Affronter la tempête cyber

GCA Éric BUCQUET

Directeur de la Direction du Renseignement et de la Sécurité de la Défense (DRSD)

Ministère des Armées

L'attaque *SOLARWINDS* d'une sophistication incroyable visait le pré-positionnement d'agents logiciels dormants dans des systèmes d'information sensibles ou critiques aux États-Unis.

L'attaque de l'opérateur d'oléoducs *COLONIAL PIPELINE* a généré une crise de plusieurs jours sur toute la côte Est des États-Unis privée sa principale source de carburant et de kérosène.

Le récent siphonage des données de 700 millions d'utilisateurs de LinkedIn représente autant de possibilités par rebond de cyber malveillances, d'escroqueries ou de fraudes en tous genres, etc. La revente de données volées à des services de renseignement étrangers est désormais une option qu'il ne faut pas exclure.

Ces trois exemples récents sont symptomatiques du climat cyber actuel. La croissance du nombre d'attaques, de leur diversité, de leur intensité et de leur sophistication ne semble avoir aucune limite, aucune frontière. Les groupes mafieux se sont professionnalisés, certains ont formé des cartels, et ont acquis une telle expertise offensive que certains États n'hésitent pas à faire appel à leurs services

Selon l'agence européenne de cybersécurité (ENISA), 38% des acteurs malveillants seraient rattachés à des États-nations[1].

A quel type d'attaque cybernétique majeure, la France numérisée doit-elle se préparer ?

Les services spécialisés de l'État seront-ils en mesure de prévenir ou de faire face à un cataclysme numérique d'ampleur nationale ? Comment affronter la Tempête Cyber ?

De l'amplitude et l'intensité d'attaques préoccupantes

Une prise de conscience progressive de la menace est palpable, mais la réalité de cette dernière est probablement sous-estimée.

Le Président Macron déclarait, le 18 février 2021, à propos de la menace cybernétique, qu'elle était « extrêmement sérieuse, parfois vitale et touchait tous les secteurs ».

Interrogé par la commission des Affaires européennes du Sénat, le directeur général de l'agence européenne de cybersécurité (ENISA), Juhan Lepassaar a donné des chiffres vertigineux. En 2020, le coût des cybercrimes

[1] https://www.enisa.europa.eu/publications/report-files/ETL-translations/fr/etl2020-cyber-espionage-ebook-en-fr.pdf

s'est élevé à 5,5 milliards d'euros, un chiffre multiplié par deux par rapport à l'année précédente.

Pour l'ANSSI, « c'est fois 4. Il y a véritablement une explosion ». Et encore, ces chiffres ne recouvrent donc que les cas de rançonnage sur lesquels l'agence nationale a été amenée à intervenir. C'est ainsi que Guillaume Poupard a caractérisé la situation sur le front des cyberattaques stratégiques, en France, en 2020. Il identifie trois grandes menaces : l'espionnage « c'est une menace dont on ne parle pas », la grande criminalité, et « des risques quasiment militaires ». Sa conclusion est très claire : « l'impact sur notre sécurité nationale serait maximal », si d'aventure un acteur malveillant venait à passer à l'offensive.

Notre culture stratégique nationale comme celle de nombre de pays occidentaux s'est concentrée sur la défense de nos intérêts vitaux établissant une liste confidentielle d'environ 250 entreprises basées en France dans 12 secteurs d'activité.

Pour autant, leur talon d'Achille vient le plus souvent de leurs chaines d'approvisionnement, ces centaines et milliers de PME/ETI, sous-traitants plus ou moins vulnérables de nos institutions et des grands groupes du CAC40. Pour le périmètre des entreprises de la sphère de défense dite « BITD »[2] ce sont ainsi 4 000 entreprises soit plus de 200 000 personnes dans un écosystème critique pour notre souveraineté nationale, sur lesquelles veille la DRSD en proximité. Ajoutons à ce chiffre les 10 000 entités suivies au titre de la protection du potentiel scientifique et technique de la Nation.

Le protocole signé le 4 mars de cette année entre la ministre des Armées et cybermalveillance.gouv.fr (GIP ACYMA) a permis au ministère, et à la DRSD qui le représente, de disposer d'une vision plus élargie de la cyber malveillance en France.

Ainsi, le bilan 2020 du dispositif Cybermalveillance.gouv.fr est éclairant et le constat que fait Jérôme Notin, directeur général du GIP ACYMA est clair : il existe de très fortes similitudes, à quelques nuances près, entre les professionnels du public et ceux du privé ayant requis une assistance. Cela tend à démontrer que ces deux catégories de publics sont touchées par les mêmes phénomènes cybercriminels dans des proportions comparables. En progression de 30%, les vagues d'attaques par rançongiciels sont devenues en 2020 la principale menace à laquelle les professionnels ont été confrontés. Les chiffres du 1er semestre 2021 confirment que les rançonnages tiennent la première place des attaques, immédiatement suivis par les piratages de comptes en lignes qui font un bond depuis l'assouplissement des mesures sanitaires et la conséquente reprise d'activité.

Jérôme Notin fait, par ailleurs, état de 837 entreprises touchées en 2020, contre 667 en 2019. Une chose est certaine, l'écart dans l'observabilité effective des attaques est énorme et Jérôme Notin est lui-même certain de ne pas disposer d'une image complète de la situation réelle.

Nous n'avons tous qu'une image partielle. La DRSD contribue à la définition d'une image globale de la menace.

Quel serait alors l'impact d'une tempête cyber sur le territoire national ?

C'est une question fondamentale qui concerne l'ensemble des services de l'État et un grand nombre d'opérateurs privés car elle sous-tend notre stratégie nationale de cyberdéfense. Mais je vais essayer d'y répondre simplement et, afin éclairer cette réflexion, je ferai le parallèle avec les 2 tempêtes d'origine naturelle qui ont successivement ravagé la France en décembre 1999.

Le 26 décembre, un premier passage ravage le nord de la France, provoquant de nombreuses victimes et des dégâts sur les habitations et sur les réseaux d'infrastructure (routes, téléphone, électricité). Les services de secours sont saturés d'appels, ne peuvent intervenir partout à la fois et l'opérateur EDF est

[2] BITD - Base industrielle et technologique de défense.

totalement débordé par l'ampleur des travaux d'assistance des usagers et les réparations de son réseau. La seconde tempête, 24 heures plus tard, ravage le sud de la France, provoquant un chaos supplémentaire. Malgré une solidarité exemplaire et une mobilisation collective, en faisant appel à des réservistes et des retraités, le bilan humain et matériel sera lourd et le retour à la normale prendra des mois.

Les ravages numériques causés lors d'un conflit dans le cyberespace par des bataillons de cyberattaquants seraient similaires aux effets des éléments naturels déchainés. A ce chapitre, l'attaque mondiale SOLARWINDS est un avertissement fort : une cyberattaque de ce niveau de sophistication, initiée à des fins de sabotage ou de destruction systémique, n'épargnerait personne.

Notre devoir est de nous préparer collectivement à ces « cyber tempêtes » qui seront fulgurantes. Ce n'est pas le jour de la tempête qu'il faudra construire les liens entre tous les acteurs publics et privés concernés. La DRSD s'emploie au quotidien à construire la confiance avec les entreprises dont elle a la charge.

Cela pourrait paraitre paradoxal pour un service tel que la DRSD mais quand bien même nous nous qualifierions de « service de renseignement discret », le brin d'ADN endémique de notre direction est bel et bien la protection du secret de la Défense nationale. Ainsi, depuis 150 ans, nous veillons à la sécurité physique et depuis une quarantaine d'année à la sécurité numérique de l'écosystème de défense français face aux menaces TESSCO[3].

Comment se préparer aux pires et aux moins mauvaises météo cyber ?

Premier point : Anticiper l'indisponibilité des systèmes d'information et de communication. Notre action commence tout d'abord par de la sensibilisation et de la formation de populations très diverses, des dirigeants d'administrations ou d'entreprises aux collaborateurs en passant par les officiers de sécurité et les responsables de la sécurité des systèmes numériques.

J'utilise volontairement cette sémantique de « systèmes numériques » car notre compétence porte à la fois sur les traditionnels systèmes d'informations et sur les systèmes électroniques de sécurité (contrôle d'accès ou d'intrusion, vidéoprotection, etc.).

En 2020, malgré la pandémie, le Service a mené 230 actions de sensibilisation de PME/ETI dans les territoires et 7 auprès des COMEX de grands groupes de défense essentiellement localisés en Ile de France. Selon le public ciblé plusieurs formes de sensibilisations peuvent être offertes, de la présentation de type « PowerPoint » à la simulation ad hoc d'attaque cyber par ingénierie sociale, en passant simulation générique d'attaques de type vol de mot de passe ou rançonnage (avec notre plateforme CENTAURE).

Nous avons également un rôle d'audit et de contrôle du respect des lois et règlementations, garantissant le secret de la défense nationale. En 2020, plus de 130 inspections ont ainsi été effectuées dont 85% en milieu industriel.

Dans le contexte actuel de crise sanitaire, « l'industrie de défense est dans l'œil du cyclone ». Cette phrase est tirée de l'excellent rapport d'information n° 605 (2019-2020) de messieurs Pascal Allizard et Michel Boutant, fait au nom de la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat, déposé le 8 juillet 2020.

Conjugué à l'explosion du cybercrime, c'est notre écosystème de défense qui est structurellement menacé. Nous avons par conséquent engagé des travaux de transformation de notre mission historique de contrôle règlementaire vers une logique démultipliée de connaissance partagée des failles et vulnérabilités et des menaces, de conseil, pragmatique

[3] TESSCO - Terrorisme, espionnage, subversion, sabotage, crime organisé.

basé sur des cas réels, et d'assistance à la maitrise du risque numérique.

Cette maitrise du risque et le renforcement des fondamentaux de la cybersécurité, les bonnes pratiques d'hygiène informatique sont des prérequis au bon fonctionnement des entreprises en temps normal. Ils ne suffiraient probablement pas à éviter des bataillons de cyberattaquants de niveau étatique mais cela permettrait de se relever, de redémarrer plus rapidement et plus facilement après la tempête.

Par ailleurs, dans le cadre de la convention cyberdéfense signée par le ministère des Armées et 8 grands maitres d'œuvre industriels, un travail conséquent a été accompli sur le volet capacitaire aboutissant à la constitution d'un groupe sectoriel des CSIRTs de défense doté de règles de gouvernance et d'outils de partage communs.

Cette phase de développement capacitaire est suivie par une phase de préparation opérationnelle, de formation et d'entrainement aux opérations de cybersécurité au profit de l'ensemble de l'écosystème de défense, des plus forts aux plus fragiles. La DRSD entend bien assumer ses responsabilités aux cotés de l'ANSSI pour ce qui concerne les OIV de défense et sur l'ensemble des 4000 TPE/PME/ETI de la BITD.

Avis de tempête

A l'opposé des prévisions météorologiques, il n'existe pas à ce jour de modélisation prédictive des attaques dans le cyberespace à l'échelle mondiale ou nationale.

Pour autant, certaines manœuvres de groupes malveillants peuvent être observées et concourir à anticiper des postures d'attaque. Cette connaissance des menaces, plus ou moins focalisées, plus ou moins stratégiques, est partagée dans des cercles restreints d'analystes et experts en cybersécurité du secteur public et du secteur privé, en France, en Europe et dans le monde. La consolidation et le partage de ces données techniques sur les cybermenaces que l'on appelle communément « *CTI - Cyber Threat Intelligence* » permettrait de mieux anticiper les attaques et par conséquent d'être en mesure de produire des avis de vigilance cyber voire des avis de tempête transcendante sur le cyberespace. L'objectif est d'avoir et de partager une vision plus large et exhaustive de la menace.

Comment venir au secours des victimes les plus fragiles ?

L'enjeu premier n'est pas de comprendre les causes, mais de pallier les conséquences déstabilisant l'organisation sociétale.

Il s'agit donc pour les décideurs face à une catastrophe naturelle de masse, de classer, prioriser et coordonner l'action des services de secours spécialisés, qui dans l'assistance aux personnes, qui dans la réparation de services vitaux, qui dans la logistique ou l'acheminement des moyens de secours matériels et humains, etc.

En matière cyber l'approche est très comparable. Le secrétariat général de la défense nationale (SGDSN) dans la dernière revue de la stratégie nationale de cyberdéfense[4] a introduit le concept de classement des attaques informatique selon la gravité de l'événement de 0 à 5. Cet outil d'aide à la décision a été adopté par l'ANSSI, le COMCYBER et de nombreux CSIRTs en France.

Il est désormais intégré dans la doctrine d'engagement des éléments d'intervention cyber de la DRSD (cf. infra). Au-delà de son usage collectif à l'échelle nationale, il permet de construire une vision partagée de la situation opérationnelle cyber dans l'union européenne et devrait favoriser la collaboration internationale de réponse à incident majeur.

En ligne avec la LPM 2019-2025[5], le renforcement capacitaire de notre direction est continu ; notre effectif a augmenté passant de 1330 agents en 2018 à

[4] SGDSN - Revue nationale de cyberdéfense - 12 février 2018.

[5] LPM - Loi du 13 juillet 2018 relative à la programmation militaire pour les années 2019 à 2025.

plus de 1500 agents en 2020, dont 30% de femmes, 32% de civils.

40 postes supplémentaires du domaine cyber sont à pourvoir d'ici 2025.

Le renforcement capacitaire porte notamment sur la mise en place d'une capacité de réponse aux compromissions de systèmes numériques : l'élément d'intervention cyber (EIC).

Cette force d'intervention actuellement positionnée auprès de notre SOC (Security Operation Center)[6] en région parisienne constitue l'élément fondateur du CERT DRSD. Cette capacité sera progressivement développée dans l'ensemble de nos directions en régions au gré de recrutements d'ingénieurs et techniciens cyber et de formations dispensées par notre propre centre de formation ou par des prestataires spécialisés. Cette capacité de primo intervention de proximité et la combinaison d'expertise métiers ou techniques, est une des clés de la réponse aux cyberattaques du quotidien.

En cas d'agression d'ampleur, elle serait mobilisée aux côtés des autres services de l'État à l'échelon interministériel et au niveau des zones de défense et sécurité pour répondre le plus efficacement possible aux nombreuses demandes d'assistance des victimes sur l'ensemble du territoire national et pour appuyer la phase de reconstruction éventuelle des lignes de défense.

Cette organisation générale repose sur la disponibilité d'outils critiques de communication, communs ou interopérables, assurant une circulation fluide de l'information. De ce point de vue, nous pouvons dire que la crise du COVID aura été un accélérateur de modernisation de ces outils de communication et de partage rapide. Il n'en reste pas moins que certains outils restent propres à certains services de l'État comme c'est le cas à la DRSD et c'est une force en soit car la redondance de plateformes numériques prendrait tout son sens si une autorité venait à être impactée par le cataclysme d'origine cybernétique.

Quid de la coopération européenne ?

L'ancien chef du CERT-FR de 2017 à 2019, représentant la France dans le réseau des centres de cybersécurité nationaux de l'UE - le *CSIRT Network* - me disait combien la construction de la cyberdéfense européenne avait drastiquement progressé en quelques années au bénéfice des services essentiels tels que définis par la première directive SRI[7] - *NIS directive* – malgré les différences historiques ou culturelles des approches nationales.

La prochaine mouture de cette directive NIS, au spectre sectoriel élargi, la création officielle fin 2020 du réseau CyCLONe (Cyber Crisis Liaison Organisation Network)[8] sont la suite logique du travail de coopération des États membres pour se préparer et répondre en cas d'incident cyber d'ampleur ou de crise transfrontalière. Gageons que CyCLONe et l'ensemble des cyberforces vives en France seront suffisamment puissants pour faire face, unis, aux attaques tempétueuses contre nos services essentiels voire vitaux !

Pour une « Boussole stratégique » cybersécurisée

Cette dynamique de coopération cyber du domaine civil transnational gagnerait à être instillée au domaine des activités de défenses domestiques, très souvent souveraines alors même que nos champions industriels ont de leur côté noué de nombreux partenariats à l'international, et que la structuration d'une défense européenne progresse. Un potentiel axe de réflexion pour le volet cyber de la prochaine présidence française du conseil de l'UE.

---

[6] SOC - Le centre opérationnel de sécurité assure la supervision des systèmes d'information au sein d'une entité afin de se protéger des cyberattaques.

[7] La loi française de transposition de la directive européenne 2016/1148 de sécurité des réseaux et de l'information (*Network and Information Security - NIS*) du 6 juillet 2016 a été promulguée lundi 26 février 2018.

[8] CyCLONe - Réseau de coopération stratégique des Etats membres de l'union européenne.