GRILLE DE LECTURE DE LA MENACE CYBERNÉTIQUE À TRAVERS LA MISE EN PLACE DE LA FORCE CYBER BELGE

Pierre CIPARISSE

© Bel Defence, Quentin Moonen

Nu de cyberspace zich doet gelden als nieuw strijdtoneel, zet België een historische stap met de oprichting van zijn cybermacht. Het huidige artikel biedt een inkijk in het hart van deze nieuwe strijdkracht van Defensie. Zo wordt dieper ingegaan op haar fundamenten en opdrachten, alsook op de dreigingen waartegen ze moet optreden. Aan de hand van een strategische en operationele lezing, worden de uitdagingen belicht van een domein dat even onzichtbaar als cruciaal is en waar fotonen, codes en invloeden elkaar kruisen.

Le général-major Pierre CIPARISSE a repris le commandement de la Force cyber le 19 septembre 2025. Ingénieur en télécommunication, issu de la 145e promotion Polytechnique de l'École royale militaire, sa carrière alterne entre fonctions opérationnelles et d'état-major dans les domaines des systèmes de communication et d'information ainsi que du renseignement technique. En sa qualité d'officier transmission para-commando, il a été déployé en Albanie et au Burundi, a commandé le 4 Gp CIS et compte plus de neuf ans au sein du Service général du renseignement et de la sécurité (SGRS).

Cela faisait 51 ans que la Belgique n'avait pas créé un nouveau service, une nouvelle Force ou, selon la terminologie utilisée ces 25 dernières années, une nouvelle « composante ». Le 3 juin 2025, Sa Majesté le Roi confiait le nouvel emblème de la Force cyber au général-major Van Strythem. Événement hautement symbolique marquant l'achèvement de quatre années de travail pour l'ensemble du personnel qui – partant des solides bases de la direction cyber ancrée au sein du Service général du renseignement et de la sécurité (SGRS) – a mis en place, intégré et développé un ensemble cohérent de capacités dites « cyber ».

Il est certainement important de définir le mot « cyber » qui, lorsqu'il n'est pas utilisé seul, apparaît avec toutes sortes de substantifs. Il s'agit tout d'abord d'une capacité de la Défense car, si le cœur de celle-ci se trouve dans les faits au sein du SGRS, son rayonnement en tant que Force est transversal, en appui de et en interaction avec les autres Forces et services de la Défense belge. La cyberdéfense englobe donc

toutes les activités que des forces armées peuvent déployer. Ces dernières agissent dans des domaines opératifs, dont le plus ancien est sans aucun doute le domaine terrestre, suivi par le domaine maritime. La conquête de l'air et, plus récemment, de l'espace ont ouvert deux dimensions auxquelles est venu s'ajouter le cyberespace, il y a maintenant presque 10 ans[1].

Au sein de la Force cyber belge, nous remplaçons systématiquement le mot « cyber » par « cyberespace » pour souligner clairement qu'il s'agit d'un domaine englobant trois couches :

- une couche physique (le « matériel »), qui englobe tous les éléments actifs, c'est-à-dire, les « appareils ». Il s'agit de tous les éléments nécessaires pour construire un réseau et communiquer. En outre, ces éléments existent physiquement : on peut les prendre en main et les positionner sur terre ; ils ont des coordonnées et/ou des effets physiques. Nous incluons également les satellites, le spectre électromagnétique ou encore les ondes radio, certes plus difficiles à saisir, mais dont le trajet est déterminé ;

- une couche logique (le « logiciel »), lieu d'utilisation du code. Cette couche se compose d'éléments créés par l'homme et qui, dès lors, sont sujets à erreur. Si le mot « cyber » ne faisait référence qu'à un seul élément, tout le monde conviendrait que c'est celui-ci. C'est dans ce domaine que les activités de cybersécurité sont mises en œuvre et que les *malwares* – des logiciels malicieux – sont utilisés ;

- enfin, une couche cognitive ou virtuelle (les « données »), qui comprend notre représentation d'êtres humains dans le cyberespace et est parfois décrite comme la « cyber-persona ». On pense par exemple aux comptes Facebook ou LinkedIn, mais aussi à notre activité en ligne, notre manière de faire défiler des pages ou des applications. Ces informations définissent notre intérêt publicitaire et constituent une source de renseignements marketing.

[1] L'OTAN a reconnu officiellement le cyberespace comme un domaine opératif en 2016, lors du sommet de Varsovie.

Ainsi, si le terme « cyber » se réfère la plupart du temps à la couche logique, pour nous au sein de la Force cyber, il s'applique à la guerre électromagnétique dans la couche physique jusqu'aux opérations d'influence dans la couche virtuelle. Des photons et électrons aux trolls en passant par les bits et les bytes. De toute évidence, les acteurs malveillants usent et abusent largement de ces trois couches dans la guerre hybride.

Le Cyber Command – une unité jeune, expérimentée et en développement – fait partie du SGRS, le service de référence pour le renseignement extérieur et de défense au sein de la communauté du renseignement belge. Cette unité est jeune parce qu'elle a été créée en 2022, en tant qu'unité spécialisée, comme une sorte de direction technique. Expérimentée, car elle a été formée en unifiant toutes les unités et services existants – certains avec plus de 30 ans d'expérience – ayant pour dénominateur commun les trois couches du cyberespace. En développement, car l'objectif à terme est de mener quatre types d'opérations : protéger, défendre, collecter et combattre dans les trois couches.

Nous protégeons la Défense belge par des mesures de sécurité, de sensibilisation et de soutien cryptographique. Nous la défendons en gérant des incidents – comme une attaque malveillante – depuis la détection jusqu'à la récupération. Nous définissons les menaces et collectons des informations sur le cyberespace à travers toutes les couches pour soutenir les exigences de sécurité et de renseignement du SGRS. Enfin, nous injectons l'élément cyber dans les opérations militaires ou de renseignement, que ce soit dans le cadre d'une approche d'entrave ou en planifiant de réels effets cyber pouvant être intégrés dans des opérations multi-domaines.

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 cyberespace selon les spécificités individuelles de ces Forces et services.

Le cyberespace est un domaine vaste où nous menons une gamme complète d'opérations, mais force est de constater que nos adversaires potentiels le font aussi.

LES ACTEURS

Parmi les acteurs du domaine cyber, nous pouvons distinguer trois catégories[2] :

- Les acteurs étatiques sont liés aux organisations régaliennes, principalement les services militaires ou de renseignement. Si l'on prend l'exemple de la Russie, il s'agit du FSB, du SVR et du GRU. Ces trois services usent et abusent du cyberespace, chacun avec ses objectifs spécifiques. En Chine, il s'agit du ministère de la Sécurité de l'État (MSS en anglais), le ministère de la Sécurité publique (MPS en anglais) et de l'Armée populaire de libération (PLA en anglais).

- Ensuite, on distingue les acteurs sponsorisés par l'État, qu'il s'agisse de groupes criminels ou du secteur privé. Nous savons que l'industrie cyber russe soutient les activités d'acteurs étatiques. La position de sociétés comme Kaspersky ou NTC Vulkan est cruciale pour fournir les compétences et les outils nécessaires aux efforts cyber russes. Nous pouvons également mentionner, en Chine, la législation spécifique qui impose à toute entreprise découvrant une vulnérabilité de la déclarer auprès des services de sécurité, mais aussi l'implication de sociétés privées, telle qu'iSoon, qui fournissent des services de hacking commerciaux.

- Enfin, les cybercriminels et groupes hacktivistes sont de plus en plus nombreux. Les *ransomwares* attirent bien sûr toute l'attention, mais il s'agit en fait d'un écosystème complet de services de hacking spécialisés et lié au crime organisé[3]. Techniquement, il existe des preuves de chevauchement au niveau des outils et de l'infrastructure utilisés par les acteurs étatiques et les groupes de

[2] Les deux premières étant celles qui mènent des campagnes de longue durée appelées « menaces persistantes avancées » (ou *Advanced Persistent Threat*, APT)

[3] MAKOWSKI J. (2025, January) *Cybercrime ecosystem and international operations.* https://www.linkedin.com/posts/underdark-ai_cybercrime-ecosystem-and-international-operations-activity-7288111344938029056-kNCv/

cybercriminalité, indiquant un degré de porosité entre ces menaces[4]. Les liens potentiels entre les deux vont au-delà de l'aspect technique. Les cybercriminels étant tolérés dans certains pays, il y a probablement des flux d'argent dans les deux sens : paiement pour exécution de mission ou corruption.

LES ACTIVITÉS

Si nous analysons la menace sous l'angle des activités, que voyons-nous ?

Il y a tout d'abord les activités que nous pouvons qualifier de perturbatrices. Ce sont les activités les plus visibles : brouillage GPS, attaques en déni de service distribué (DDoS) et, certainement, la désinformation.

Appartenant à la couche physique du cyberespace, la guerre électronique est apparue dès que le caractère incontournable des communications par radiofréquence s'est imposé sur le champ de bataille. L'Union soviétique – et la Russie à sa suite – l'a bien compris en y consacrant des moyens de la taille d'une compagnie au niveau de la brigade[5]. Le brouillage fait partie intégrante des tactiques russes car il dégrade le commandement et le contrôle de l'adversaire. La guerre électronique ne se limite pas aux communications ni au radar. Les signaux des systèmes de positionnement par satellites sont faciles à brouiller avec une faible puissance d'émission. On constate également de plus en plus de cas de *spoofing*, c'est-à-dire, l'émission de signaux qui prennent la place de ceux des satellites et induisent un calcul de position permettant de faire naviguer la cible à un autre endroit. Cette technique est utilisée par Israël[6] pour se protéger des attaques de missiles, mais également par l'Iran pour viser le trafic maritime en mer Rouge. La consultation de cartes sur des sites internet comme *GPSJAM* ou *Flightradar* permet de voir les points névralgiques des conflits de par le monde.

---

[4] ANSSI MMXXIV *Panorama de la cybermenace.* https://cyber.gouv.fr/publications

[5] APT-7-100.1 Russian Tactics (2024, February) HQ Department of the Army. https://armypubs.army.mil/

[6] JACOBS, F. (2025, February 24). *GPS jamming, a weapon in hot and hybrid wars, will soon be obsolete. Big Think.* https://bigthink.com/strange-maps/gnss-jamming/

Dans la couche logique, nous pouvons observer deux changements en Ukraine. Au début de l'invasion en 2022, les activités cyber-perturbatrices faisaient partie du processus opérationnel, avec des attaques contre les systèmes de communication ou, plus tard, contre les infrastructures électriques[7]. Au cours des trois années écoulées, nous pouvons toutefois constater que le nombre de cyberattaques perturbatrices contre l'Ukraine diminue. Le cycle de ciblage cyber est beaucoup plus long que le cycle de ciblage cinétique. Le deuxième changement se situe en dehors de l'Ukraine. Nous voyons que les alliés de l'Ukraine sont de plus en plus soumis à des opérations perturbatrices dans la couche logique. Il ne s'agit pas ici du débordement de l'attaque contre VIASAT mais d'attaques DDoS que les systèmes alliés subissent tous tour à tour. Leurs effets sont limités, ce qui est probablement intentionnel, afin d'éviter d'atteindre un seuil qui déclencherait une réponse forte.

Il y a clairement des activités perturbatrices dans la couche virtuelle. La défiguration de sites web ou le détournement de diverses web TV sont perturbateurs et font partie des campagnes de désinformation. La manipulation d'information et l'ingérence informationnelle d'origine étrangère[8] influencent l'opinion publique.

L'autre catégorie d'activités caractéristiques du cyberespace est certainement l'espionnage. Le renseignement est la première ligne de défense. Ainsi pense aussi l'adversaire. Ces activités sont moins visibles, pour ne pas dire presque invisibles. Elles ne se limitent pas à des zones de conflit telles que l'Ukraine. Notre pays figure lui aussi sur la liste des cibles. Aucune opération perturbatrice ne peut se faire sans reconnaissance. Il faut connaître les fréquences à brouiller et déterminer les opinions à influencer. A fortiori, dans la couche logique, toute future opération perturbatrice nécessite des accès, un premier point d'appui dans le système. Faisant à nouveau référence à l'Ukraine, un changement a clairement eu lieu. Alors que les activités cyber perturbatrices diminuent, les observations montrent que la Russie a de plus en plus souvent recours au cyberespace pour soutenir le ciblage cinétique.

[7] WILLETT M. (2024). *Chap 5 of Cyber Operations and Their Responsible Use* (1st ed.). Routledge. https://doi.org/10.4324/9781003601333

[8] Définition de l'EU : FIMI, ou *Foreign Information Manipulation and Interference*

Nous avons par ailleurs tous un espion dans notre poche : le smartphone est un outil de collecte de données, mais il n'est pas l'allié du soldat en première ligne. Le smartphone est une mine d'or d'informations, mais laisse des traces sur l'Internet. Des informations personnelles peuvent être utilisées pour développer d'autres opérations cyber, mais aussi pour déterminer des positions/des informations clés pour bombarder une unité. Dans le conflit russo-ukrainien, les deux adversaires rivalisent de créativité dans l'exploitation de cette source d'information pour accélérer le processus de ciblage.

Les *ransomwares* ou logiciels de rançons pourraient également être considérés comme faisant partie des activités perturbatrices et de renseignement. En effet, au-delà de la recherche d'argent en échange d'une clé de déchiffrement, il y a également la collecte d'information qui est caractéristique des *ransomwares*. Ces informations sont utiles pour préparer d'autres attaques, être monnayées sur le *dark web* ou être transmises à un État qui ferme les yeux sur ce genre d'activité criminelle. Un ransomware reste cependant une collecte ponctuelle profitant de l'opportunité du moment plutôt qu'une mission de renseignement sur le long terme, puisqu'une fois le piratage découvert, la victime fera tout pour bloquer l'adversaire.

LE CYBERESPACE, UN DOMAINE ISOLÉ ?

Tout d'abord, une des principales caractéristiques des activités dans le cyberespace est qu'elles sont facilement contestables. Nous voyons cela également dans le domaine maritime. La non-attribution de l'attaque du gazoduc Nord Stream est liée à sa « déniabilité ». Il en va de même pour la coupure de câbles sous-marins. Une coupure de câble constitue une activité dans le domaine maritime ou terrestre ayant un impact sur le domaine cyber. Les coupures de câbles sont faciles à nier et ont des effets énormes : perte de débit, voire perte de communication, et coût économique. Une partie de ces coupures sont accidentelles, mais nous devons également prendre en compte les coupures intentionnelles.

Les activités dans le domaine cyber ont, à leur tour, un impact sur les autres domaines de la guerre. Comme mentionné précédemment, le renseignement via le cyberespace passe en grande partie par la collecte de données, notamment via le renseignement en sources ouvertes (*open source intelligence*, OSINT). L'OSINT est devenu un phénomène communautaire qui n'est pas limité aux soldats ou aux officiers de renseignement, mais accessible à tous. Chacun peut y contribuer. Rappelons-nous le smartphone, cet espion dans notre poche. Chaque citoyen publiant des photos contribue à la collecte de données. Ainsi, il soutient son propre camp ou, sans y prêter suffisamment attention, le trahit. La collecte de renseignements dans le cyberespace contribue au ciblage cinétique[9] et à l'évaluation des dommages, ce qui constitue un lien entre le domaine cyber et le domaine terrestre.

Dans le cas de la désinformation, nous voyons un véritable lien bidirectionnel entre les domaines. Les activités dans la vie réelle sont potentiellement amplifiées par les activités dans le cyberespace. Nous l'avons observé lors d'événements ayant eu lieu chez nous, tels que l'introduction de l'EVRAS[10] ou les émeutes à Heusden-Zolder en mars 2024. Nous le voyons aussi avec des activités cyber perturbatrices comme les attaques contre les infrastructures critiques, destinées à renforcer la campagne en ligne visant à discréditer le gouvernement en place. Ces techniques ont été largement utilisées par la Russie en Ukraine entre 2014 et 2022.

CONCLUSIONS

La création de la Force cyber belge marque une étape historique et stratégique dans l'évolution de la Défense, car elle répond à une menace cybernétique toujours plus complexe et omniprésente. En structurant ses capacités autour des trois couches du cyberespace – physique, logique et cognitive –, la Belgique affirme sa volonté de

[9] BLACK D. (2024, July 22) *Russia's Cyber Campaign Shifts to Ukraine's Frontlines.* https://www.rusi.org/explore-our-research/publications/commentary/russias-cyber-campaign-shifts-ukraines-frontlines

[10] Éducation à la vie relationnelle, affective et sexuelle. Voir FILLON T. (2025, April 9) EVRAS, dans le feu des contestations. https://ligue-enseignement.be/education-enseignement/articles/dossier/evras-dans-le-feu-des-contestations

mener des opérations complètes et coordonnées, allant de la protection à la lutte active contre les acteurs malveillants. L'analyse des activités perturbatrices, de l'espionnage et des interactions entre domaines montre que le cyberespace n'est ni isolé ni secondaire, mais bien un champ de bataille à part entière, où se jouent des enjeux de souveraineté, de sécurité et d'influence. Face à des acteurs étatiques et non étatiques utilisant des méthodes de plus en plus sophistiquées, la Force cyber s'impose comme un outil indispensable pour anticiper, comprendre et contrer les menaces hybrides du XXIe siècle.

Mots-clés : Force cyber, cyberespace, SGRS, menaces cyber, renseignement cyber

© Be Defence