la-defense/protect-defend-collect-and-fight-in-cyberspace/

communication.

3/ COLLECT : la Défense continue d'étendre son expertise en matière de renseignement dans le cyberespace. L'accent est mis sur les capacités et les intentions des acteurs cyber dans les régions où elle est présente. Le Commandement cyber emploie des méthodes pour collecter des informations pertinentes sur les activités d'espionnage et de sabotage de nos adversaires.

4/ FIGHT: la capacité de renseignement peut également être utilisée pour préparer et appuyer des cyberattaques. Cela peut se faire en recherchant les vulnérabilités dans les systèmes de communication, d'information et d'armement de nos adversaires.

33. Les différentes composantes du Commandement cyber sont actives, en fonction de leur rôle spécifique, dans une ou plusieurs « couches » du cyberespace décrites ci-dessus et contribuent à l'exécution d'une ou plusieurs missions susmentionnées (*infra*).

4.
GESTION DE L'UNITE CYBER

34. La Loi Renseignement stipule que le pays dispose de deux services de renseignement et de sécurité : la VSSE, le service de renseignement et de sécurité civil, et le SGRS, le service de renseignement et de sécurité militaire.[38] Bien que la loi ne définisse pas explicitement ce qu'est un service de renseignement et de sécurité, ceci ressort clairement de la description légale des missions de renseignement et de sécurité dans les articles 7 L.R&S (VSSE) et 11 L.R&S (SGRS). Il découle de cette disposition l'interdiction légale pour le pouvoir exécutif de créer, tant *de iure* que *de facto*, de nouveaux services de renseignement et de sécurité.

35. Dans le cadre de la présente enquête de contrôle, il est important de noter que les Forces armées n'ont pas le pouvoir de créer, au sein du SGRS, un nouveau service de renseignement et de sécurité lequel, d'un point de vue juridique (par arrêté royal), ferait certes partie du service, mais serait *de facto* autonome compte tenu de la manière dont les structures de contrôle interne et les instruments de gestion seraient organisés au sein et à l'égard de la Force de combat et du SGRS (par exemple, les règles relatives à la hiérarchie, à l'évaluation, à la discipline, à la gestion du personnel, au budget).

36. Comme indiqué précédemment, l'AR Structure de la Défense stipule que le Commandement cyber est organisé au sein du SGRS.[39] Afin de vérifier si le Commandement cyber fait réellement partie du SGRS, le Comité a interrogé le service, son Chef et le Commandant cyber sur la structure de contrôle interne concrète et les instruments de gestion. Etant donné que le SGRS et le Commandement cyber sont tous deux dirigés par un officier supérieur du même grade, le Comité s'est demandé si le Chef du SGRS exerçait réellement un contrôle (suffisant) sur le Commandement cyber. Le Comité n'a constaté aucun problème à cet égard. La réponse circonstanciée qu'il a reçue à ses questions l'a dès lors pleinement convaincu de l'absence de violation de l'interdiction légale visée à l'article 2, § 1er L.R&S.

37. Les éléments suivants indiquent que le Commandement cyber fait partie du SGRS :

    - En ce qui concerne *les évaluations annuelles des deux directeurs du Commandement cyber* (à savoir la Direction Cyber Operations et la Direction Development & Readiness), le Commandement cyber est l'évaluateur concerné, mais un recours est

38 Art. 2, § 1er, al. 1er L.R&S.

39 Art. 42, al. 2, première phrase AR Structure de la Défense.

possible auprès du supérieur hiérarchique de l'évaluateur, c'est-à-dire le Chef du SGRS.[40] Leurs responsabilités sont détaillées dans le règlement DGHR-REG-EVAL-001 [41];

- Dans le cadre du *règlement disciplinaire pour le personnel militaire* [42], les sanctions sévères sont infligées en premier lieu par le Commandant du corps compétent à l'égard du militaire concerné. Au sein du Commandement cyber, cette fonction est remplie par les trois *unit commanders* (commandants d'unité), à savoir le chef de la CSCU, le chef de la DCOU et le chef de la DICU, ainsi que par les deux directeurs chargés des éléments restants au sein du Commandement cyber.[43] Si une intervention à un niveau supérieur du Chef de Corps est nécessaire, le Commandant cyber et, enfin, le Chef du SGRS sont impliqués dans une procédure disciplinaire ;[44]

- Les collaborateurs peuvent bénéficier d'une mobilité interne entre le SGRS et le Commandement cyber) ;[45]

- Le Chef du SGRS dispose de plusieurs instruments de pilotage vis-à-vis du Commandement cyber :

  — Au niveau individuel : voir ci-dessus les compétences du Chef du SGRS en matière de discipline et d'évaluation.
  — Le Chef du SGRS dispose d'autres instruments de pilotage [46] :
    - Le Plan directeur (pluriannuel) du SGRS dans lequel figure une partie consacrée au Commandant cyber ;
    - A l'instar des autres services au sein du SGRS, le Chef du SGRS donne des directives au Commandant cyber par le biais d'objectifs annuels ;
    - Les listes (annuelles) de ce que l'on appelle les « méthodes spéciales » (entre autres l'interception de communications à l'étranger) sont soumises au Chef du SGRS, qui peut donner des instructions ponctuelles ;
    - Toutes les deux semaines, le Chef du SGRS organise une réunion bilatérale avec le Commandement cyber afin de synchroniser le Commandement cyber relevant du SGRS et la Force cyber ;
    - Toutes les deux semaines, le Chef du SGRS organise une réunion bilatérale avec son Commandement, à laquelle sont notamment présents le

40 Note du SGRS adressée au Comité R/I n°25-00159405 du 1er octobre 2025, p.8.

41 Règlement DGHR-REG-EVAL-001 du 26 juillet 2023 « L'évaluation professionnelle du militaire » (ed. 1).

42 Règlement DGHR-REG-CARDI-001 du 15 juillet 2014 « Discipline » (ed. 1).

43 La description des tâches des services mentionnés sera abordée dans une section ultérieure.

44 Note du SGRS adressée au Comité R/I n°25-00159405 du 1er octobre 2025, p. 9 et Règlement DGHR-REG-CARDI-001, p. 25.

45 Note du SGRS adressée au Comité R/I n°25-00159405 du 1er octobre 2025, p.8.

46 Note du SGRS adressée au Comité R/I n°25-00159405 du 1er octobre 2025, P. 3, 7, 10 et 11.

Commandant cyber et les deux directeurs au sein du Commandement cyber. Le Chef du SGRS a la possibilité de donner ses instructions aux services concernés relevant de son autorité, y compris donc le Commandant cyber ;

- Le Chef du SGRS tient également une réunion bilatérale toutes les deux semaines avec, entre autres, le Directeur des Opérations Cyber, le Directeur Cyber Development & Readiness, ainsi que le Directeur Renseignements et le Directeur Sécurité ;
- Le Chef du SGRS reçoit des briefings *ad hoc* au début des opérations ainsi que des briefings actualisés fréquents sur les opérations en cours, desquelles font partie les opérations cyber commandées par le Commandement cyber. Le Chef du SGRS a la possibilité de donner des instructions ponctuelles ;
- Les outils utilisés au sein du SGRS pour l'attribution des dossiers prévoient une structure hiérarchique à suivre, dans laquelle le directeur est considéré comme la plus haute autorité. Cela permet au Commandant cyber de communiquer son avis au Chef du SGRS qui prend la décision finale ;
- En cas de conflit en matière de capacités cyber disponibles entre, d'une part, les besoins en informations du SGRS et, d'autre part, les besoins en informations de tiers (en l'occurrence la police fédérale, la VSSE), c'est le Chef du SGRS qui doit prendre la décision finale.

— Le Commandement cyber est situé dans le complexe immobilier du SGRS (avec le même contrôle d'accès) ;
— Cyber Intel est intégré comme plateforme dans le « collection management » du SGRS ;
— Le personnel du Commandement cyber participe au repas de corps du SGRS.

5.
SITUATION BUDGETAIRE

38. La réponse du SGRS aux questions posées par le Comité permet de conclure que la structure budgétaire de la Défense, du SGRS et de l'Unité cyber ne pose actuellement aucun problème pour l'intégration du Commandement cyber au sein du SGRS. Le Comité s'est en outre interrogé sur la situation budgétaire actuelle de la cybercapacité militaire, se demandant si celle-ci suffisait à répondre aux nombreuses attentes des autorités politiques et des acteurs militaires et civils concernés.

39. La décision prise par l'OTAN en 2016 lors du sommet de Varsovie de reconnaître [47], le cyberespace comme un domaine d'opération distinct, au même titre que la terre, l'air et la mer, justifie pleinement la décision du gouvernement de créer par voie réglementaire la Force cyber en tant que force opérationnelle et d'organiser le Commandement cyber en tant que section juridique distincte du SGRS. Une telle décision implique logiquement la responsabilité du gouvernement et du ministre de la Défense de mettre à disposition les ressources humaines, matérielles et financières nécessaires afin de développer de manière adéquate la cybercapacité militaire et de la mettre au service de la sécurité nationale et des engagements internationaux de la Belgique.

5.1. GENERALITES[48]

40. Dans sa réponse au Comité, le SGRS affirme que : « [l]e budget alloué est réparti au sein du Ministère de la Défense entre les différents organes et sous-sections, parmi lesquels tant le SGRS que les différentes forces : Terre, Air, Marine et Service médical et, depuis le 21 juillet, la Force cyber également. » (traduction libre). Et de poursuivre : « [l]e Commandement cyber reçoit une part fixe du budget de la Défense, qui est répartie en interne en fonction des besoins stratégiques et opérationnels. » (traduction libre).

41. A la question posée par le Comité quant à savoir qui décide en cas de conflit dans la gestion des capacités disponibles du Commandement cyber pour, d'une part, les missions du SGRS et, d'autre part, les missions de la Force cyber, le service répond :

    — « En tant que chef du Commandement cyber, le Commandant cyber a une ligne hiérarchique, via le Chef du SGRS, directement vers le Ministre. D'autre part, il a une ligne hiérarchique, via le CHOD, vers le Ministre. En théorie, ce sera donc à ce

47 En 2019, l'OTAN a reconnu l'espace comme étant le cinquième domaine d'opération.

48 Note du SGRS adressée au Comité R/I n°25-00159405 du 1er octobre 2025, p. 5, 6 et 12.

dernier de prendre une telle décision. » (traduction libre).

- Et « [d]ans la pratique, tous les moyens sont actuellement alloués au SGRS, c'est donc le Chef du SGRS qui décide des priorités. L'objectif est d'affiner les processus internes existants au sein de la Défense qui déterminent comment les capacités sont mises en œuvre au service du SGRS et/ou de la Force cyber et sur quels critères les priorités doivent être basées. » (traduction libre)

42. Tant dans la réponse écrite du SGRS que dans les entretiens oraux du Commandement cyber, il a été communiqué au Comité que l'intention était de recruter au sein de la Force cyber des membres du personnel qui seraient employés par les autres forces. Dans le rapport au Roi joint à l'Arrêté royal du 30 juin 2025, cela est formulé comme suit : « La Force cyber, qui fait partie des Forces armées, contrôle de manière cohérente des modules capacitaires décentralisés qui sont capables de remplir des missions militaires. » (traduction libre).

5.1. BUDGET CHIFFRE

43. Le SGRS ne dispose pas d'un budget spécifique (crédits de personnel, crédits de fonctionnement, crédits d'investissement). Les budgets du SGRS sont répartis dans le budget de la Défense dans les domaines suivants : personnel, opérations & formation, crédits d'investissement et de fonctionnement dans le cadre des ressources matérielles, crédits dans le cadre de la formation et crédits de fonctionnement résiduels.

44. Les données chiffrées relatives aux budgets du SGRS, du Commandement cyber et de la Force cyber ont été classifiés CONFIDENTIEL (Loi 11.12.1998).

6.
ORGANISATION EXTERNE DE L'UNITE CYBER

6.1. COMMANDEMENT CYBER *VS.* FORCE CYBER

45. En vertu de l'Arrêté royal fixant la structure générale du Ministère de la Défense, il existe au sein du SGRS un Commandement cyber (Cyber Command) qui agit dans le cyberespace et qui exerce des missions visées à l'article 11 de Loi du 30 novembre 1998 organique des services de renseignement et de sécurité.[49] Le Commandement cyber est dirigé par le Commandant cyber.[50]

46. Le SGRS dans son ensemble est constitué d'un Commandement général – composé du Chef du SGRS (C), du Chef adjoint du SGRS (DCOM), du Commissaire en chef (HCC) et du Commissaire en chef adjoint (HCC Adj) – ainsi que (des directeurs de) la direction Renseignements (Dir Rens), la direction Sécurité (Dir S), la direction Plans & Policy (Dir P&P) et la direction Appui (Dir Sp). Outre le Commandement général, il y a un Commandement cyber, dirigé par le Commandant cyber (CyC) et composé de la direction Cyber Operations (Dir Cy Ops) et de la direction Cyber Development & Readiness (Dir Cy D&R).

47. Lors des réunions de commandement (bimensuelles) – *de facto* le comité de direction du SGRS – le Chef du SGRS se réunit avec son adjoint, le Commissaire en chef et le Commissaire en chef adjoint, le Commandant cyber ainsi que les directeurs des directions citées.[51]

48. Il convient d'établir une distinction entre le Commandement cyber et la Force cyber (Cyber Force). Celle-ci est une des cinq forces de combat au sein des Forces armées belges.[52] A l'instar des autres forces, la Force cyber a son propre commandant.[53] Il est important de noter que le Commandant du Commandement cyber est également le Commandant de la

---

49 *Cf.* art. 42, al 1er A.R. du 30 juin 2025 fixant la structure générale du Ministère de la Défense et les attributions de certaines autorités (*M.B.* 15 juillet 2025; ci-après : AR Structure de la Défense).

50 Art. 42, al. 2, première phrase AR Structure de la Défense.

51 Note du SGRS adressée au Comité R/I n° 25-00159405 du 1er octobre 2025, p. 2 et 10.

52 Aux côtés de la Force terrestre, aérienne, de la Marine et du Service médical (*cf.* art. 1er, al. 1er, 5° AR Structure de la Défense).

53 Art. 37, deuxième phrase AR Structure de la Défense.

Force cyber.[54] Dans les Forces armées belges, la fonction de chef de l'organe d'exécution cyber du service militaire de renseignement et de sécurité et la fonction de chef de la force chargée du cyberespace sont donc réunies en une seule et même personne.

49. D'un point de vue juridique, le Commandement cyber et la Force cyber sont deux entités distinctes au sein des Forces armées. Ce n'est pas le cas du point de vue organisationnel. Il existe une structure hiérarchique unique, avec un seul responsable, qui exerce à la fois la fonction d'organe d'exécution au sein du service militaire de renseignement et de sécurité ainsi que d'une des forces de combat et qui exerce toutes les missions concernées. Au sein de cette unité, il n'existe pas non plus de départements distincts chargés des missions du SGRS ou des missions de la Force cyber. Il existe une organisation unique au sein de laquelle tous les membres du personnel sont (doivent être), le cas échéant, au service des deux fonctions.

50. Dans la pratique, cette double fonction peut parfois être source de confusion. A titre indicatif, même sur le site internet du Ministère de la Défense, la Force cyber est présentée comme suit : « *Cyber Force is part of ACOS IS* ».[55] Mais cette affirmation n'est pas du tout correcte. La Force cyber est en effet une des cinq forces de combat et ACOS IS un des quatre départements d'état-major.[56] Une affirmation correcte serait que « *Cyber Command is part of ADIV/SGRS* ».

51. La double fonction du Commandant cyber a des conséquences tant sur les structures de l'autorité en place à l'égard de l'unité que sur l'exécution des tâches et sur le cadre juridique applicable. L'unité agit en tant qu'organe d'exécution du SGRS, elle relève de la hiérarchie directe du Chef du SGRS, qui relève à son tour de l'autorité directe du ministre de la Défense en ce qui concerne l'exécution des missions de renseignement et de sécurité.[57] Si l'unité agit comme Force cyber, elle est placée sous l'autorité directe du Chef de la Défense.[58] Selon la fonction en vertu de laquelle l'intervention a lieu, il existe donc d'autres lignes de commandement pour l'Unité cyber et, partant, d'autres autorités publiques auxquelles le Commandant cyber doit rendre des comptes.

---

54 Art. 42, al. 2, deuxième phrase AR Structure de la Défense.

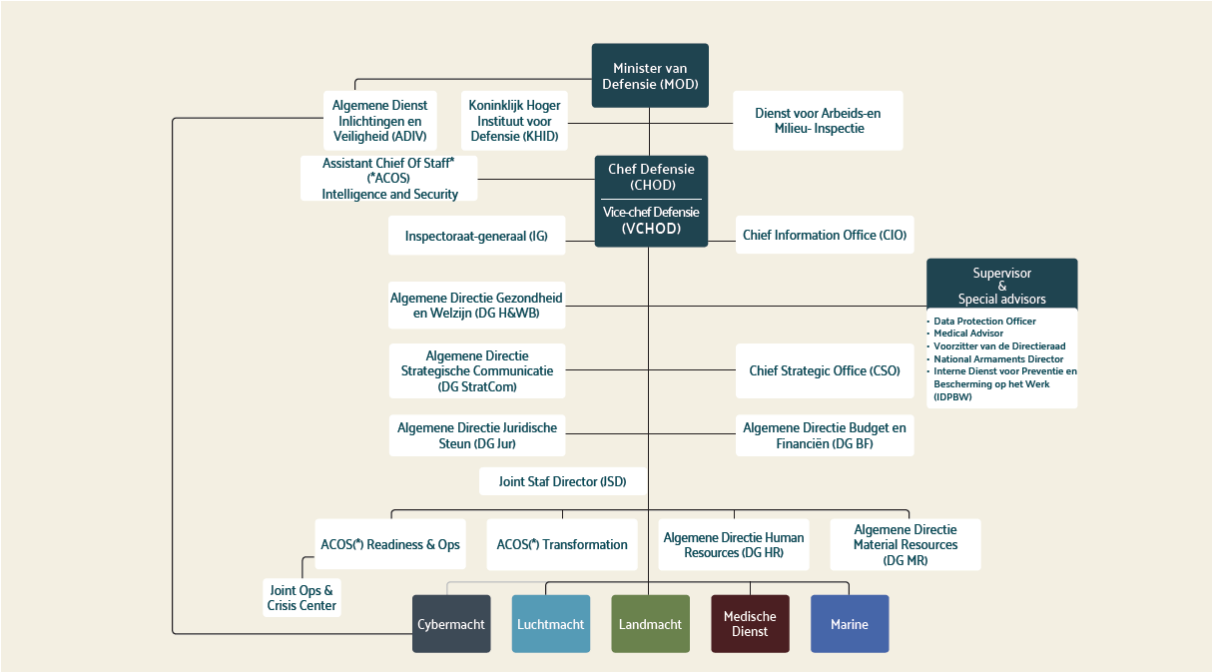
55 www.mil.be/fr/a-propos-de-la-defense/ (consultation le 20 octobre 2025).

56 Les erreurs sont compréhensibles. Dans la pratique, il n'y a en effet aucune différence entre, d'une part, la Force cyber et le Commandement cyber, et, d'autre part, entre le SGRS et ACOS IS.

57 Il convient de mentionner que le Chef du SGRS a également la qualité de sous-chef d'état major renseignements et sécurité (ACOS IS) et qu'à ce titre, il relève directement du Chef de la Défense.

58 *Cf.* art. 6, § 1er, al. 1er, *in limine* et 4° et art. 7, § 3, al. 2 AR Structure de la Défense.

Schéma du Ministère de la Défense[59]



52. Cela montre clairement que le cadre juridique et la fonction à partir desquels l'Unité cyber exerce ses activités et ses tâches ont leur importance. La délimitation des missions entre le Commandement cyber (c'est-à-dire les missions du SGRS dans le cyberespace) et la Force cyber, détermine, dans un cas concret, le lien hiérarchique qui existe vis-à-vis de l'autorité et la responsabilité qui en découle pour le Chef du SGRS, le Chef de la Défense et le ministre de la Défense.

53. En tant qu'organisation, l'unité exerce deux catégories de missions : les activités dans lesquelles l'unité intervient en tant que section du SGRS, et donc en tant qu'organe d'exécution du service militaire de renseignement et de sécurité (ci-après : les missions du Commandement cyber), et les activités dans lesquelles elle intervient comme Force cyber, et donc comme une des forces de combat belge (les missions de la Force cyber). Les missions du Commandement cyber sont régies par la Loi Renseignement[60] et par la Loi Classification.[61] Les missions de la Force cyber sont quant à elles régies par l'Arrêté royal qui organise le Ministère de la Défense (AR Structure de la Défense) ainsi que par la Loi Mise en œuvre et Mise en condition Défense et ses arrêtés d'exécution.[62] Pour ces deux

59 Source : https://www.mil.be/fr/a-propos-de-la-defense/#

60 Loi du 30 novembre 1998 organique des services de renseignement et de sécurité.

61 Loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé (L. C&HS)

62 Loi du 20 mai 1994 relative aux périodes et aux positions des militaires du cadre de réserve, ainsi qu'à la mise en oeuvre et à la mise en condition des Forces armées (*M.B.* 21 juin 1994 ; ci-après : Loi Mise oeuvre et Mise en condition Défense) et l'A.R. du 6 juillet 1994 portant détermination des

types de missions, il convient de se référer dans une large mesure à la réglementation de l'OTAN, aux documents politiques et doctrinaux[63] en vue d'obtenir des explications et des précisions supplémentaires.[64, 65]

54. Il existe des raisons valables d'intégrer le Commandement cyber au sein du SGRS. En tant que section du service militaire de renseignement et de sécurité, une unité peut en effet exploiter pleinement l'espace dont dispose le SGRS dans le cadre des missions et compétences qui lui sont légalement attribuées. Ce sont surtout les possibilités en matière de méthodes particulières de renseignement (p. ex. *legal hackings*, demande de métadonnées) et d'activités SIGINT (p. ex. le droit d'avoir recours à des opérateurs de télécommunications dans le cadre de l'interception de communications à l'étranger) qui sont nécessaires pour assurer un travail de renseignement numérique efficace. Les missions du SGRS dans lesquelles le Commandement cyber a un rôle à jouer sont énumérées ci-dessous.

6.2. MISSIONS DU COMMANDEMENT CYBER

6.2.1. Missions de renseignement, y compris dans le cyberespace

55. Le SGRS a pour missions de renseignement suivantes, y compris dans le cyberespace :

(a) de rechercher, d'analyser et de traiter le renseignement relatif à toute activité qui menace ou pourrait menacer l'intégrité du territoire national ou la population, les plans de défense militaires, le potentiel scientifique et économique en rapport avec les acteurs liés à la Défense,

---

formes d'engagement opérationnel, d'assistance et d'appui militaire et des activités préparatoires en vue de la mise en œuvre des forces armées (*M.B.* 20 juillet 1994; ci-après : AR Mise en œuvre et Mise en condition Défense).

63 La « Allied Joint Publication (Doctrine) » (AJP) de l'OTAN est une série de publications qui définissent la doctrine et les principes fondamentaux des opérations conjointes. Les éléments clés sont l'APJP 1, qui reprend la doctrine globale de toutes les opérations conjointes. Il définit le contexte stratégique et les principes de base des opérations conjointes. Et l'AJP-6, qui décrit la doctrine des opérations au niveau opérationnel, y compris la coordination entre les différentes entités.

64 Le document OTAN AJP-2 (Allied Joint Doctrine for Intelligence, Counterintelligence and Security) est la pierre angulaire de la doctrine de l'OTAN en matière de renseignement. Il fournit les lignes directrices et principes fondamentaux pour le renseignement dans le cadre des opérations conjointes. Plusieurs publications subsidiaires sont plus détaillées, par exemple (1) au niveau Joint Functional Doctrine : AJP-2.1 Intelligence Procedures, AJP-2.2 CI & Security Procedures, AJP-2.3 HUMINT, AJP-2.4 SIGINT, AJP-2.7 JISR, et (2) à un niveau encore plus détaillé (Level-3-Intel Publications) : AInP-16 IRM&CM, AInp-10 Technical Exploitation, AInP-5 HUMINT TTPs, AInP-10 Technical Exploitation, AInP-14 JISR TTPs.

65 D'autres documents AJP plus détaillés sont notamment : AJP-10.1 (Information Operations) et AJP-3.20 (Cyberspace Operations), AJP-3.6(B) (Electronic Warfare).

l'accomplissement des missions des Forces armées ou la sécurité des ressortissants belges à l'étranger, et d'en informer sans délai les ministres compétents.[66]

Le champ de compétences du SGRS dans le cadre de cette partie de la mission de renseignement est déterminée par les intérêts à protéger combinés aux menaces à maîtriser. En d'autres termes, pour déterminer si le service de renseignement militaire est compétent dans un cas concret, il convient de vérifier s'il existe un lien avec au moins un intérêt et au moins une menace.

(b) de rechercher, d'analyser et de traiter le renseignement relatif aux facteurs qui influencent ou peuvent influencer la sécurité nationale et internationale dans la mesure où les Forces armées sont ou pourraient être impliquées, en fournissant un soutien en renseignement à leurs opérations en cours ou à leurs éventuelles opérations à venir, et d'en informer sans délai les ministres compétents.[67]

L'objectif de cette partie de la mission de renseignement, appelée « soutien aux opérations militaires », consiste à protéger les troupes et à appuyer leurs propres opérations[68], en collectant et en traitant des informations sur les puissances étrangères, les forces régulières ennemies ou potentiellement ennemies (ou des éléments de celles-ci), des parties combattantes irrégulières et des zones et des circonstances dans lesquelles des opérations sont menées ou pourraient être menées à l'avenir.[69]

(c) de rechercher, d'analyser et de traiter le renseignement relatif aux activités des services de renseignement étrangers sur le territoire belge.[70]

Le SGRS, tout comme d'ailleurs la Sûreté de l'Etat (VSSE), est chargé de surveiller les différents types d'activités des services de renseignement étrangers sur le territoire belge. Le législateur oblige les deux services à conclure un accord de coopération en la matière sur la base des directives du Conseil National de Sécurité (CNS).[71] Dans le Plan Stratégique National du Renseignement (PSNR) de 2022, le CNS a décidé, sur proposition conjointe de la VSSE et du SGRS, que les actions des services de renseignement étrangers contre les intérêts belges seraient traitées de manière transversale, indépendamment de l'origine de

---

66 Art. 11, § 1er, 1°, deuxième partie, et § 2, 1° à 4° L.R&S.

67 Art. 11, § 1er, 1°, première partie L.R&S.

68 *Doc. parl.* Chambre 2015-2016, n°. 54-2043/001, 8, p. 31 à 33.

69 Dérivée de la définition de l'OTAN de la notion d'« intelligence », c'est-à-dire : *« The product resulting from the processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organisations engaged in such activity. »* AAP-6 (ed. 2009) « NATO Glossary of Terms and Definitions ».

70 Art. 11, § 1er, 5° L.R&S.

71 Art. 20, § 4 L.R&S.

la menace (militaire ou civile) ou de la cible (militaire ou civile).[72]

6.2.2. Missions de sécurité, y compris la cybersécurité

56. Le SGRS est également chargé par le législateur de plusieurs **missions de sécurité, y compris de cybersécurité** :

(a) de veiller au maintien de la sécurité militaire :

- la sécurité du personnel, des installations, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires;[73]
- l'appui sécuritaire aux opérations militaires.[74]

Dans ce contexte, le Règlement IF5 « Instruction sur la Sécurité Militaire » du 26 septembre 2023, émanant du SGRS, revêt une importance particulière. Ce règlement comprend toutes les directives relatives à la sécurité militaire au sein du Ministère de la Défense, y compris les directives relatives à la cybersécurité/sécurité de l'information.

(b) de protéger le secret militaire :

- la protection du secret lié aux installations militaires, armes et systèmes d'armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires, aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le ministre de la Défense gère.[75]

Le rapport au Roi joint à l'AR Structure de la Défense indique que le Commandement cyber a un rôle à jouer dans *« l'octroi des accréditations nécessaires et la réalisation de visites de contrôle afin de protéger le secret des systèmes informatiques et de communications militaires ou ceux que le ministre de la Défense gère conformément à l'article 11, § 1er, 3°, de la même loi »*.[76](traduction libre)

---

72 Plan National Stratégique de Renseignement 2022 (CONFIDENTIEL Loi 11.12.1998), p. 10., autorisation de déclassification.

73 Art. 11, § 1er, 2°, première partie L.R&S.

74 Art. 11, § 1er, 2°, première partie L.R&S, à comparer avec l'art. 21, 1° AR Structure de la Défense (*a contrario*).

75 Art. 11, § 1er, 3° L.R&S. L'ajout de « systèmes d'armes » se fait par analogie avec l'art. 11, § 1er, 2°, première partie L.R&S.

76 Le Comité constate que, curieusement, le rapport au Roi joint à l'A.R. du 30 juin 2025 n'a pas été publié au Moniteur. Toutefois, le texte en question a été intégralement transmis au Comité et a été fréquemment cité dans la réponse du SGRS aux questions posées par le Comité (*Cf.* note du SGRS adressée au Comité R/I n°25-00159405 du 1er octobre 2025).

(c) d'agir en tant qu'autorité de sécurité compétente en ce qui concerne la Défense en :

- octroyant des habilitations de sécurité et des autorisations pour des installations physiques, des systèmes de communication et d'information et des produits cryptographiques, ainsi qu'en effectuant des contrôles et des inspections[77];
- délivrant un avis de sécurité pour les (candidats) membres du personnel de la Défense.[78]

Le Commandement cyber n'a légalement aucune compétence dans le cadre de l'octroi en tant que tel des habilitations, autorisations ou avis susmentionnés. Il peut toutefois être sollicité dans le cadre des enquêtes ou vérifications préalables, ainsi que dans le cadre des contrôles ou inspections *a priori* ou *a posteriori*.

(d) d'effectuer des *screenings* de sécurité :

- enquêtes de sécurité préalables à l'évaluation relative à l'octroi d'une habilitation de sécurité [79];
- vérifications de sécurité, préalables à la délivrance d'un avis de sécurité (p. ex. pour des candidats militaires).[80]

6.2.3. Missions cyber spécifiques

57. Enfin, en plus de l'exécution susmentionnée des missions de renseignement et de sécurité dans le cyberespace, le SGRS est chargé des **missions cyber spécifiques** suivantes :

(a) neutraliser, dans le cadre du maintien de la sécurité militaire, une cyberattaque de systèmes informatiques et de communications ou de ceux que le ministre de la Défense nationale gère, [de] neutraliser l'attaque et [d']en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit international.[81]

Le rapport au Roi joint à l'AR Structure de la Défense stipule explicitement que le Commandement cyber a un rôle à jouer dans *« l'identification, l'entrave, la neutralisation de la cybermenace, et, en dernier recours, la contre-attaque en vue d'assurer la protection des réseaux informatiques et des systèmes d'armes que le ministre de la Défense gère ainsi que d'autres réseaux dans le cadre d'une crise nationale de cybersécurité, conformément aux articles 11, § 1er, 2°, 2°/1 et 44/1 de la même loi »* (traduction libre). Le caractère récent de l'arrêté royal concerné – qui établit juridiquement tant le Commandement cyber que la

77 Art. 1*bis*, 14°, c), et 1er*quinquies*, al.2 L.C&HS.

78 Art. 40 et s. L.C&HS.

79 Art. 11, § 1er, 4° L.R&S *juncto* art. 1er*bis*, 9° et 10°, en art. 18, al. 1er L.C&HS.

80 Art. 11, § 1er 6° L.R&S *juncto* art. 23° et 24°, et art. 32, § 1er, 2° L.C&HS.

81 Art. 11, §1er, 2°, deuxième partie L.R&S.

Force cyber – permet de déduire que le ministre de la Défense attribue cette mission spécifiquement au Commandement cyber.

Cette mission s'inscrit à la fois dans le cadre de la mission de sécurité (à savoir neutraliser une cyberattaque) et dans celui de la mission de renseignement (à savoir identifier les auteurs de la cyberattaque). Le législateur a jugé nécessaire de donner le droit au SGRS de contre-attaquer face à une cyberattaque aux fins de protection de la sécurité militaire.[82] Comme l'indique le terme juridique, il s'agit d'une contre-attaque. La nature de la contre-attaque implique que l'action cyber menée par le SGRS soit ponctuelle et réactive et qu'elle soit limitée dans le temps à compter du moment où elle débute. En ce qui concerne la contre-attaque, il s'agit également d'une activité qui consiste à neutraliser l'attaque initiale et à en identifier l'auteur. Le pouvoir de contre-attaquer est clairement un corollaire des activités de renseignement et de sécurité du SGRS dans le cyberespace. Du point de vue des possibilités offensives cyber de la Défense, la possibilité de contre-attaquer ne concerne toutefois qu'un aspect limité. Les missions et compétences offensives proprement dites n'appartiennent d'ailleurs pas au SGRS, mais à la Force cyber (*infra*).

(b) neutraliser, dans le cadre d'une crise nationale de cybersécurité, une cyberattaque de systèmes informatiques et de communications que le ministre de la Défense ne gère pas et [d']en identifier les auteurs, sans préjudice du droit de réagir immédiatement par une propre cyberattaque, dans le respect des dispositions du droit international.[83]

Une crise nationale de cybersécurité est un événement lié à la cybersécurité qui, en raison de sa nature ou de ses conséquences : (1) menace les intérêts vitaux du pays ou les besoins essentiels de la population (notamment la sécurité, la tranquillité et la santé publiques ; le potentiel scientifique et économique du pays ; la souveraineté nationale et les institutions établies par la Constitution et les lois ; et l'intégrité du territoire national[84]), (2) nécessite une prise de décision urgente et (3) requiert la coordination des efforts de différents départements et organismes.[85] Les activités du SGRS – et donc du Commandement cyber – dans ce cadre doivent être considérées comme un appui de la Défense à la Nation.[86]

82 Cette compétence a été attribuée via l'art. 4 Loi MRD du 4 février 2010.

83 Art. 11, § 1er, 2°/1 L.R&S.

84 *Doc. Parl.*, Chambre 2021-2022, n° 55-2706/001, 13.

85 Art. 11, § 2, 5° L.R&S.

86 *Doc. parl.*, Chambre 2021-2022, n° 55-2706/001, p. 11 et 14.

6.2.4. Pouvoirs (d'enquête)

58. Le SGRS dispose d'un large éventail de **pouvoirs (d'enquête)** pour mener à bien ses missions. Outre les pouvoirs d'enquête généraux (ce que l'on appelle les méthodes de renseignement ordinaires, spécifiques et exceptionnelles), qui correspondent à ceux de la VSSE, le législateur a également attribué au SGRS des pouvoirs spécifiques en vue d'obtenir des informations bien précises. Ainsi, dans le cadre de l'exécution de ses missions, le SGRS peut détecter, intercepter, écouter et prendre connaissance de toute forme de communication émise ou reçue à l'étranger, et il peut l'enregistrer (art. 44 L.R&S). Le SGRS dispose également de la possibilité de pénétrer dans un système informatique situé à l'étranger (art. 44/1 L.R&S).[87] Dans la pratique, ces méthodes sont également appelées méthodes *spéciales* de recueil de données.

59. Comme indiqué précédemment, tout cela amène le Comité à conclure que le travail de renseignement cyber effectué par les capacités cyber attribuées aux Forces armées, la cybersécurité du Ministère de la Défense et l'exécution opérationnelle de certaines opérations cyber ne peuvent s'inscrire en dehors du cadre juridique du SGRS.[88]

60. Ce cadre juridique impose également des restrictions légales strictes quant aux missions et compétences que le gouvernement peut attribuer à la Force cyber par voie réglementaire. Une attribution qui, selon le Comité, est toutefois nécessaire. Le flou qui entoure la délimitation des missions du Commandement cyber et de la Force cyber, et la confusion qui en résulte, créent une incertitude quant à la délimitation des pouvoirs et des responsabilités respectifs du ministre de la Défense et du Chef de la Défense en tant qu'autorités compétentes.

61. Une disposition réglementaire devrait également préciser quelles instructions le sous-chef d'état-major mise en condition et opérations (ACOS R&O) peut confier à la Force cyber. En vertu de l'article 15, 3°, de l'AR Structure de la Défense, ACOS Ops exerce en effet le commandement opérationnel des unités des Forces armées, et donc également de la Force cyber. Cela signifie que *« un déploiement opérationnel des capacités pour l'exécution des missions des forces de combat s'effectue sous la direction de l'état-major Readiness & Operations et, en substance, le Commandant de la Force cyber n'exerce plus d'autorité hiérarchique directe à ce moment-là. Il en va de même pour toutes les autres capacités des Forces de combat (terre, air et marine) »* (traduction libre).[89]

---

87 Ces trois pouvoirs d'enquête ne peuvent pas être utilisés dans le cadre d'une enquête de sécurité.

88 Il s'agit en particulier des missions légales du SGRS (art. 11 L.R&S), des méthodes de renseignement ordinaires et particulières (art. 14 à 18/17 L.R&S), des compétences SIGINT (art. 44 à 44/2 L.R&S) et des compétences en matière de transmission de renseignements (art. 19 L.R&S et L.C&HS). En ce qui concerne la mise en oeuvre de certaines opérations cyber, il s'agit des missions cyber spécifiques qui ont été légalement confiées au SGRS (art. 11, §§2° et 2°/1 L.R&S).

89 Note du SGRS adressée Comité R/I n°. 25-00159405 du 1er octobre 2025, p. 15.

6.3. MISSIONS DE LA FORCE CYBER

62. Conformément à l'article 38 de l'AR Structure de la Défense, « [l]es commandants des forces – et donc aussi la Force cyber – sont spécifiquement responsables de la mise en condition de leurs capacités respectives avec le personnel, le matériel, l'infrastructure et les moyens d'entraînement qui leur sont attribués. Ils sont également responsables de la mise en œuvre de leurs capacités respectives, en y incluant les capacités interforces qui leur ont été attribuées, et ce en appui de la mise en condition des Forces armées [...] ».

63. Le Comité constate que, comme c'est le cas pour les autres forces de combat, ni l'AR Structure de la Défense ni la Loi Mise en œuvre et Mise en Condition Défense ou son arrêté d'exécution ne contiennent une énumération concrète des missions spécifiques de la Force cyber. Dans un sens, c'est compréhensible. La loi et l'arrêté d'exécution précités contiennent déjà, en termes généraux, les différentes formes d'engagement opérationnel, d'aide et d'assistance militaires, ainsi que les activités de préparation en vue de la mise en œuvre des Forces armées. En outre, il incombe aux commandants des forces concernées, et donc aussi au Commandant cyber, d'en poursuivre l'élaboration. Ceci est également précisé de manière ad hoc et concrète sous la direction du sous-chef d'état-major mise en condition et opérations. Comme indiqué précédemment, pour mener des opérations, le chef d'état-major concerné dispose, en effet, du commandement opérationnel sur les unités et les forces[90], et donc aussi de la Force cyber.

64. Le Commandant cyber donne, entre autres, les détails suivants : « La Force Cyber s'inscrit dans la continuité de l'unité Cyber Command par le déploiement de cyber-combattants au sein des autres Forces. Ils allieront l'expertise cyber à la connaissance du métier et à la connaissance opérationnelle spécifique à chaque Force bénéficiant de l'appui cyber. Progressivement, les capacités opérationnelles terrestre, aérienne, marine et médicale seront renforcées pour assurer la protection, la défense, le renseignement et le combat dans le cyberspace selon les spécificités individuelles de ces Forces et services.».[91]

90 Art. 15, 3° AR Structure de la Défense.

91 Général-major Ciparisse, « Grille de lecture de la menace cybernétique à travers la mise en place de la Force Cyber belge », Wetenschap en technologie, 23 september 2025.

65. Dans le même temps, on ne peut ignorer le fait que cette interprétation n'est pas suffisante, d'autant plus que la Force cyber ne peut être entièrement assimilée aux autres forces. La Force cyber est la seule force dont le commandant est également le commandant d'un organe d'exécution d'une autre partie des Forces armées. Compte tenu de la délimitation claire des responsabilités du Chef du SGRS (autorité directe sur le Commandement cyber) et du Chef de la Défense (autorité directe sur la Force cyber), une description claire des tâches de la Force cyber s'impose (en l'occurrence dans l'AR Structure de la Défense). Le Comité rappelle à cet égard que le sous-chef d'état-major renseignements et sécurité a également obtenu une description claire de ses tâches dans l'arrêté royal concerné, précisément parce que le Chef du SGRS a également la qualité de sous-chef d'état-major renseignements et sécurité et compte tenu de la confusion possible entre les tâches du SGRS et celles d'ACOS IS en ce qui concerne l'appui sécuritaire et en matière de renseignement aux opérations militaires (art. 21, 1° AR Structure de la Défense). Les responsabilités du Chef de la Défense et du ministre de la Défense requièrent notamment une délimitation claire des tâches entre les deux.

66. Pour l'application des statuts du personnel, du recrutement et de la représentation dans certains organes, chaque membre du personnel militaire appartient, selon le cas, à la Force terrestre ou aérienne, à la Marine, au Service médical ou fait partie du personnel civil.[92] Chaque membre du personnel militaire est ainsi lié à une force déterminée. Il n'existe toutefois pas de catégorie « Force cyber » pour l'application des règlements susmentionnés. Un tel choix est légal et légitime, mais a logiquement aussi des conséquences sur la position et l'organisation de la Force cyber au sein de la Défense.

67. Bien que l'AR Structure de la Défense ne contienne pas de description spécifique de la Force cyber, il énumère les différentes compétences dont est chargé le Commandant cyber, en tant que commandant d'une force de combat, et qui sont communes à tous les commandants au niveau stratégique au sein des Forces de combat[93] :

68. Dans son domaine de compétence relatif à la Force cyber, le Commandant cyber est ainsi chargé des tâches génériques suivantes :

- conseiller le Chef de la Défense, lui fournir à cette fin des données et des informations lui permettant de proposer une politique de défense cohérente au ministre de la Défense
- développer, dans le cadre de la politique définie, la planification, la programmation pour la mise en condition et les directives générales de fonctionnement des Forces armées, en concertation avec les sous-chefs d'état-major, les directeurs généraux,

92 *Cf.* art. 1er, al. 3 AR Structure Défense.

93 Les pouvoirs génériques sont ceux qui sont attribués au Vice-chef de la défense, au directeur état-major interforces, au sous-chef du personnel, aux directeurs généraux, aux autres commandants des forces et à l'inspecteur général.

les commandants des autres forces et l'inspecteur général ;[94]

- fournir un appui au directeur état-major interforces, aux sous-chefs d'état-major, aux directeurs généraux, aux commandants des autres forces et à l'inspecteur général dans la gestion de la qualité et des risques spécifiques à leurs domaines de compétence ;
- rendre compte au Chef de la Défense de la maturité de son système de gestion de la qualité et des risques spécifiques à ses domaines de compétence, conformément à la politique et aux objectifs de la Défense ;
- fournir au Vice-chef de la Défense, au directeur état-major interforces, aux sous-chefs d'état-major, aux directeurs généraux, aux commandants des autres forces et à l'inspecteur général les données et informations qui leur permettent d'exercer leurs compétences respectives [95];
- assurer la production, la collecte et l'exploitation des informations de gestion et d'évaluation relatives aux processus et aux objectifs de gestion[96] relevant de ses domaines de compétence ;
- élaborer les projets d'accords relevant de ses domaines de compétence respectifs et veiller au respect, d'une part, des accords conclus au nom ou pour le compte du département et, d'autre part, des accords internationaux ratifiés par la Belgique.[97]

69. Au sein de la Force cyber, le commandant cyber a les tâches génériques suivantes :

- mettre en œuvre la politique du directeur état-major interforces, des sous-chefs d'état-major, des directeurs généraux, des commandants des autres forces et de l'inspecteur général applicable à son service ;
- intégrer la gestion de la qualité et des risques dans le cycle de planification, de gestion et de fonctionnement interne, pour toutes les politiques applicables à son service, conformément à la politique et aux objectifs du département ;
- assurer la production, la collecte et l'exploitation des informations de contrôle et d'évaluation pour son service ;
- formuler des avis et des recommandations sur les besoins et les moyens alloués à l'exécution de sa mission ;

---

94 Le sous-chef d'état-major renseignements et sécurité le fait après avoir consulté le directeur état-major interforces, tout comme le sous-chef d'état-major mise en condition et opérations, le sous-chef d'état-major transformation, le directeur général *human resources*, le directeur général *material resources* et les autres commandants des forces.

95 Cette disposition crée une obligation d'information pour ACOS IS à l'égard de certains commandants au sein des Forces armées, même en ce qui concerne les informations traitées dans le cadre des missions de renseignement du SGRS (*cf*. art. 10, § 1er, 5° AR Structure de la Défense *juncto* art. 10, 11 en 13, § 1e L.R&S).

96 Tels que visé dans l'A.R. du 15 mai 2022 relative à la maîtrise de l'organisation au sein de certains services du pouvoir exécutif fédéral (*M.B.* 17 juin 2022).

97 Art. 10, § 1er AR Structure de la Défense.

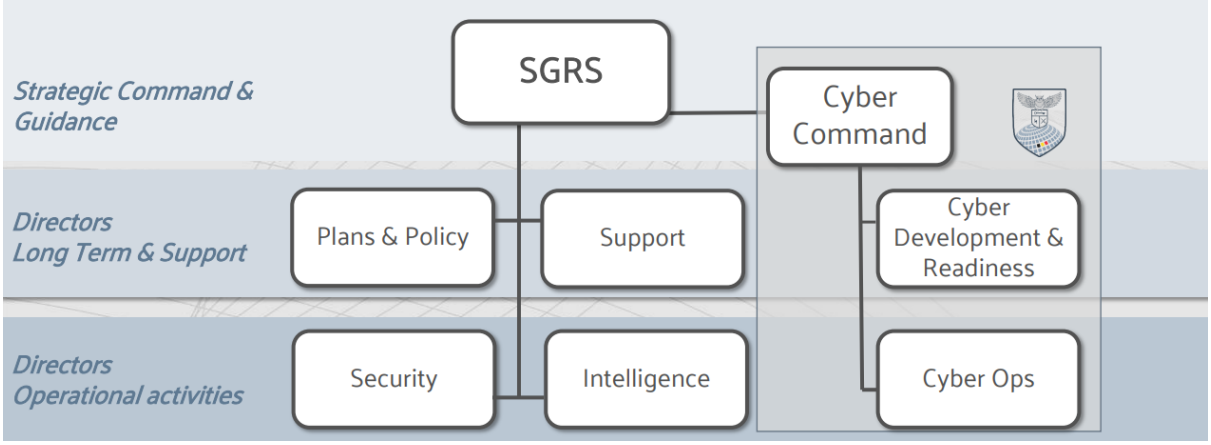
- assumer la responsabilité des ressources humaines, matérielles et budgétaires qui lui sont attribuées.[98]

70. En conclusion, à la question posée par le Comité au SGRS de savoir qui décide en cas de conflit dans la gestion des capacités cyber disponibles au profit, d'une part, des missions du SGRS et, d'autre part, des missions de la Force cyber, le SGRS a répondu que « [d]ans la pratique, tous les moyens sont actuellement alloués au SGRS, c'est donc le Chef du SGRS qui décide des priorités. L'objectif est d'affiner les processus internes existants au sein de la Défense qui déterminent comment les capacités sont mises en œuvre au service du SGRS et/ou de la Force cyber et sur quels critères les priorités doivent être basées. » (traduction libre). Le Comité approuve sans réserve ces directives. Cela n'enlève rien à la nécessité d'établir un cadre réglementaire qui clarifie la description des tâches de la Force cyber . Un tel cadre réglementaire est indispensable pour déterminer la manière dont les capacités concernées peuvent être réparties entre les activités et les tâches concrètes.

98 Art. 10, § 2 AR Structure de la Défense.

7.
ORGANISATION INTERNE DE L'UNITE CYBER

71. Le Cyber Command ou Commandement cyber (CyCom) est totalement intégré au sein du Service Général du Renseignement et de la Sécurité (SGRS). L'aperçu de la structure du CyCom est basé sur cinq briefings qui ont été donnés au Comité R/I, à sa demande, par des collaborateurs du CyCom, en mai et juin 2025, ainsi que sur un document classifié datant de juin 2025.

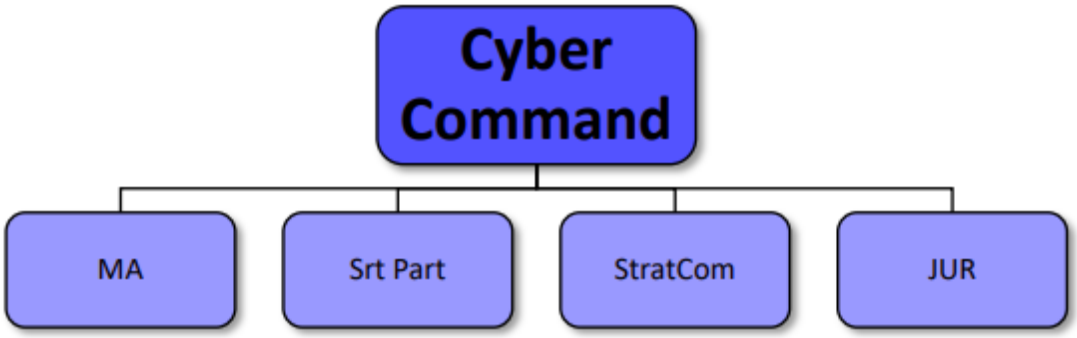


7.1. LA DIRECTION INTELLIGENCE DU SGRS

72. La structure du Commandement cyber comporte un certain nombre d'organes de collecte et d'analyse. Ces organes de collecte répondent aux besoins d'informations des partenaires extérieurs tels que la VSSE, mais aussi, naturellement, d'autres sections du SGRS. Au sein du SGRS, c'est surtout la Direction Intelligence qui formule ces besoins d'informations sous la forme d'*Intelligence Collection Plans* (ICP).

7.2. LE COMMANDEMENT DU CYCOM

73. Le Commandement cyber est exercé par le Commandant cyber (CyC). Il est assisté dans l'exercice de ses missions par un Deputy (DCOM – fonction exercée en cumul – Director Cyber Operations) et un Chief of Staff (COS – fonction exercée en cumul – Director Cyber Development & Readiness). Le Commandement est appuyé par un assistant militaire (MA), un secrétariat particulier (Srt Part), une section juridique (JUR) et une section de Communication stratégique (StratCom).[99]



7.2.1. Le Commandant du Cyber Command (CyC)

74. Le Commandant cyber est responsable de l'exécution des missions du SGRS dans le cyberespace. Il est également le Commandant de la Force cyber (Cyber Force).

7.2.2. Le Military Assistant

75. Le Military Assistant (MA) assiste le CyC, en réalisant des tâches de synthèse et en apportant un appui tant dans pratique que dans le contenu. Le MA appuie la prise de décision au niveau du Commandement.

7.2.3. Sécretariat (SrtPart)

76. Le Secrétariat gère la correspondance IN/OUT du CyC et attribue un numéro officiel dans le Enhanced Document Tracker (EDT) pour les notes de service.

---

99 Ce paragraphe a été repris de la note classifiée CONFIDENTIEL « *Structure 2.1 et compétences au sein su SGRS* ». A la demande du Comité R/I, le SGRS en a accepté la déclassification.

7.2.4. StratCom

77. La section StratCom est chargée, en étroite coordination avec la cellule StratCom du Commandement général du SGRS, d'élaborer une stratégie de communication orientée cyber, tant interne qu'externe, visant, d'une part, à promouvoir les flux d'informations et, d'autre part, à améliorer l'image du service.

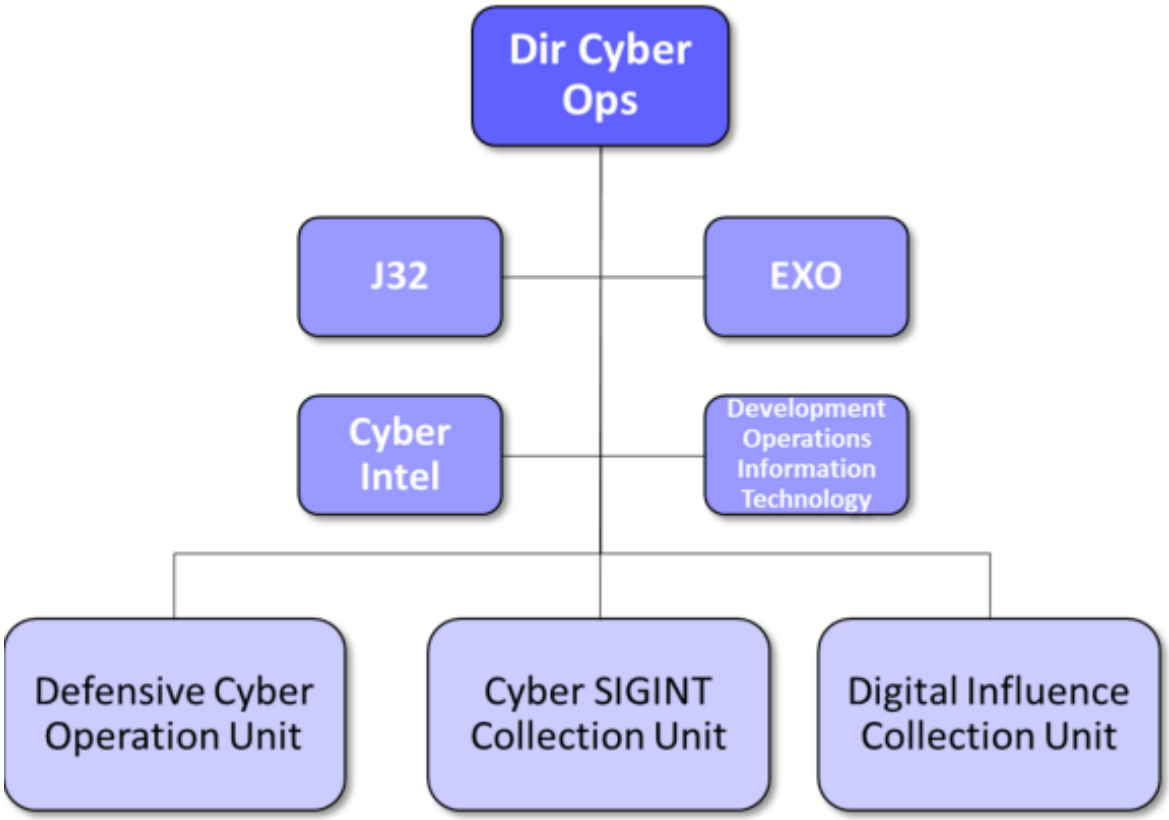
78. Elle est également chargée de l'organisation de cyber-événements (recrutement, relations publiques, etc.). Enfin, elle est le point de contact central pour la coordination et le traitement de toutes les demandes émanant de la presse et de toutes les questions parlementaires relatives au cyberespace, en étroite coordination avec la cellule StratCom du Commandement général du SGRS.

7.2.5. JUR (Cyber)

79. Au sein du Commandement cyber, la section JUR Cyber joue le rôle de conseiller pour toutes les questions revêtant des aspects juridiques dans le cyberespace concernant le renseignement, la sécurité, la cybersécurité et la protection des données à caractère personnel pour le Commandement cyber. Cette section s'acquitte des mêmes tâches (analyse de la législation, avis juridiques, contrôle de la conformité juridique, etc.) que la cellule juridique du Commandement général du SGRS, mais spécifiquement dans le domaine du cyberespace. Dans l'exécution de ses tâches, elle coopère avec cette cellule juridique du Commandement général et, si besoin, avec la DG JUR.

7.2.6. Directie Cyber Operations (CyOps)

80. La Direction Cyber Operations (CyOps) est chargée de la protection, de la défense, de la collecte et de la neutralisation dans le cyberespace et, dans certains cas, de la réaction en menant une attaque. Elle remplit quatre types de missions : Cybersecurity Operations, Defensive Cyber Operations, Cyber ISR (Intelligence, Surveillance, Reconnaissance) Operations et Offensive Cyber Operations.



7.2.6.1. J32

81. J32 est un service d'état-major qui combine les fonctions « renseignement et sécurité » (J2) et « opérations » (J3).

7.2.6.2. Cyber(space) Intelligence (Cyber Intel)

82. Cette plateforme est chargée de suivre et d'analyser les activités cyber malveillantes qui visent les intérêts belges, provenant d'acteurs étatiques ou de groupes soutenus par les Etats.

7.2.6.3. Development Operations Information Technology (DO IT)

83. Cette section fournit au Dir CY OPS une infrastructure informatique sécurisée. Elle gère, entre autres, les équipements IT spécifiques et les réseaux internes nécessaires à la conduite des opérations cyber.

7.2.6.4. Defensive Cyber Operations Unit (DCOU)

84. Cette unité est responsable de la protection et de la défense des réseaux et systèmes d'armes militaires.

7.2.6.5. Cyber-SIGINT Collection Unit (CSCU)

85. Cette unité est responsable de toutes les opérations de collecte menées dans les couches physique et logique du cyberespace.

7.2.6.6. Digital Influence Collection Unit (DICU)

86. Cette unité est responsable de la collecte de données provenant de sources ouvertes et de médias sociaux (OSINT & SOCMINT) et de l'analyse des activités d'influence et de guerre de l'information. L'unité contribue aux missions « Collect » et « Defend », et ce dans la couche « sociale » du cyberespace.

7.2.7. Direction Cyber Development & Readiness (Cy D&R)

87. Cette Direction est chargée du développement des capacités cyber du Commandement cyber et de la Force cyber.

7.2.7.1. Innovation

88. Cette section sensibilise les partenaires industriels et universitaires à la promotion de la recherche et du développement dans le domaine cyber.

7.2.7.2. Support CyJ1/CyJ2/CyJ4/CyJ8

89. CyJ1 réalise des analyses structurelles RH sur la capacité cyber de la Défense belge et organise des examens et le suivi du recrutement par l'intermédiaire de Travaillerpour.be, E-Gov, etc. Elle joue le rôle de point de contact entre CyCom et le J1 du SGRS pour les canaux de recrutement classiques, et entre CyCom (et le SGRS) et la DGHR pour les canaux de recrutement spécifiques ICT (p. ex. E-Gov), gère le secrétariat administratif et la fonction DAES du CyCom, à l'exception des sections DICU, CSCU et DCOU, qui disposent de leur propre DAES. Enfin, la section CyJ1 s'occupe des aspects de *cultural management* (à savoir le *Own Way of Working*).

90. CyJ2 est le point de contact entre le Commandement cyber et J2 SGRS et assume les missions d'officier de sécurité pour les systèmes et l'infrastructure de CyCom.

91. CyJ4 gère le matériel de CyCom en étroite coordination avec la Dir Sp/J4.

92. CyJ8 conseille le CyC sur l'utilisation des budgets alloués au CyCom. Elle établit un plan

budgétaire et fixe des priorités en fonction des ressources disponibles. Le service évalue l'évolution des budgets, en étroite coordination avec J8 SGRS. Elle coordonne tous les aspects pécuniaires des missions pour le personnel de CyCom avec ACOS Ops&Trg. Elle est responsable du traitement des dossiers d'achats locaux et agit en tant que fonctionnaire dirigeant pour plusieurs contrats qui sont spécifiquement attribués au CyCom. Elle est responsable de la gestion du Bureau des contrats (BCU) du CyCom.

93. CyICS est chargé de la maîtrise de l'organisation, en appui direct de la Dir P&P/ICS.

94. CyIM organise les flux d'informations au sein de CyCom.

7.2.7.3. External relations

95. Cette section entretient des contacts avec les partenaires et participe aux groupes de travail nationaux, de l'UE et de l'OTAN, notamment en ce qui concerne le cyberespace, et ce en étroite coordination avec la Dir P&P/REL/RELINT et RELNAT.

7.2.7.4. Education & Training

96. Cette section est responsable de l'organisation de la formation et de l'entraînement des troupes du cyberespace, en établissant des normes de formation pour l'ensemble du personnel cyber, en assurant le suivi des contrats de formation et en évaluant les formations en étroite coordination avec J7 SGRS. Elle organise et coordonne les exercices et les événements du cyberespace ainsi que les formations internes et externes. Elle est chargée de la formation Awareness (JICCS) et du dossier Awareness y afférent. Enfin, elle offre un appui aux activités dans le cadre du recrutement.

7.2.7.5. TRADOC

97. Cette section assure le développement de la Cyberspace Doctrine, ainsi que l'élaboration et le suivi des programmes structurels dans le domaine du cyberespace pour CyCom et la Défense dans son ensemble, en étroite coordination avec les forces et en contact direct avec la Dir P&P/Plans du SGRS.

8.
RECOMMANDATIONS

Le Comité estime que le choix de confier à une seule cybercapacité militaire à la fois des missions de renseignement et de sécurité dans le cyberespace et les missions cyber afférentes à la fonction de force de combat est tout à fait défendable, tant pour des motifs opérationnels que pour des motifs liés au personnel et à la gestion.

Le Comité souhaite toutefois formuler les recommandations suivantes à cet égard :

TOEC.2025.317/01

Le Comité recommande de décrire plus en détail, tout comme pour l'état-major renseignements et sécurité, les missions spécifiques de la Force cyber, donc de l'Unité cyber agissant comme force armée, dans l'A.R. du 30 juin 2025 fixant la structure générale du Ministère de la Défense et les attributions de certaines autorités. Le Comité recommande plus particulièrement au gouvernement de définir de manière concrète, par arrêté royal, les formes d'engagement opérationnel de la Force cyber et, le cas échéant, les formes d'aide et d'assistance militaires.

Le Comité rappelle que la Force cyber ne peut en aucun cas être chargée, au point de vue réglementaire ou opérationnel, de mener des activités de renseignement, telles que visés à l'article 11 L.R&S, ni de l'exécution des missions de sécurité décrites dans cette disposition et dans la Loi Classification. A cet égard, le Comité attire en outre l'attention sur le fait que les activités relevant du champ d'application légal du maintien de la sécurité militaire (art.11 § 1er, 2° L.R&S) ou de la protection du secret militaire (art. 11, § 1er, 3°L.R&S) ne peuvent être confiées à la Force cyber (à savoir par voie réglementaire via un arrêté royal ou par voie opérationnelle via une instruction d'un sous-chef d'état-major mise en condition et opérations).

TOEC.2025.317/02

Au sein du SGRS, il est d'usage d'organiser une réunion de commandement toutes les deux semaines entre le Chef du SGRS, le chef adjoint, le Commissaire en chef et le Commissaire en chef adjoint, le Commandant cyber ainsi que les directeurs de toutes les directions. Cette réunion de commandement fait *de facto* office de comité de direction du SGRS. Le Comité recommande de conférer une valeur juridique à cette réunion dans un arrêté royal ou ministériel.[100] Une telle réunion, organisée de manière réglementaire, permettrait de confirmer une bonne pratique et de la consolider juridiquement. De plus, cela créerait une obligation pour

[100] En comparaison : le comité de direction de la VSSE et sa composition ont été fixés par arrêté royal (art. 4 de l'A.R. du 5 décembre 2006 relatif à l'administration générale de la Sûreté de l'Etat).

le Chef du SGRS et le Commandant cyber de se concerter formellement, et ce en vue d'une intégration plus poussée du Commandement cyber au sein du SGRS.

TOEC.2025.317/03

Le Plan National Stratégique de Renseignement de 2022 prévoit une coopération renforcée dans le domaine cyber entre la VSSE et le SGRS. Ce plan indique que, compte tenu de l'augmentation des ressources prévues, la SGRS apporte un appui à ses partenaires nationaux, qui se traduit notamment par l'utilisation des capacités de collecte et d'analyse du SGRS en faveur de la VSSE.

Au cours de son enquête de contrôle, le Comité a reçu des éléments indiquant que la VSSE n'aurait, jusqu'à présent, guère utilisé les capacités cyber du SGRS. Le Comité souligne qu'il n'a pas approfondi cette question et qu'il ne peut donc ni confirmer ni infirmer cette information. La présente enquête de contrôle ne portait pas sur ce point (*cf.* 1.3. Finalité de l'enquête). Néanmoins, le Comité estime que le SGRS devrait procéder à une évaluation quantitative et qualitative des services et produits fournis par l'unité à d'autres organismes, et ce tant pour les clients de la Défense que pour les clients externes. Compte tenu des attentes du gouvernement, comme cela ressort du Plan National Stratégique de Renseignement, il convient de prêter une attention accrue aux services et aux produits fournis à la VSSE.

TOEC.2025.317/04

La situation géopolitique actuelle exige une attention accrue pour la cybercapacité militaire de notre pays. L'organisation administrative et juridique du Commandement cyber et de la Force cyber constitue une première étape requise. Le Comité recommande que le gouvernement et la Défense accordent une attention suffisante aux moyens nécessaires permettant de faire face aux nombreuses attentes des autorités politiques et militaires à l'égard de cette unité. Le Comité recommande à cet égard que le budget des unités cyber comparables dans les Etats membres de l'OTAN soit pris comme référence. Si, à partir de ce point de référence, les ressources de l'Unité cyber ne peuvent être jugées suffisantes, le Comité recommande d'en adapter le budget.

TOEC.2025.317/05

Au cours de l'enquête de contrôle, le SGRS a annoncé avoir lancé une étude visant à déterminer si une modification de la Loi Renseignement s'imposait en ce qui concerne les missions cyber spécifiques du SGRS et, en particulier, la compétence dite « de contre-attaque ». Le SGRS et l'Unité cyber doivent examiner si cette compétence ne devrait pas être supprimée comme compétence du SGRS (Commandement cyber) et être transférée à la Force cyber. Même si, à première vue, cela semble logique, le Comité estime que ce n'est absolument pas le cas. Comme précisé plus haut, le pouvoir de mener une contre-attaque à la suite d'une cyberattaque est indissociable des missions de renseignement et de sécurité du SGRS. De plus, un tel transfert juridique à la Force cyber ne serait possible que si celle-ci était établie comme entité par la loi. Le Comité ne voit aucune raison pour que la Force cyber soit établie par une loi si les autres forces de combat, tel que prévu par la Constitution pour l'organisation des Forces armées, sont établies par arrêté royal.

Par ailleurs, le Comité rappelle que le gouvernement a récemment choisi de lier cette compétence au Commandement cyber (*cf.* le rapport au Roi joint à l'AR Structure de la Défense du 30 juin 2025 où *« l'identification, l'entrave, la neutralisation de la cybermenace, et, en dernier recours, la contre-attaque en vue d'assurer la protection des réseaux informatiques et des systèmes d'armes que le ministre de la Défense gère ainsi que d'autres réseaux dans le cadre d'une crise nationale de cybersécurité, conformément aux articles 11, § 1er, 2°, 2°/1 et 44/1 de la même loi »* (traduction libre) ont été spécifiquement reprises parmi les missions du commandement cyber.

TOEC.2025.317/06

Le Comité constate que le gouvernement a décidé de créer la Force cyber comme force armée distincte. Dans le même temps, on doit constater que pour diverses raisons, chaque membre du personnel militaire est affecté à une force déterminée, ce qui ne s'est pas traduit lors de la création de la Force cyber. En application de cette réglementation, chaque militaire appartient aux Forces terrestre, aérienne, à la Marine, au Service médical ou au personnel civil. Le Comité recommande d'examiner si et dans quelle mesure une catégorie 'Force cyber' peut être ajoutée au fonctionnement des régimes mentionnés.

TOEC.2025.317/07

Le Comité est habilité à prendre l'initiative d'ouvrir une enquête de contrôle sur l'Unité cyber agissant en tant que Force cyber. Dans ce contexte, le Comité recommande que la Commission parlementaire Suivi des Missions Militaires, qui est chargée du contrôle parlementaire des aspects opérationnels des Forces armées et, partant, des activités de la cybercapacité militaire dans le cadre d'une opération militaire, soit rendue légalement compétente pour confier au Comité R/I la réalisation d'une enquête de contrôle sur la capacité cyber agissant en tant que Force cyber. Au sein du Parlement fédéral, la Commission d'accompagnement et une commission d'enquête parlementaire ont déjà le pouvoir de charger le Comité R/I de réaliser une enquête de contrôle.

ABREVIATIONS

ACOS IS	Assistant Chief of Staff Intelligence and Security
ACOS R&O	ACOS Readiness & Ops - Sous-chef d'état-major mise en condition et opérations
AJP	Allied Joint Publication
AJP-2	Allied Joint Doctrine for Intelligence, Counterintelligence and Security
ANS	Autorité Nationale de Sécurité
C	Chef du SGRS
CCB	Centre pour la Cybersécurité Belgique
CCRS	Comité de Coordination pour le Renseignement et la Sécurité
CFP	Cyber Force Protection
CHOD	Chief of Defense (Chef de la Défense)
CNS	Conseil National de Sécurité
Comdo	Commandement général
COS	Chief of Staff
CSMC	Cyber SIGINT Mission Centers
CSCU	Cyber SIGINT Collection Unit
CSOC	Cyber Security Operations Center
CTS-B	Cosmic Top Secret Bohemian
CyC	Commandant Cyber Command
CyCom	Cyber Command
Cyber Intel	Cyber(space) Intelligence
DAES	Department Administrator and Employee Support
DCOM	Chef adjoint du SGRS
DCOU	Defence Cyber Operation Unit
DICU	Digital Influence Collection Unit
Dir Cy D&R	Directie Cyber Development & Readiness
Dir Cy Ops	Direction Cyber Operations
Dir P&P	Direction Plans & Policy
Dir Rens	Direction Renseignements
Dir S	Direction Sécurité
Dir Sp	Direction Appui
DO IT	Development Operations Information Technology
EDT	Enhanced Document Tracker
ERM	Ecole Royale Militaire
EU CDCC	European Union Cyber Defence Coordination Centre
EXO	Executive Officer
HCC	Commissaire en chef
HCC Adj.	Commissaire en chef adjoint
JCDRFU	Joint Cyberspace Defense Resilience Force Unit
JUR	Section juridique

J1	Ressources humaines
J2	Renseignement et sécurité
J3	Opérations
J4	Logistique
J7	Formation
J8	Budget
J32	Section Coordination opérationnelle
Loi MRD	Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité
L.C&HS	Loi du 11 décembre 1998 relative à la classification et aux habilitations, aux avis de sécurité et au service public réglementé
L. Contrôle	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.R&S	Loi du 30 novembre 1998 organique des services de renseignement et de sécurité
LtGen	Lieutenant-général
MA	Military Assistant
NCCB	National Cybersecurity Council Belgium
NCCN	Centre de crise National
NEO	Non-Combatant Evacuation Operation
PSNR	Plan Stratégique National du Renseignement
SGRS	Service Général du Renseignement et de la Sécurité
Sp	Support
Srt Part	Secrétariat particulier
StratCom	Communication stratégique
TTP's	Tactics, Techniques and Procedures
VSSE	Sûreté de l'Etat