Manœuvrer dans le cyberespace

Laurent Prosperi

laurent.prosperi@ens-paris-saclay.fr

21 octobre 2020

Dans *La mesure de la force*, le cœur de la problématique décisionnelle de toute stratégie est de « sélectionner des options stratégiques (offensives ou défensives) et de les traduire en terne de manœuvre. » [1] La manœuvre désigne « la combinaison d'actions planifiées, dans l'espace et dans le temps, menées dans un domaine particulier et contribuant à atteindre l'objectif fixé, dans le cadre de la mission ». Le cyberespace est un terrain favorable au développement de la conflictualité contemporaine. C'est un espace « englobant » et transverse, dans le sens où il conditionne le bon déroulement des opérations militaires mais aussi le bon fonctionnement de la société.

Nous allons adopter une définition opérationnelle du cyberespace s'appuyant sur la théorie des « trois couches » [2] afin de faciliter et segmenter l'analyse. La première est *matérielle*, elle est composée de l'infrastructure (câbles, satellites, serveurs et datacenters), des périphériques d'accès (postes de travail, objets connectés) et elle rassemble tout ce qui traite du matériel électronique (comme les microprocesseurs). Les attaques ciblant cette couche sont difficiles à mettre en œuvre mais dans le même temps dures à mitiger du fait de la longue durée de vie des systèmes physiques. La seconde est *logicielle*, elle peut être découpée en deux sous-couches, selon Frédérick Douzet [3]. D'une part, l'infrastructure logique assure la transmission de l'information entre deux points et le fonctionnement des systèmes (par exemple un système d'exploitation). D'autre part, la couche applicative permet aux utilisateurs

1. M. Motte et al. *La mesure de la force*. Thallandier. Paris, 2018, p. 94.
2. D. Ventre. « Le cyberespace : définitions, représentations. » In : *Revue Défense Nationale* 751 (2012), p. 33.
3. F. Douzet. « La géopolitique pour comprendre le cyberespace ». In : *Hérodote* 152-153.1 (2014), p. 3-21.

d'interagir avec le cyberespace (par exemple un gestionnaire de mail, un moteur de recherche ou un navigateur internet). La troisième couche est *sémantique*, c'est le lieu des interactions sociales entre utilisateurs. C'est la couche des dimensions sociale et informationnelle. Bien qu'utile pour se représenter le cyberespace, ce découpage en strates ne doit pas figer l'analyse : le plus souvent, les actions et les phénomènes sont transverses à plusieurs couches, ou s'appuient sur des propriétés des couches sous-jacentes. Chacune de ces couches est un terrain d'affrontement entre acteurs allant de la pose de bretelles sur des câbles sous-marins à la déstabilisation politique pendant des campagnes électorales.

Analyser la manœuvre dans le cyberespace nous amène à définir les objectifs canoniques des opérations (Section 1) avant de s'intéresser aux actions offensives menées dans les couches logiques (Section 2) et sémantique (Section 3). Dans un second temps, nous décrirons l'anatomie des actions de défense (Section 4) avant de poser la question de l'attribution d'une opération adversaire (Section 5), point conditionnant une possible réaction.

1 Les objectifs canoniques d'opérations

Les objectifs des assaillants sont très divers et le plus souvent flous, cependant six grandes catégories non exclusives peuvent être distinguées : l'espionnage, la cybercriminalité (trafics illicites, arnaques, extorsion des données, d'argent), la déstabilisation souvent informationnelle, le sabotage d'infrastructures (par exemple la destruction des centrifugeuses iraniennes par le virus Stuxnet est l'une des premières campagnes de sabotage connues), la destruction de ressources cyber (mise hors d'état d'un serveur) et la coercition.

Pour atteindre leur but, les attaquants disposent de multiples modes d'action pouvant être combinés. Les plus courants se repartissent entre ceux ciblant directement l'humain comme le (spear-)phishing [4], l'arnaque au président, l'ingénierie sociale et l'usurpation d'identité ; et ceux à dominante technique comme la compromission à travers l'exploitation de failles zéro-days [5]. Dans la majorité des cas, l'erreur humaine couplée à un système non à jour représente la porte d'entrée principale. Une attaque cyber se matérialise sous diverses formes, les plus connues étant

4. Le phishing (ou hameçonnage) repose traditionnellement sur un mail générique contenant (ou redirigeant) vers un code malveillant. Le spear-phishing est une variante dans laquelle les messages envoyés sont personnalisés.

5. Ce sont des vulnérabilités inconnues de l'éditeur et ne disposant pas de correctifs.

les rançongiciels, les attaques par dénis de service pour paralyser un système, l'utilisation de malwares contre une infrastructure précise [6], l'utilisation de virus avec un spectre plus large voire atteignant un ciblage de masse [7] (comme pour NotPetya) et l'injection de code arbitraire dans des logiciels ou plateformes existants (vecteur principal lors du défacement de site web).

L'espionnage cyber constitue le gros de l'emploi étatique. En date du 5 février 2019, il représente 237 cas sur 288 attaques attribuées à des États depuis 2005 selon le Council on Foreign Relations cyber operations tracker [8]. Une interaction profonde existe entre les actions cyber et les méthodes du renseignement. En plus de représenter l'objectif central d'un nombre important d'opérations, la majorité des actions offensives cyber nécessite une première phase de repérage (à minima technique) et même d'espionnage [9] afin de délimiter l'objectif ainsi que les capacités adverses de réaction. Par ailleurs, le cyber sert d'amplificateur aux opérations d'espionnage en rendant possible une surveillance de masse en temps réel comme les révélations d'Edward Snowden l'ont montré. La tendance à l'augmentation des débits avec l'arrivée de la 5G et le développement d'une couverture satellitaire importante (avec les projet Starlink de SpaceX et OneWeb) va favoriser l'espionnage et limiter la marge de manoeuvre de la défense [10] car le temps d'exfiltration des données sera fortement réduit (par plusieurs ordres de grandeur suivant les cas) et la détection compléxifiée car les indices vont être noyés dans la masse.

Ensuite viennent les actions de sabotage, souvent perçues comme la forme canonique de la menace par la population du fait de la forte médiatisation [11] en allant de Stuxnet, un virus ayant endommagé les centrifugeuses iraniennes utilisées pour enrichir de l'uranium à la fin des années 2000, à NotPetya en passant par Wannacry. Les deux derniers ont défrayé la chronique en 2017 avec l'infection de plusieurs centaines de milliers de machines dans le monde et la paralysie de certaines entreprises comme Saint-Gobain.

Enfin, ces dernières années ont été témoin d'une recrudescence d'opérations dans la sphère informationnelle, le plus souvent non motivées par des inquiétudes d'ordre

6. C'est une entreprise longue et coûteuse nécessitant plusieurs mois (années) de préparation.
7. Notamment, dans le cas d'extorsion de données, d'argent ou dans le cas d'un perte de contrôle de la propagation de la charge utile
8. Q. E. Hodgson et al. *Fighting Shadows in the Dark : Understanding and Countering Coercion in Cyberspace*. Santa Monica : CA : RAND Corporation, 2019, p. 1.
9. O. Kempf. « Du cyber et de la guerre ». In : *Fondation pour la recherche stratégique* (Note n°17/2019 12 septembre 2019), p. 5.
10. *Entretien réalisé le 3/07/2020 avec un responsable de la DGSI.*
11. Kempf, op. cit., p. 6.

militaire mais plus par la diffusion et le contrôle de contenus [12] (Sony Pictures en novembre 2014) ou par la volonté d'influer indirectement sur les choix politiques d'une nation. En Occident, l'aspect informationnel du cyberespace a été délaissé à la fin des années 1990, il n'est revenu sur le devant de la scène qu'à partir de la deuxième moitié des années 2010 sous la pression du terrorisme et des ingérences extérieures dans les processus électoraux suite à l'élection présidentielle américaine de 2016 entachée par des actions de déstabilisation menées sur les réseaux sociaux. Il en va différemment de la Chine, de la Russie et de l'Iran qui perçoivent la sphère informationnelle et la libre circulation de l'information comme la menace principale contre la stabilité des régimes, provenant de l'Occident (à cause du principe de libre expression et du concept de propriété intellectuelle). Plus généralement, le cyber est un vecteur de choix pour des actions de propagande ou de désinformation par la pénétration croissante des usages numériques dans nos sociétés.

2 Anatomie d'une cyberattaque

Prenons l'exemple d'un ransomware (Figure 1). L'opération commence par le choix des outils, soit en se fournissant auprès de tierces personnes (sur un marché parallèle ou légalement) soit en les développant en interne. Pour réaliser une attaque, l'assaillant s'appuie sur une cyber armurerie (détecteur de failles, implants, canaux de communication, outils de contrôle, infrastructure pour garantir son anonymat) et sur une infrastructure de commande-contrôle permettant de contrôler discrètement la charge utile une fois celle-ci mise en place. Pour ce faire, l'attaquant peut utiliser des botnets ou des réseaux d'anonymisation, l'idée étant de se fondre dans la masse. Enfin, il lui faut, si besoin, une infrastructure d'exploitation pour exfiltrer les données. Celle-ci doit être discrète et fournir la bande passante nécessaire ; ces deux propriétés sont inversement proportionnelles, le défi à relever est de trouver le juste milieu à une situation données. À moyen terme, la question ne se posera plus avec l'augmentation de la bande passante promise par la 5G et le développement de la connectivité par satellite. Au-delà de l'aspect technique, un assaillant de premier plan (étatique ou un APT) doit disposer de ressources humaines qualifiées et en nombre pour pouvoir mener de multiples opérations en parallèle, chacune d'entre elles immobilisant des ressources pendant de longues durées.

12. « Cybersécurité : Extension du domaine de la lutte ». In : *Politique étrangère* 2 (2018), p. 9-230, p. 11.

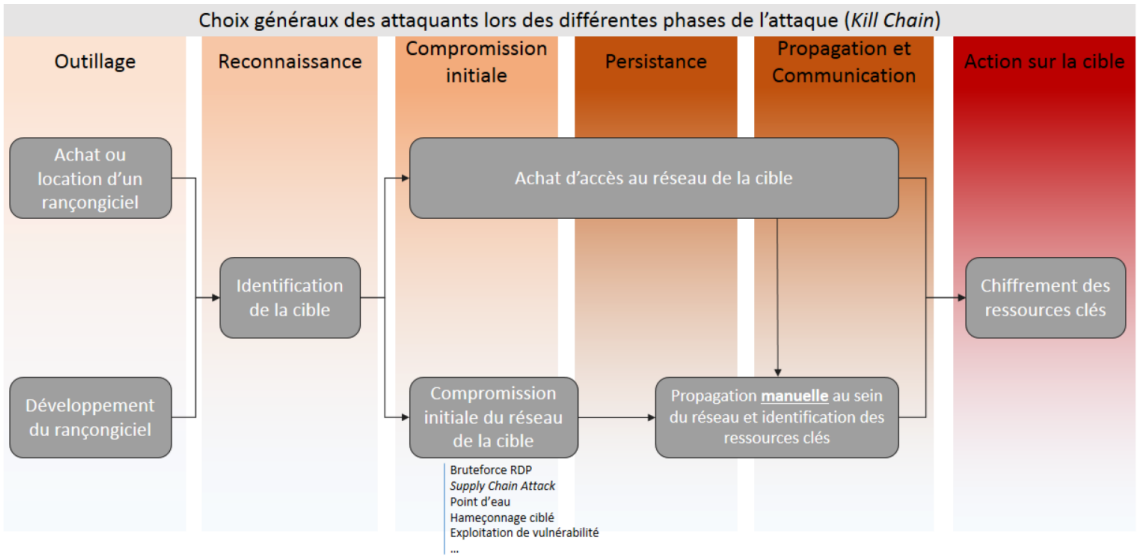

FIGURE 1 – Choix généraux lors des différentes phases d'une attaque dans le cadre d'un ransomware [a]

a. ANSSI. *Etat de la menace rançongiciel à l'encontre des entreprises et des institutions*. 5 février 2020, p. 9.

L'attaque proprement dite se déroule en quatre temps [13] en commençant par la reconnaissance de la cible qui peut durer de quelques secondes (dans le cas d'une attaque à spectre large) à quelques semaines voire quelques mois dans le cadre d'une attaque ciblée. Il s'en suit l'introduction dans le système à l'aide d'une erreur humaine, d'une intervention physique (brancher une clé USB sur un serveur) ou d'une exploitation technique allant de l'utilisation de vulnérabilités déjà connues mais non protégées, d'un système mal configuré à l'exploitation de failles zéro-days. Une fois la compromission initiale réussie commence l'installation des implants pour perdurer et la latéralisation afin de compromettre d'autres parties encore saines de l'infrastructure cible. Notons que dans certains cas l'accès à l'infrastructure d'une cible peut être acheté ou loué sur le marché noir. Enfin, l'attaque se finit par l'exploitation du système, cela va de l'extraction d'informations à la destruction du système (données, réseau ou sabotage) ou à la corruption des données. En pratique, la séparation en quatre temps est brouillée, l'extraction de données peut débuter dès la compromission initiale afin de découvrir des réseaux et des systèmes inaccessibles jusque là ou alors l'extraction nécessite de compromettre un (ou plusieurs) système intermédiaire pour atteindre l'infrastructure cible, de même l'exploitation d'un système compromis peut ne pas avoir lieu afin de bénéficier d'une utilisation "instantanée"

13. SGDSN. *Revue stratégique de cyberdéfense*. 2018, p. 19.

au moment voulu ; ce principe, appelé prépositionnement, correspond à la mise en sommeil de charges utiles au sein d'un réseau ou d'une infrastructure d'une entité pour un usage postérieur instantané afin d'exercer des représailles ou dans le cadre d'un conflit futur.

3 Opérations d'influence

Les opérations d'influence (aussi appelées information warfare) sont apparues, sous cette dénomination, au sein de l'armée et de la communauté du renseignement américain dans les années 1980. Elles regroupent une grande variété d'activités liées à la guerre psychologique [14], comprenant la collecte d'informations tactiques, la validation d'informations, la propagation ou la désinformation afin de perturber la population ou les forces adverses, ou encore la lutte contre les opérations d'influence adverse. Les opérations d'influence s'articulent avec les activités diplomatiques, les opérations militaires et la contre-ingérence.

L'Occident démarre avec un temps de retard dans la prise en compte de l'importance du cyber comme vecteur d'influence. Son réveil remonte aux années 2015-2016 alors que, dès la construction du cyberespace, le contrôle de l'information et la cyberdéfense technique ont été les deux faces d'une même pièce pour la Russie et la Chine. Par exemple, les unités russes chargées de la cyberdéfense sont le plus souvent rattachées aux organisations en charge de la manipulation de l'information [15]. Aujourd'hui encore, l'influence reste assujettie à la technique et en soutien aux opérations dans la conception occidentale. Les Américains ont théorisé l'« information warfare » dans le milieu cyber comme l'utilisation de l'avancée technologique au service du contrôle de l'information. En France, le document de prospective stratégique *Action Terrestre Future* de 2016 en fait un facteur de supériorité opérationnelle et les éléments de doctrine du COMCYBER considèrent la sphère informationnelle comme l'un de leur trois terrains d'action.

Les évolutions technologiques et socio-économiques transforment l'environnement informationnel et renforcent la place du cyberespace. La création et la diffusion d'information ne sont plus concentrées entre quelques mains mais largement décentralisées (le contrôle tend à se centraliser dans les mains de quelques plateformes). Dans le même temps, le système médiatique est fragilisé par les choix économiques des médias traditionnels au détriment de l'intégrité et de la correction des informa-

14. A. Kiyuna et L. Conyers. *Cyberwarfare Sourcebook*. Lulu. com, 2015.
15. *Entretien réalisé avec un responsable de l'ANSSI.*

tions. Les individus sont eux aussi soumis à une évolution similaire, en partie du fait de l'instantanéité des communications : ils ont perdu l'habitude de vérifier et croiser leurs sources. Cela les rends d'autant plus vulnérables aux campagnes d'influence.

Les objectifs, les cibles et les concepts stratégiques des cyber opérations d'influence (CIO) sont utilisés en dehors de la sphère cyber [16]. La différence se fait au niveau des outils, des acteurs et de l'échelle, du fait des spécificités du cyberespace que sont l'instantanéité de la transmission, la propagation en exponentiel, la grande diversité de plateformes ainsi que la facilité d'automatisation des procédés et l'ubiquité du milieu [17]. Le développement des techniques de publicité ciblées fournit d'excellents outils pour définir les cibles potentielles de campagne d'influence [18].

Les objectifs principaux sont la modification de la motivation et des idées des cibles. Ils peuvent varier en fonction du contexte et inclure par exemple la déstabilisation d'une région ou, dans le cadre d'un conflit armé, s'attaquer à la volonté de se battre des forces adverses. Les cibles se répartissent en trois groupes [19] : les cibles de masse à l'échelle d'une société, souvent utilisées lorsque l'objectif est de s'attaquer à des infrastructures critiques comme un gouvernement ou un système de vote, avec des messages reposant sur les symboles et l'histoire communément partagés par la société ; le ciblage socio-démographique revient à concentrer l'action sur une région, sur une minorité ou sur le personnel militaire dans un conflit avec des messages adaptés au contexte ; le ciblage psychologique correspond à la sélection d'individus en fonction de leur profil et la mise au point d'une communication personnalisée. Les technologies actuelles commencent à permettre le passage à l'échelle du ciblage psychologique en s'appuyant sur des techniques de recommandation, alimentées par les grandes quantités de données personnelles disponibles, pour définir les cibles puis en utilisant des systèmes de synthèse automatique ou semi-automatique (en s'appuyant par exemple sur des unités de "trolls" professionnels).

La large diffusion des technologies cyber, ainsi que leur faible coup d'entrée, permettent à n'importe qui de s'engager dans des opérations d'influence à échelles variables, que ce soit des acteurs étatiques (comme des actions de déstabilisation

16. *Cyber Influence Operations : An Overview and Comparative Analysis*. Zurich : Center for Security Studies (CSS), ETH Zürich, octobre 2019, p.11.

17. Limitée par certaines mesures techniques comme par exemple les réseaux fermés et soumis à un fort contrôle comme ceux de la Chine ou de l'Iran.

18. Par exemple utilisés par la société Cambridge Analytica dans le but de mener des campagnes d'influence sur Facebook lors de l'élection américaine de 2016 ou lors du référendum concernant le Brexit.

19. J. Pamment, H. Nothhaft et A. Fjällhed. « Countering information influence activities : The state of the art ». In : (2018).

lors de l'élection présidentielle des États-Unis en 2016 ou lors du référendum du Brexit), des mouvements hacktivistes, des groupes terroristes (à l'image de Daesh), des réseaux criminels ou des individus isolés, ceux-ci pouvant s'entremêler dans une logique de faire faire et d'utilisation de proxy, notamment de la part d'États. La guerre informationnelle repose « bien moins sur des compétences techniques que sur l'impact informationnel généré par une attaque » [20] que ce soit de la part d'un acteur non étatique ou de la part d'un État . En effet, il suffit de savoir faire de la retouche d'images et utiliser les réseaux sociaux pour pouvoir se lancer dans l'influence. De plus, ces dernières années ont vu se démocratiser les techniques de "deepfake" donnant naissance à des outils faciles et assez puissants d'édition vidéo et audio, tel FaceApp qui permet de changer les visages d'une vidéo afin de faire des faux convaincants. Être en mesure de réussir et d'évaluer ces actions est cependant une autre histoire.

Les cyber opérations d'influence (CIO) peuvent être classifiées entre les opérations d'influences techniquement permises par le cyber (CeTIO) et les opérations socialement permises par le cyber (CeSIO). Les premières sont le plus souvent des opérations de Lutte informatique offensive (LIO) en soutien d'actions d'influence [21] afin de perturber la couche logique du cyber, en détruisant ou altérant des informations sur un système cible [22]. Les secondes ne nécessitent pas l'usage de capacité cyber pour altérer les couches physiques ou logiques du cyberespace, elles se concentrent dans la couche sémantique. Elles sont parfois qualifiées de "soft" opérations d'influence. Elles s'appuient sur diverses techniques comme l'achat de publicité sur les plateformes, l'analyse de données en source ouverte, la publication de contenus plus ou moins ciblés sur diverses plateformes et restent légales dans l'ensemble, à la différence des CeTIO. En effet, l'enjeu tactique est de s'adapter aux évolutions des comportements en cours : l'information de masse se transforme en information individuelle et sélective, les utilisateurs sont alors enfermés automatiquement dans des bulles, ce qui nécessite de mener des actions ressemblant au ciblage marketing. Au préalable, il faut analyser l'environnement et comprendre les mécaniques sous-jacentes. Quels sont les principaux acteurs et les enjeux locaux ? Ceci donne toute

20. Bertrand Boyer dans B. Boyer. « Les opérations sur l'environnement : la nouvelle guerre de l'information ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 209-217, p. 210

21. V. Mariel chef de bataillon. « L'influence militaire pour créer la surprise dans un champ de bataille transparent ? » In : *Lettre d'information du centre de doctrine et d'enseignement du commandement* (février 2019), p.3.

22. P. Brangetto et M. A. Veenendaal. « Influence Cyber Operations : The use of cyberattacks in support of Influence Operations ». In : *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE. 2016, p. 113-126.

sa place au renseignement d'intérêt cyber et aux États pouvant s'appuyer sur des plateformes concentrant les contenus et disposant de nombreux utilisateurs [23].

Ces opérations d'influence sont particulièrement profitables car elles permettent de saper la puissance conventionnelle d'un État en ne nécessitant que de faibles ressources et en offrant une grande flexibilité d'action. Le tout en ne prenant que peu de risques car les risques de détection puis d'attribution sont par nature faibles mais surtout parce que les stratégies d'influence restent bien en deçà du seuil d'emploi de la force limitant ainsi l'escalade et les potentielles représailles. Cependant, comme le souligne le rapport de Center for Security Studies [24], déterminer l'efficacité stratégique (directe ou indirecte) d'opérations d'influence est une chose malaisée par la difficulté à en observer les effets. Pour autant, cela ne signifie pas que de telles actions restent sans conséquence surtout si elles produisent des effets stratégiques. L'administration d'Obama a répondu économiquement et diplomatiquement (voire clandestinement) aux ingérences russes de 2016, cependant les démocraties occidentales n'apparaissent que faiblement armées pour y faire face en temps de paix : regardons le temps qu'il a fallu pour coordonner et mener des actions de contre-influence contre Daesh. Les CIO ne sont pas forcément mises en œuvre contre des puissances étrangères mais aussi dans le cadre de conflits internes comme par exemple en Syrie par les forces d'Assad. Les questions qui se posent à ce jour concernent l'évaluation de l'efficacité de ces opérations et leurs coûts réels.

4 Anatomie de la défense

La posture défense des années 1990 (et début 2000) est périmétrique, l'objectif étant de construire une sorte de muraille impénétrable autour du système à protéger pour l'isoler de l'extérieur, sans aucune restriction sur ce qui peut être fait à l'intérieur. C'est un dispositif insuffisant car la muraille ne couvre pas efficacement l'ensemble du système, la surface d'attaque est en expansion et en mutation permanentes, cela ne protège pas contre la menace d'un attaquant intérieur (que l'origine soit volontaire ou non) et la défense périmétrique devient inopérante une fois qu'un assaillant a pris pied dans un système : elle ne permet pas d'entraver sa progression. Les systèmes classiques de défense se reposant sur la combinaison classique de parfeux et d'antivirus se révèlent inefficace contre un bon tiers des at-

23. Les États-Unis avec les GAFAM, la Chine avec les BATX, la Russie avec les plateformes composant le Runet

24. *Cyber Influence Operations : An Overview and Comparative Analysis*, p. 20.

taquants [25], notamment tous ceux de haut niveau. Ces limitations ont fait émerger le principe de la défense en profondeur [26], son objectif est de ralentir et de compliquer la latéralisation. Le principe s'inspire du *swiss cheese model* [27] : les lignes de défense sont des tranches de fromage suisse alignées les unes derrières les autres de telle sorte que les trous (de sécurité) de l'une soit masqués par la suivante. L'idée est d'organiser la protection en une succession dynamique et coordonnée de lignes de défense (composées de barrières pouvant être de nature humaine, procédurale ou technique, statique ou dynamique) afin de couvrir la mise en œuvre du système et les technologies utilisées. Par ailleurs, il s'agit de mettre en place des actions de neutralisation des menaces au sein du système à défendre (n'impliquant pas d'actions offensives) et d'adapter la défense par une gestion des risques, un système de renseignement (principalement de veille) visant à connaitre les acteurs et les menaces, une planification des réactions et une politique de retour d'expérience afin d'améliorer la posture. En pratique, des assaillants compétents prennent pied dans un réseau en quelques heures, par contre, si la défense en profondeur est bien conçue, il peut leur falloir plusieurs semaines ou mois pour se latéraliser sans déclencher d'alertes [28]. À titre de comparaison, nous pouvons considérer une maison où toutes les pièces sont protégées par des portes blindées qu'un voleur, une fois dans le vestibule, doit forcer une à une sans déclencher d'alarmes.

La principale limite de la défense en profondeur est que l'utilisateur est considéré comme une menace et mis sur la touche dans la gestion de la défense. En effet, plus que la faille technique, l'humain est la porte d'entrée principale que ce soit dans le cadre d'arnaques au président, d'une campagne de phishing (vecteur de près de 90% des cyberattaques [29]) ou pour installer, volontairement ou non, un malware sur une infrastructure cible. Aujourd'hui, un nouveau concept est introduit [30] afin de mieux capturer la place centrale de celui-ci. L'objectif est d'améliorer l'expérience de l'utilisateur et de tenter de sortir de l'opposition entre cybersécurité et facilité d'usage afin de l'impliquer dans les lignes de défenses. Au niveau technique, une

25. *Entretien réalisé le 29/06/2020 avec un responsable de l'ANSSI.*

26. D. centrale de la sécurité des systèmes d'information. *La défense en profondeur appliquée aux systèmes d'information*. 19 juillet 2004.

27. J. Reason. « The contribution of latent human failures to the breakdown of complex systems ». In : *Philosophical Transactions of the Royal Society of London. B, Biological Sciences* 327.1241 (1990), p. 475-484.

28. *Entretien réalisé avec un responsable de l'ANSSI.*

29. C. Weber et C. Jean-Philippe. « De l'importance du facteur humain ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 52-59, p. 52.

30. Ce fut notamment l'un des thèmes du Forum International de la Cybersécurité 2020, ayant rassemblé près de 12 500 personnes à Lille les 28, 29 et 30 janvier 2020.

nouvelle famille de solutions appelée Endpoint Detection and Response (EDR) visant à sécuriser les terminaux (smartphones, poste de travail) est en train de voir le jour afin de compléter les mesures existantes [31]. Le principe est de placer des sondes dans chacun des terminaux, de collecter de l'information (notamment les traces réseaux, les comportements des applications) de les diriger vers un système d'ingestion et stockage [32] puis de faire du traitement statistique afin de chercher les corrélations et détecter les anomalies. Celles-ci seront alors soumises à un expert humain afin de conduire une investigation approfondie. Par ailleurs, ce type de système doit aussi répondre automatiquement aux anomalies détectées, par exemple en se dotant de règles automatiques de cloisonnement. La réponse technologique à la menace, bien qu'indispensable, n'est donc pas suffisante sans l'assistance des utilisateurs. Pour ce faire, il serait intéressant de les former et les sensibiliser, outre les mesures passives, de développer des comportements réactifs comme pour les exercices contre les incendies afin de réduire le temps de réaction en cas d'attaque, facteur de premier plan pour atténuer son impact. Par ailleurs, une politique de non sanction des erreurs et collecte de retour d'expérience pourrait être bénéfique.

L'heure est à la stabilisation des doctrines défensives [33] avec l'émergence d'un « continuum de cyberdéfense » allant de la Sécurité des systèmes d'information à la Lutte informatique offensive en passant par la Influence numérique. La première (SSI) revient à la mise en place de moyens "passifs" visant augmenter le niveau de sécurité d'un système et à prévenir des attaques potentielles (à l'aide d'antivirus et de par-feux par exemple). Ces dernières années la SSI a été partiellement délaissée au profit de la LID (et de ses méthodes de détection) au niveau institutionnelle en ne se limitant qu'a des techniques élémentaires. Certes, la ligne de défense établie par la SSI se relève inefficace contre les attaquants du haut du spectre [34] cependant elle permet de décharger les équipes (et les systèmes) de la LID en éliminant de larges gammes d'attaques et en évitant ainsi de noyer les moyens de détection. En bout du spectre se trouve la LIO qui peut servir, en défense, à prévenir ou faire cesser une attaque.

31. *Entretien réalisé avec un responsable de l'ANSSI.*
32. Le terme générique étant data lake
33. *Entretien réalisé le 21/07/2020 avec un responsable de l'ANSSI.*
34. *Entretien réalisé avec un responsable de l'ANSSI.*

5 Attribuer une opération : entre technique et politique

À la différence de la doctrine nucléaire où la certitude en l'attribution est essentielle, l'incertitude est permanente dans le cyberespace. L'attribution relève d'une volonté politique avant d'être technique : attribuer sans prendre de mesure peut être perçu comme un signe de faiblesse et réagir peut conduire à une escalade si l'adversaire a une surface d'attaque plus faible ou si la cible se révèle être un leurre. La capacité d'attribution est ainsi un marqueur de la puissance cyber. En effet, elle repose sur l'analyse de traces techniques et sur un travail de renseignement. Elle est d'autant plus compliquée par la nature des menaces de plus en plus protéiformes, émanant d'acteurs divers poursuivant des buts troubles voire multiples, et par l'utilisation d'une multitude de *proxies* : individus isolés, hacktivistes ou réseau d'activistes agissant pour des motifs politiques (ou idéologiques), hackers louant leurs services, cyber criminels (l'espace postsoviétique en regorge), sociétés militaires privées ou de cybersécurité. L'utilisation de proxies par un État [35] permet de diluer sa responsabilité, de profiter des savoir-faire et des ressources provenant des secteurs privés ou criminels et surtout d'entretenir le doute. Celui-ci est exacerbé par le principe d'action sous "false flag", des traces (comme par exemple une adresse IP ou l'utilisation d'une langue spécifique pour les commentaires du code des outils utilisés) menant à une mauvaise attribution sont volontairement disposées dans les outils et les infrastructures utilisés. Le recours aux proxies soulève la question du contrôle par l'État de son écosystème cyber, les intérêts entre effecteurs et commanditaires peuvent diverger rapidement.

Disposer des capacités d'attribuer techniquement nécessite d'avoir les aptitudes nécessaires à l'analyse des traces recueillies ainsi que les charges utiles capturées, une bonne connaissance des acteurs et de leurs modes opératoires. L'attribution peut s'appuyer sur des actions de renseignement (d'origine cyber ou non). Attribuer une attaque dépasse la recherche de l'entité (ou des entités) effectrice. L'enquête vise à déterminer les cibles réelles : l'attaque peut avoir rebondi et s'être propagée hors de tout contrôle, ou alors l'objectif peut être volontairement noyé dans la masse comme par exemple en masquant l'exfiltration de données dans des attaques distribuées par déni de service (DDoS). Une fois les cibles trouvées, se pose la question des buts recherchés par les commanditaires qui peuvent être disjoints des effecteurs.

35. Les prestations d'attaques disponibles sur les différents marchés noirs permettent aussi à des acteurs non étatiques de disposer de "proxies".

Un nombre croissant d'entreprises de sécurité informatique, disposant d'équipes spécialisées dans le repérage et l'analyse des malwares, rendent publique leur recherche, fournissant ainsi une forme d'attribution technique.

Les Five-Eyes [36] attribuent (techniquement) massivement parce qu'ils considèrent que trouver un coupable fait partie de leur rôle et participe au renforcement de leur prestige [37]. A l'inverse, la Chine et la Russie n'attribuent techniquement pas (ou très peu) mais les Chinois dénoncent politiquement les agissements étrangers (américains pour la plupart). La France n'attribue que très peu et l'acte est éminemment politique [38]. En effet, dans la doctrine française, mettre un nom derrière une attaque revient à se donner le droit de riposter publiquement. Par ailleurs, cette frilosité dans l'attribution permet de garantir une certaine liberté d'action à la France : une attribution réalisée par un organisme privé ou par une puissance étrangère ne saurait l'engager car n'ayant pas le soutien politique français.

Plus généralement, la volonté d'attribuer une attaque va dépendre de la doctrine de l'État concerné et de deux facteurs variables [39]. Le premier est la structure de coût de la victime qui correspond à l'ensemble des dommages subis et de l'enjeu (économique, de réputation et de sécurité nationale) représenté par la cible. Le deuxième est le rapport de force entre agresseur et victime. Par ailleurs, attribuer une attaque à un acteur nécessite de définir sa responsabilité dans le déroulé de celle-ci [40].

Conclusion

Six grandes catégories d'objectifs se dégagent pour les opérations offensives. Celles-ci suivent se déroulent traditionnellement en quatre phases : reconnaissance, compromission (établissement d'une tête de pont), latéralisation (consolidation et extension de la tête de pont) et exploitation. La discrétion conditionne la réussite des trois premières étapes. Les actions associées sont conduites dans les différentes couches du cyberespace mais l'effet final recherché reste, le plus souvent, extérieur au cyberespace bien que les effets physiques directs des attaques restent encore peu

36. Les Five-Eyes est une alliance regroupant les services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis.

37. *Entretien réalisé le 23/04/2020 avec un architecte cyberdéfense de l'ANSSI.*

38. *Entretien réalisé avec un architecte cyberdéfense de l'ANSSI.*

39. S. Taillat. « Le cyberespace et la conflictualité internationale ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 26-33, p.28.

40. Jason Healey. *Beyond Attribution : Seeking National Responsibility for Cyber Attacks*. Atlantic Council's Cyber Statecraft Initiative, 22 février 2012.

fréquents.

Analyser finement la manœuvre dans le cyberespace est délicat du fait de l'incertitude y régnant. Celle-ci provient de la complexité de la menace et des systèmes à défendre, et de la difficulté d'attribution des attaques (de l'effecteur, du donneur d'ordre ou de l'objectif recherché, le tout combiné à des attaques qui peuvent être des leurres). A cela vient s'ajouter, pour la défense, les facteurs suivants de complexité : la fragmentation de la responsabilité et des systèmes, l'évolution rapide des produits, la complexité croissante de ceux-ci et leur maintien en condition de sécurité.

Bibliographie

Bibliographie générale

Boyer, B. « Les opérations sur l'environnement : la nouvelle guerre de l'information ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 209-217.

Motte, M., G.-H. Soutou, J. de Lespinois et O. Zajec. *La mesure de la force*. Thallandier. Paris, 2018. 416 p.

Taillat, S. « Le cyberespace et la conflictualité internationale ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 26-33.

Weber, C. et C. Jean-Philippe. « De l'importance du facteur humain ». In : *La Cyberdéfense*. U. Paris : Armand Colin, 2018, p. 52-59.

Kiyuna, A. et L. Conyers. *Cyberwarfare Sourcebook*. Lulu. com, 2015.

Rapports

ANSSI. *Etat de la menace rançongiciel à l'encontre des entreprises et des institutions*. 5 février 2020.

Cyber Influence Operations : An Overview and Comparative Analysis. Zurich : Center for Security Studies (CSS), ETH Zürich, octobre 2019.

Hodgson, Q. E., L. Ma, K. Marcinek et K. Schwindt. *Fighting Shadows in the Dark : Understanding and Countering Coercion in Cyberspace*. Santa Monica : CA : RAND Corporation, 2019.

SGDSN. *Revue stratégique de cyberdéfense*. 2018.

Jason Healey. *Beyond Attribution : Seeking National Responsibility for Cyber Attacks*. Atlantic Council's Cyber Statecraft Initiative, 22 février 2012. url : `https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/`.

d'information, D. centrale de la sécurité des systèmes. *La défense en profondeur appliquée aux systèmes d'information*. 19 juillet 2004.

Articles de recherche

Kempf, O. « Du cyber et de la guerre ». In : *Fondation pour la recherche stratégique* (Note n°17/2019 12 septembre 2019).

« Cybersécurité : Extension du domaine de la lutte ». In : *Politique étrangère* 2 (2018), p. 9-230.

Pamment, J., H. Nothhaft et A. Fjällhed. « Countering information influence activities : The state of the art ». In : (2018).

Brangetto, P. et M. A. Veenendaal. « Influence Cyber Operations : The use of cyberattacks in support of Influence Operations ». In : *2016 8th International Conference on Cyber Conflict (CyCon)*. IEEE. 2016, p. 113-126.

Douzet, F. « La géopolitique pour comprendre le cyberespace ». In : *Hérodote* 152-153.1 (2014), p. 3-21.

Ventre, D. « Le cyberespace : définitions, représentations. » In : *Revue Défense Nationale* 751 (2012), p. 33.

Reason, J. « The contribution of latent human failures to the breakdown of complex systems ». In : *Philosophical Transactions of the Royal Society of London. B, Biological Sciences* 327.1241 (1990), p. 475-484.

Articles de presse

Mariel chef de bataillon, V. « L'influence militaire pour créer la surprise dans un champ de bataille transparent ? » In : *Lettre d'information du centre de doctrine et d'enseignement du commandement* (février 2019).

Conférences

Forum International de la Cybersécurité (FIC). Lille, 2020.

Symposium sur la sécurité des technologies de l'information et des communications (SSTIC). Rennes, 2018.

Liste des entretiens

Entretien réalisé le 21/07/2020 avec un responsable de l'ANSSI.

Entretien réalisé le 23/04/2020 avec un architecte cyberdéfense de l'ANSSI.

Entretien réalisé le 29/06/2020 avec un responsable de l'ANSSI.

Entretien réalisé le 3/07/2020 avec un responsable de la DGSI.

40. Le terme d'agent désigne un poste technique, le terme de conseiller désigne un poste s'intéressant à la stratégie et le terme de responsable désigne un poste d'encadrement et de décision.