DÉFENSE

Cyberespace, le nouveau champ de ba

Intrusion dans une chambre d'hôtel et exfiltration de données, un type d'opération fréquent, sans qu'on nous en dise davantage. © PIERRE-YVES THIENPONT.

Ce mercredi, la Défense inaugure son Cyber Command, première étape vers la création d'une cinquième composante dans l'armée belge, la composante cyber. Plus qu'un renforcement des effectifs et un nouvel organigramme, c'est une dynamique inédite que veut insuffler l'état-major.

REPORTAGE

JOËL MATRICHE

Bruissements et murmures, que du silence, bref, « se méfier des voisins, fermer les rideaux, ne pas parler, être discret », raconte Chris (tous les prénoms de cet article ont été modifiés), un civil employé depuis cinq ans par le Service général de renseignement et de sécurité (SGRS) belge. Pour *Le Soir* et *Knack*, le service Forensic du SGRS a accepté de simuler, dans un dortoir du quartier Reine Elisabeth à Evere, une intrusion dans une chambre d'hôtel et une exfiltration de données. « C'est le genre d'opération que nous menons fréquemment », poursuit Chris, sans plus de précision. Le service de renseignement a beau vouloir communiquer, c'est à pas très feutrés.

Habillés de la façon « la plus neutre possible, afin de ne pas éveiller l'attention », gantés « pour ne pas laisser de traces », Chris et Tony pénètrent dans la chambre, la photographient sous toutes les coutures afin que chaque objet conserve sa place originelle à la fin de la visite, repèrent clefs USB, ordinateur et téléphone portable, en copient l'intégralité des données en quelques minutes seulement. Et rebroussent chemin. Ni vus, ni connus. « Que ce soit dans une chambre d'hôtel ou une habitation, tu rentres dans la vie personnelle des gens, ça fait bizarre », commente Chris. « Même mes proches ne savent pas ce que je fais exactement comme métier, je ne peux pas leur raconter mes journées. » « On sait que je travaille dans la sécurité informatique mais je ne donne aucun détail », enchaîne Tony.

Nouveau théâtre d'opérations

Créée il y a dix ans, la direction cyber des renseignements militaires se focalise sur la couche cyber logique (transmission de virus, notamment) dans le cadre de la sécurité de l'information et du renseignement. Mais ça ne suffit pas : il faut en effet développer une approche intégrée avec les couches physiques (câbles, réseaux, transmissions satellites) et virtuelles du cyberespace, qui a été reconnu comme milieu d'opérations par l'Otan depuis juillet 2016. Consacrée par le plan Star qu'a rendu public la ministre Ludivine Dedonder (PS) il y a quelques mois afin de définir le nouveau cadre de la Défense, la protection du cyberespace exigeait des moyens humains, technologiques et matériels accrus. Tant il est vrai, décrit le plan Star, que la maîtrise par la Belgique de l'arme cyber pourrait lui offrir « à coût relatif réduit une capacité d'action supplémentaire qui lui permettra d'être intégrée dans des actions multinationales et d'assurer une dissuasion essentielle ».

Il fallait donc passer à la vitesse supérieure : le cybercommandement officiellement mis en place ce mercredi est en quelque sorte l'état-major de cette composante cyber qui devrait être opérationnelle avant la fin de la législature. Et rejoindra donc les composantes terre, mer, air et médicale dans l'organigramme de l'armée belge.

> *Même mes proches ne savent pas ce que je fais exactement comme métier, je ne peux pas leur raconter mes journées*
>
> **Chris**
>
> Civil employé par le Service général de renseignement et de sécurité (SGRS) belge

Capacités offensives

Intégrée au SGRS, dirigée par le général Van Strythem, contrôlée à la fois par le Comité permanent de contrôle des services de renseignement (Comité R) et la commission Défense de la Chambre, cette composante bénéficiera d'ici 2030, lorsqu'elle devrait être pleinement opérationnelle, d'une enveloppe de 139 millions à laquelle il faut ajouter plus de 133 millions pour le renseignement d'origine électromagnétique (SIGINT) ainsi que plus de 12 millions pour le renseignement open source. De quoi accroître les capacités de surveillance défensives mais aussi offensives de l'armée belge dans ce nouveau théâtre d'opérations qu'est le cyberespace. « En février dernier », rappelle le capitaine-commandant Daniel, assistant du général Van Strythem, « lorsque la guerre en Ukraine a débuté, le fournisseur de réseau par satellite ViaSat a été perturbé. Vraisemblablement parce qu'il était massivement utilisé par l'armée ukrainienne. Mais cette attaque a également temporairement empêché la maintenance d'un parc de 3.000 éoliennes en Allemagne. » Réponse du berger à la bergère, des cyberattaques ont visé la Russie avec une ampleur inédite, comme l'a reconnu le ministre des Affaires étrangères russes à la mi-avril 2022 dans un communiqué. Parallèlement, l'organisation DDoSecrets, « vouée à permettre la libre transmission de données dans l'intérêt public », a délibérément mis en ligne plusieurs téraoctets de données confidentielles russes et biélorusses. « Les pays font des guerres en utilisant les dernières technologies et les guerres elles-mêmes accélèrent le changement technologique », résumait en juin dernier le président de Microsoft dans un rapport consacré au conflit russo-ukrainien.

En Belgique, le réseau des Affaires étrangères a subi en 2019 une tentative d'intrusion, des pénétrations du système informatique du SPF Intérieur ont été décelées en mars 2021 et en décembre dernier (lire ci-contre), c'est aux serveurs de la Défense que se sont attaqués des pirates, vraisemblablement chinois.

Chien de garde de ce nouvel espace d'affrontement, la nouvelle composante devra aussi pouvoir contre-attaquer, porter le fer en dehors de nos lignes, comme le précise le général Van Strythem : « A la manière d'un sniper car s'il est en mission d'observation 99,9 % du temps, il peut, sur ordre, tirer de façon précise, sans dommages collatéraux ou en les limitant au maximum. »

Difficultés de recrutement

Dans un bâtiment adjacent au dortoir que Chris et Tony ont réquisitionné pour leur démonstration, Niels est penché sur deux ordinateurs portables : le sien et un autre, Bluetooth activé, qui servira de cible. Pour *Le Soir* et *Knack*, en visite – très encadrée – de deux jours au siège bruxellois du SGRS, ce trentenaire accepte de prendre le contrôle d'un PC distant. En quelques dizaines de secondes, l'intrusion est terminée en s'appuyant sur Bleedingtooth, un ensemble de failles affectant le protocole Bluetooth et connu depuis 2020. Quelques lignes de code et poignées de secondes supplémentaires lui suffisent pour s'arroger des droits d'administrateur sur l'ordinateur ciblé et ainsi en exfiltrer n'importe quelle donnée à l'insu de sa cible. « Ce type d'attaque est efficace jusqu'à dix mètres de distance », précise Niels. « Il faut juste connaître l'identifiant Bluetooth de l'adversaire, ce qui nécessite quand même un travail préalable de reconnaissance. »

Docteur en informatique, passionné par la programmation depuis qu'il est « très jeune », Niels aurait pu tenter une carrière académique ou rejoindre une société privée de sécurité mais il a préféré le service public, « parce que c'est important pour le pays » et pour participer à, « par exemple, prévenir des attaques terroristes ». Du pain béni pour les recruteurs des renseignements militaires.

Erik, 53 ans, a pour sa part fait une première carrière dans le privé, « dans une start-up puis pour une grosse société ». C'est parce qu'il commençait à « s'y ennuyer » qu'il a un jour tout plaqué pour reprendre le chemin de l'université, version doctorat en cybersécurité. C'est en postulant sur la plateforme egovselect.be, en charge du recrutement de personnel IT pour le gouvernement fédéral, qu'il s'est retrouvé devant un poste de travail du SGRS. « Je suis malware analyst », décrit-il. « Je traque ces logiciels malveillants, je cherche comment on peut s'en débarrasser, j'essaye d'identifier leurs auteurs… »

Aux côtés d'Erik, Lea et Anabelle sont de formation militaire : la première, 22 ans, a rejoint les rangs sitôt bouclées ses humanités puis est devenue analyste réseau au SGRS. La seconde, 39 ans, éclaireuse-voltigeuse depuis 2006 puis informaticienne, a rejoint Lea à la surveillance des réseaux. Une carrière, disent-elles, où « on ne s'ennuie pas » mais qui oblige à travestir la réalité lors des repas de famille : « Mes parents savent que je suis informaticienne à la Défense mais ils ne connaissent pas les détails. »

« Nous recrutons sans cesse mais la concurrence est rude, notamment avec le secteur privé, tout le monde pêche dans le même vivier », commente le commandant Daniel. Beaucoup de nouveaux venus sont présentés par le Selor et egov mais ce parcours est réservé aux titulaires d'un master ou au moins d'un baccalauréat. De nouvelles portes d'entrée ont été aménagées ou sont en passe de l'être, en collaboration notamment avec MolenGeek et Bruxelles Formation. « Les hackers par contre, n'en déplaise aux amateurs de films américains, n'ont pas été la priorité de nos recrutements. Ils n'ont pas de diplôme reconnu par le Selor… »

Une nouvelle dynamique

« Il fallait créer quelque chose de neuf, partir d'une page blanche », résume le commandant Daniel. A charge donc du cybercommandement officiellement lancé ce 19 octobre de développer non un simple corps d'armée supplémentaire qui synchroniserait des compétences hier encore éclatées entre le SGRS et la Défense mais une nouvelle approche intégrée. Non seulement avec les acteurs traditionnels de la stratégie cyber en Belgique mais aussi avec la société civile, l'industrie, le milieu académique.

En recherche & développement, un partenariat a été ratifié avec la société anversoise Innocom afin de transférer à la Défense le savoir-faire de l'américain Lockheed Martin, constructeur des F35, en matière de sécurité électronique. Des liens ont aussi été tissés avec les principaux acteurs de la cybersécurité, notamment Orange Cyberdefense, Proximus, RHEA Group, Naval Group, Nviso, IBM…

Les échanges avec le milieu universitaire se font via l'Ecole royale militaire (ERM). « Notre groupe travaille avec le SGRS depuis 1993 », précise Julien Petit, chargé de cours au département de mathématiques à l'ERM et responsable du groupe de cryptographie et sténographie. « En développant notamment des outils sur mesure, par exemple des générateurs de nombres aléatoires pour les outils de cryptage. »

JO.MA.