La construction d'un Cyber Command

Alexandre DANIEL

Le capitaine-commandant Alexandre DANIEL est officier des troupes de reconnaissance. Il a rempli des fonctions dans le renseignement militaire et a eu l'opportunité d'acquérir des connaissances dans le domaine de la sûreté des entreprises. Il est aujourd'hui officier synthèse au sein de l'équipe de projet « Cyber & Influence » qui encadre la construction d'un Cyber Command.

De alomtegenwoordigheid van informatietechnologie heeft een niet te onderschatten impact op alle aspecten van ons dagelijkse leven, ook op onze veiligheid. Staten zien zich daardoor genoodzaakt een cyberstrategie te ontwikkelen. De toekomstige Cyber Command maakt integraal deel uit van de Belgische cyberstrategie en zal zich toespitsen op vier taken:* Cyber Readiness of the Forces, Readiness of the Cyber Forces, Conduct of Cyber Operations en Homebase Support. *De Algemene Dienst Inlichtingen en Veiligheid (ADIV) blijft verantwoordelijk voor de cybercapaciteiten van Defensie. Daarnaast zullen deze capaciteiten ook ingezet kunnen worden ter ondersteuning van militaire operaties.

La révolution numérique, c'est-à-dire l'omniprésence des technologies de l'information, façonne les réalités quotidiennes, transforme les communautés humaines et modifie notre perception du réel. Pas un seul aspect de notre existence n'a échappé à cette lame de fond de l'histoire. L'impact du digital est global et la transformation numérique ne peut se résumer à sa seule dimension technologique. Celle-ci est holistique : politique, culturelle, sociale, économique, et donc aussi militaire.

Dès lors, nous observons l'apparition de nouvelles formes d'affrontement dans le cyberespace. Celles-ci présentent des porosités manifestes entre acteurs criminels et étatiques, et les repères classiques s'estompent pour laisser place à d'obscures alliances. La maîtrise des technologies de l'information permet aujourd'hui

d'influencer nos démocraties, d'affaiblir nos capacités militaires et de menacer la disponibilité de nos infrastructures critiques, sans que l'on puisse attribuer l'origine de ces actes avec une absolue certitude. Ainsi, certains pays, profitant de l'anonymat favorisé par le cyberespace, développent leur économie par le pillage des propriétés intellectuelles de nos entreprises et n'hésitent plus à porter atteinte à notre souveraineté nationale.

Pour faire face à ces nouvelles menaces, les États ont dû se réorganiser et développer une « cyberstratégie ». Celle-ci se subdivise idéalement en plusieurs parties : un volet de cybersécurité qui vise à atteindre la résilience de toute la société face aux menaces cyber ; une politique de cyberdiplomatie, qui définit la manière dont un pays se positionne au niveau international dans ce domaine et fixe les coopérations internationales dans un cadre cohérent ; une approche policière et judiciaire spécialisée dans la lutte contre la cybercriminalité ; un effort d'enseignement, de recherche, de développement technologique et de politique industrielle qui permet d'acquérir les compétences et les nouvelles capacités ; un plan de cyberrenseignement qui coordonne les services de renseignement et de sécurité dans le cyberespace ; et, enfin, une stratégie de cyberdéfense qui précise la façon dont les forces armées intègrent l'utilisation du cyberespace dans les problématiques de défense. Une cyberpuissance ne se décrète donc pas, elle se construit. Elle est le produit d'une « cyberstratégie » nationale qui met en adéquation les moyens et les objectifs d'une société tout entière.

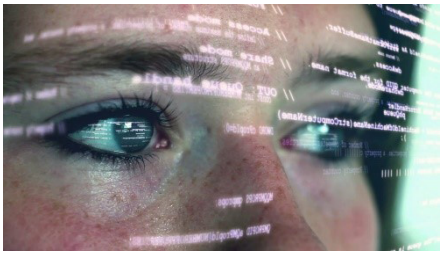
Une adaptation doctrinale majeure

De par son importance, le cyberespace est à la fois devenu un « centre de gravité » des sociétés modernes et un espace d'affrontement incontournable : y maintenir une liberté de mouvement, une capacité à collecter de l'information et générer des effets dans le but d'affaiblir l'adversaire sont donc autant de prérequis pour assurer l'efficacité des armées modernes. Plus aucune manœuvre ne peut se concevoir sans intégrer les contraintes de l'espace numérique et électromagnétique et exploiter les opportunités qu'il offre. Pour les forces armées, les conséquences doctrinales et organisationnelles sont majeures.

Premièrement, l'interconnexion du cyberespace génère l'interdépendance et force, sous peine d'échec, à une approche intégrée qui doit inclure les acteurs publics interdépartementaux et internationaux, les acteurs privés, ainsi que la société civile.

Les rôles traditionnellement dévolus aux services de renseignement et de sécurité, aux forces armées, à la police ou encore aux organisations civiles et aux entreprises privées se brouillent parfois, voire se superposent et obligent à la convergence des intentions, des processus et, parfois, des structures. La coopération est une condition nécessaire de l'efficacité et de la résilience des nations.

Deuxièmement, la révolution numérique bouleverse les modalités traditionnelles de l'art de la guerre. Les technologies de l'information modifient les limites spatiales du champ de bataille et brouillent les repères temporels du combat. L'émergence des réseaux C6ISRT[1] rend possible la mise en réseau de capteurs et d'armes à l'échelle mondiale, obligeant à maintenir une posture de défense permanente. Il ne suffit donc plus de préparer la guerre ; il faut s'assurer de gagner « la guerre avant la guerre », de sanctuariser nos sources de puissance et de participer au développement d'une société résiliente capable d'absorber le choc des batailles, fussent-elles géographiquement éloignées. La manœuvre militaire moderne exige donc de préserver une capacité d'action dans le cyberespace et de soustraire à l'ennemi les possibilités qui lui permettent d'exploiter l'espace numérique.



© Direction Cyber

Une posture de cyberdéfense requiert une vigilance de tous les instants

Troisièmement, nous constatons une convergence entre les capacités de collecte, de traitement et de diffusion de l'information. Les unités de lutte informatique, celles de la lutte électronique, de la collecte du renseignement et celles dédiées à la guerre de l'information (*information operations*) ont tendance à se regrouper, voire à fusionner entre elles. Cette concentration des moyens est bâtie sur la doctrine de l'*information dominance*. Celle-ci conçoit l'information comme une capacité génératrice d'effets militaires et stipule que son opérationnalisation nécessite une coordination, non seulement dans le cyberespace, mais sur l'ensemble du champ informationnel et immatériel où évoluent les forces armées. Partant donc d'une vision où l'information était exclusivement perçue comme une capacité d'appui des forces traditionnelles, nous évoluons vers une doctrine d'emploi qui conçoit l'information comme une capacité de manœuvre. On bascule donc d'une vision du combat soutenu par l'information à celle d'un combat qui, dans certaines phases, doit pouvoir s'envisager par, pour et contre l'information.

[1] *Cyber Defence, Command, Control, Computers, Communication, Combat Systems, Intelligence, Surveillance, Reconnaissance, Targeting*

Cette prise de conscience des nouvelles réalités de la guerre mène donc à concevoir le cyberespace comme un cinquième domaine opérationnel[2] doté de caractéristiques physiques exclusives et d'une logique opérationnelle unique qui justifie la création de capacités spécialisées. Par conséquent, de nombreux pays créent aujourd'hui des forces de cyberdéfense capables de mener le combat numérique et développent une doctrine d'emploi cyber en synchronisation avec la manœuvre globale de leurs forces armées. En Belgique, la responsabilité de créer, mettre en condition et mettre en œuvre ces forces spécialisées incombera au futur « Cyber Command », une nouvelle entité du Service général de renseignement et de sécurité (SGRS).[3]

Des capacités déjà existantes, mais pas suffisantes

Avant de détailler les futures missions et organisations du Cyber Command belge, il faut comprendre que les capacités de cyberdéfense de nos forces armées émanent historiquement du SGRS et sont donc, à la base, articulées autour des missions de ce service.

Pour les missions de sécurité, la loi organique des services de renseignement et de sécurité du 30 novembre 1998 (L.R&S) attribue au SGRS la mission « de veiller au maintien de la sécurité militaire […] des […] systèmes informatiques et de communications […] et, dans le cadre des cyberattaques, […] de neutraliser l'attaque et d'en identifier les auteurs », ainsi que la mission « protéger le secret qui […] s'attache […] aux renseignements et communications militaires, ainsi qu'aux systèmes informatiques et de communications militaires ou ceux que le ministre de la Défense nationale gère »[4] [5].

[2] En 2016, lors du sommet de Varsovie, l'OTAN a reconnu le cyberespace comme domaine opérationnel au même titre que la terre, la mer, l'air et l'espace. Ce cyberespace est subdivisé en trois couches : la couche physique (l'ensemble des systèmes d'information interconnectés), la couche logique (les systèmes logiciels) et la couche virtuelle (celle des interactions sociales, où s'exercent les influences numériques).

[3] L.R&S, art. 11, §1er, 2°

[4] L.R&S, art. 11, §1er, 3°

[5] Une récente révision de L.R&S, attribue également au SGRS la possibilité de réagir en cas d'attaques sur des systèmes informatiques non gérés par le Ministère de la Défense en cas de crise nationale de cybersécurité.

© Direction Cyber

Le SGRS offre des possibilités de carrière de cyberdéfense exclusives, tant pour son personnel civil que pour son personnel militaire.

Par ces deux paragraphes, le législateur assigne au SGRS une tâche d'une ampleur non négligeable[6]. Premièrement, il charge le service de veiller sur plusieurs dizaines de systèmes d'armes et de réseaux, parmi les plus complexes du pays, souvent construits autour de technologies hétérogènes. Tous les programmes majeurs d'équipement qui doivent bientôt entrer en service à la Défense correspondent à ces « systèmes d'armes » que le SGRS doit pouvoir intégrer dans son *Cyber security operations centre* et pour lesquels de nouvelles architectures de *command & control* et d'échange de données devront être développées. Enfin, pour pouvoir assurer la protection du secret, dans un environnement technologique en mutation constante, il est nécessaire de disposer tant de compétences pointues en matière d'accréditation des réseaux et des systèmes d'armes que de spécialistes de la cryptographie capables de rivaliser avec les meilleurs adversaires au monde.

Deuxièmement, la notion de « neutralisation » telle que reprise par la L.R&S rend nécessaire la mise en œuvre de contre-mesures électroniques en cas de cyberattaques. Celles-ci doivent servir à supprimer les effets de l'attaque sur les réseaux de la Défense et peuvent être mises en œuvre pour neutraliser l'origine de cette cyberattaque dans le seul et unique but de la faire cesser. Cette option revient à monter une forme de « contre-attaque » en dehors de nos lignes et conduit donc le SGRS à devoir disposer de capacités offensives.

Troisièmement, la nécessité de pouvoir « identifier » les auteurs d'une cyberattaque implique d'investir dans des capacités de collecte et d'analyse de l'information numérique à la pointe du progrès. Tenant compte du caractère obscur du cyberespace, identifier un acteur numérique, c'est-à-dire lui « attribuer » une action, est le résultat d'un processus juridique, technique et politique complexe. Cette mission exige un personnel de pointe dans plusieurs domaines tels que l'extraction de données, l'analyse de malwares ou le *cyber threat intelligence*, capable d'établir des conclusions en lien étroit avec l'analyse de la situation sécuritaire globale produite par la direction Renseignement du SGRS.

[6] La mission de neutralisation des cyberattaques sera étendue dans la révision prévue de la L.R&S. Celle-ci pourra s'appliquer en cas de cybercrise nationale touchant des réseaux non gérés par la Défense.

En ce qui concerne les missions de renseignement, la L.R&S offre également au SGRS plusieurs possibilités d'opérer dans le cyberespace. D'une part, elle permet, dans les conditions fixées par la loi, de procéder à l'interception de communications en Belgique[7] ou à l'étranger[8] et/ou la réquisition de données[9] auprès d'opérateurs de réseaux de communication électronique ou de fournisseurs d'un service de communication électronique. D'autre part, elle permet de procéder à des intrusions informatiques à l'étranger[10] et, en Belgique, de pénétrer dans des lieux non accessibles au public pour procéder à l'intrusion informatique[11]. Inutile de préciser à quel point il est, ici aussi, nécessaire de disposer de personnel spécialisé et équipé pour pouvoir remplir ces tâches d'intrusion sur des systèmes adverses – sans se faire détecter – et qu'il est essentiel de disposer de capacités suffisantes pour pouvoir appuyer toutes les missions de la Défense belge, sur l'ensemble de ses théâtres d'opération.

Le Cyber Command, un projet qui s'inscrit dans le temps long

Consciente des défis exposés ci-dessus, la ministre de la Défense (MOD) a, dans sa note de politique générale du 29 octobre 2021, présenté la cyberdéfense comme une priorité. Celle-ci a chargé une équipe de projet d'établir une feuille de route visant au renforcement des capacités de cyberdéfense belge. Il en découle quatre objectifs : la création d'un Cyber Command, le renforcement des capacités du SGRS à effectuer ses missions dans le cyberespace, l'initiation d'une politique d'innovation technologique en lien avec l'industrie belge pour le développement et l'acquisition de nouvelles capacités et, enfin, l'orientation du processus de croissance de l'ensemble des cybercapacités de la Défense.

Conformément aux engagements pris, le Cyber Command sera déclaré « *initial operational capable* » à la fin de l'année 2022. Celui-ci sera, dans un premier temps, constitué de la fusion entre l'équipe de projet, l'actuelle direction Cyber du SGRS et d'autres entités du SGRS. Cette réorganisation s'appuie sur le principe de convergence, décrit ci-dessus, et cherche à regrouper l'ensemble des capacités

[7] L.R&S, art. 18/17
[8] L.R&S, art. 44
[9] L.R&S, art. 16/2
[10] L.R&S, art. 44/1
[11] L.R&S, Art 18/16

qui permettent au SGRS et aux forces armées d'opérer simultanément sur les trois couches du cyberespace[12]. La trajectoire de croissance du Cyber Command prévoit une importante augmentation des effectifs, le Cyber Command devant être déclaré « *full operational capable* » en 2030.

Le Cyber Command assumera quatre tâches : *Cyber Readiness of the Forces*, visant à superviser la mise en condition « cyber » de l'ensemble de la Défense, en coordination étroite avec ses composantes, ACOS et DG et à s'assurer d'une mise en cohérence capacitaire transversale au travers des trois couches du domaine « cyber » ; *Readiness of the Cyber Forces*, en vue d'assurer la mise en condition des forces spécialisées en matière de cyberdéfense, essentiellement au sein du SGRS ; *Conduct of Cyber-Operations*, dans l'optique d'assurer la conduite de missions dans le cyberespace (*protect, defend, collect, fight*) au profit du SGRS, de la Défense belge et de l'État belge ; et enfin *Homebase Support*, visant à mettre en œuvre les capacités du Cyber Command pour assurer la mission d'aide à la nation en cas de crises ou incidents nationaux au niveau cyber, tel que prévu entre autres dans la stratégie belge de cybersécurité 2.0.

Pour pouvoir diriger son organisation, le futur « Cyber Commander » jouira d'un statut unique à la Défense et assumera une triple responsabilité : il sera commandant de composante (chargé de la mise en condition), assumera la fonction de directeur « cyber » du SGRS (pour l'exécution des missions prévues par la L.R&S) et supervisera la conduite des opérations « cyber » qui émaneront de l'ACOS Ops&Trg[13], telle que l'exécution des missions militaires qui ne tomberaient pas sous le mandat du SGRS.

La structure du Cyber Command s'articulera autour de deux directions. Premièrement, une direction Opérations, chargée de la mise en œuvre des capacités. Celle-ci sera subdivisée en quatre entités : l'analyse du renseignement et des menaces spécifiques au cyberespace ; les opérations défensives ; les opérations de collecte de l'information et l'exécution des opérations offensives ; et, enfin, la collecte de l'information en sources ouvertes et l'analyse des phénomènes d'influence numérique. Deuxièmement, une direction Support, qui sera chargée de la mise en condition et du développement de la cyberdéfense belge. Par la veille technologique et sociétale permanente, cette direction tiendra à jour une doctrine d'emploi des forces cyber, pilotera son développement capacitaire et appuiera la création d'un capital humain hautement spécialisé.

[12] Physique, logique et virtuelle
[13] Assistant Chief of Staff « Operations & Training »

Pour faire face aux défis qu'impose la permanente évolution technologique, une attention particulière sera apportée à l'acquisition de nouvelles compétences, notamment par des parcours de formation individualisés et l'établissement d'une porosité volontaire entre le monde civil et celui de la Défense. Ce faisant, le Cyber Command s'intégrera à l'esprit du changement porté par la Défense et adoptera les initiatives proposées par le « réseau de la transformation ». Celles-ci visent à l'optimisation de la culture organisationnelle et à l'implémentation du *new way of working*, qui promeut l'optimisation des performances mentales et le bien-être du personnel. Puisque les organisations ne sont innovantes qu'à la mesure des êtres humains qui les constituent et que l'adaptation est une condition structurelle requise pour la survie au combat, le Cyber Command sera conçu pour offrir, à terme, une capacité évolutive en interaction constante avec son écosystème industriel, ses pôles de recherche académique, ainsi que la société civile.

Pour atteindre ses objectifs, l'équipe de projet a établi une feuille de route reprenant plusieurs axes d'efforts nécessaires à l'opérationnalisation de la capacité : le développement permanent du capital humain ; la planification des ressources matérielles et l'infrastructure ; l'établissement d'un cadre doctrinal de cyberdéfense ; la structure du Cyber Command ; la consolidation d'un cadre juridique national pour la conduite de cyberopérations ; la communication ; et, enfin, l'établissement de partenariats d'innovation avec l'industrie et le monde académique.

Au-delà du monde industriel, scientifique ou même associatif, notre capacité de cyberdéfense s'inscrit au carrefour d'un important réseau d'acteurs. Au sein de la Défense, l'équipe de projet participe au processus de réorganisation du SGRS en appui de son équipe de transition et est naturellement partie prenante des réflexions qui touchent à la future organisation de la Défense. Par ailleurs, le Cyber Command entend s'inscrire comme un acteur important de la collaboration interdépartementale avec entre autres le Centre for Cyber Security Belgium (CCB), la police, le parquet, le SPF Affaires étrangères ou la Sûreté de l'État (VSSE) et contribuera, en collaboration avec d'autres départements, à la définition d'orientations stratégiques et l'identification de cadres normatifs au sein de l'OTAN et de l'UE.

La construction d'un outil de défense est toujours le fruit d'un effort concerté qui ne peut que s'envisager sur le long terme. Il faut 15 ans pour acquérir une nouvelle capacité, mais il suffit d'une signature pour la détruire. Dès lors, pour que ce projet réussisse, il sera vital d'inscrire le trajet d'évolution du Cyber Command dans la durée et de garantir la pérennité des investissements financiers, humains et matériels, au-delà de l'horizon temporel des législatures. Cette tâche n'incombe pas uniquement à la Défense.

Mots-clés : Cyber, SGRS, ADIV