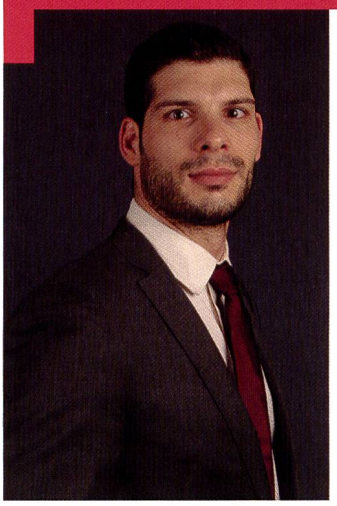
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2019)
Heft: 6

Artikel: Le cyber-espionnage : anciens principes, nouvelles pratiques
Autor: Chesaux, Julien
DOI: https://doi.org/10.5169/seals-977463



« Des informations préalables obtenues par des hommes qui connaissent la situation de l'ennemi permettent de le surpasser».
Sun Tzu

Intelligence économique

Le cyber-espionnage : Anciens principes, nouvelles pratiques

Julien Chesaux
Consultant en Cybersécurité et titulaire d'un master en Etudes Stratégiques

L'espionnage n'est pas une activité nouvelle. Elle se pratique depuis des siècles dans un contexte politique, social, économique ou militaire et reste une phase essentielle de l'acte de guerre. Néanmoins, le cyber-espionnage offre une nouvelle dimension au renseignement grâce à la quantité de données qui peuvent être collectées, structurées, et utilisées afin d'aboutir à de l'information utile à la prise de décision. Cet article explore les causes qui permettent et favorisent le cyber-espionnage ainsi que quelques exemples récents qui démontrent son efficacité.

La dépendance quotidienne aux données rend les personnes, les entreprises et les Etats plus vulnérables. En effet, la surface d'attaque est bien plus grande dans le cyberespace et le calcul coût/bénéfice est très simple et rapide : la cyber-défense est très coûteuse, notamment en terme de technologies à acquérir, de procédures à mettre en place ainsi que de personnel qualifié à engager, comparé à un *malware* (logiciel malveillant) qui est bon marché.

De nombreuses entreprises vendent des MaaS (Malware-as-a-Service) où Monsieur et Madame tout le monde peut louer un service pour *hacker* (pirate informatique) une cible tout en ayant un service après-vente en cas de problème. Cette évolution accroît le risque de cyber-espionnage en augmentant grandement le nombre d'attaquants potentiels puisqu'il y n'a plus besoin d'être spécialiste en informatique pour mener des cyberattaques.

En outre, il existe un marché pour les vulnerabilités *zero-day*, définies comme un bug logiciel critique non identifié lors du développement et non connu par l'éditeur. Ainsi, certains *hackers* tentent de découvrir des *zero-days* afin d'avertir les développeurs mais aussi pour les revendre au plus offrant. En effet, de nombreux systèmes sont rarement mis à jour et de nombreuses entreprises de logiciels ne respectent pas ou peu les principes de sécurité lors du développement en raison de la pression du marché : le développement doit être rapide et le prix du produit doit être bas, ce qui favorise l'apparition de vulnérabilités exploitables. Un réçent rapport de l'entreprise Glasswall met en avant le nombre grandissant de cyberattaques visant les entreprises technologiques et spécialement les développeurs de *software*.[1]

Ainsi, que cela soit pour suivre un dissident politique, pirater des plans d'armements ou d'un drone, il existe de nombreuses opportunités qui mènent à un complexe industriel malveillant. Certaines sociétés font l'acquisition de *zero-days* comme les sociétés françaises Vupen Security, Maltese ReVuln, les américaines Netragard, Endgame, Exodus ou Zerodium, et d'autres sont spécialisées dans les malwares d'espionnage qui exploitent des *zero-days* comme Gamma International, Cyberbit, NSO Group, ou encore Amesys.[2] Cette dernière a été accusée de vendre le système Eagle, utilisé par le régime de Kadhafi pour cyber-espionner certains citoyens tandis que Cyberbit a vendu le *spyware* (logiciel d'espionnage) PSS (PC Surveillance System) au gouvernement ethiopien pour surveiller des opposants politiques et autres journalistes à l'étranger.[3,4] Ces affaires font échos aux autres accusations de cyber-espionnage avec des solutions de la société NSO Group dans des cas au Mexique et aux Emirats Arabes Unis.[5,6] Ces petites entreprises sont présentes sur le marché aux cotés des traditionnels géants de l'armement qui se sont tous tournés vers le cyberespace tels que EADS, BAE Systems, General Dynamics, Raytheon ou Elbit Systems.

5 SCOTT-RAILTON John, MARCZAK Bill, ABDUL RAZZAK Bahr, CRETE-NISHIHATA Masashi & DEIBERT Ron, «Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware», *The Citizen Lab, Jun 19, 2017* https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

6 MARCZAK Bill & SCOTT-RAILTON John, «The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender», *The Citizen Lab, Aug 24, 2016* https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

Les entreprises ont des difficultés à contrôler toutes les chaînes de valeur technologiques; les composants d'un produit sont conçus, créés, construits/développés et stockés dans le monde entier, ce qui signifie de nombreuses possibilités d'erreur ou d'intégration d'un élément malveillant dans celui-ci. La complexité du développement des armements, de leurs composants et de la forte externalisation offrent des opportunités aux pirates informatiques qui peuvent, par exemple, infiltrer des sous-traitants de la défense au cours du processus de développement des armes ou lors d'une mise à jour ultérieure si besoin. Il y aura toujours une machine non patchée (mise à jour), une procédure manquante ou non respectée pour des questions de commodité, ou un individu qui clique sur un lien malicieux.

De nombreux exemples ayant exploités le cyber-espionnage existent pour souligner l'efficacité des cyberattaques et des emails de *phishing* (courriel d'hameçonnage). Voici plusieurs exemples: des cyber-attaques pour débusquer des espions, l'utilisation des réseaux sociaux pour influencer l'opinon publique et les soldats (Cyber PSYOPS), l'espionnage de citoyens, l'utilisation de cyber-espionnage dans un théâtre d'opération militaire et la possibilité d'effectuer de la cyber-défense dynamique.

Découvrir des taupes

Le cyber-espionnage et le piratage pratiqués par l'armée de libération chinoise ont été traditionnellement et principalement devoués aux entreprises de défense et d'aérospatial à des fins de rétro-ingénierie. Ceci a permis l'accès à des plans d'armement à la pointe de la technologie sans passer par la case recherche et dévelopement, permettant ainsi d'éviter de lourds investissements, un gain de temps considérable tout en évitant la prise de risque liée à ce type d'activité.

Mais l'un des plus grands *data leak* (fuite de données), prétendument attribué à la Chine, a été mené contre l'Office of Personal Management (OPM), un service de ressources humaines des employés fédéraux du gouvernement américain (gestion d'environ 3 millions d'employés actifs). Dévoilée dans le courant 2015 mais ayant été découverte probablement l'année précédente, cette cyberattaque a permis de compiler une base de données de 22,1 millions d'employés actuels et passés avec noms, prénoms, dates de naissance, adresses, antécédents médicaux, numéros de sécurité sociale, et même empreintes digitales, entretiens personnels, et mots de passe pour certains.[7,8]

Le but de cette cyberattaque était très certainement l'utilisation ultérieure des données. En effet, en 2017, une douzaine de sources américaines ont été tuées ou emprisonnées en territoire chinois. Ces individus étaient liés à la CIA comme informateurs ou espions et ont potentiellement été débusqués grâce à la cyberattaque de l'OPM.[9] D'autres explications incriminent également

Un PC et une connexion internet: la nouvelle menace qui permet de toucher tout le monde, partout dans le monde et en tout temps.

une taupe au sein de la CIA ou une faille dans la méthode de communication cryptée entre la CIA et ses ressources sur le terrain.[10]

Influencer les opinions

Autre possibilité qu'offre le cyberespace, à travers le cyber-espionnage, est l'action de mener des opérations de type cyber PSYOPS (du nom des opérations psychologiques menées par les Etats-Unis, notamment durant les guerres de Corée, du Vietnam et du Golf), des opérations cyber qui visent à influencer l'opinion ou créer un sentiment de doute voire même de défiance favorisant un état de tension permanent, brouillant ainsi la frontière entre guerre et paix. Ces manipulations passent par les *fakes news*, les *deepfakes*, la désinformation, l'influence, la propagande, le soutien aux manifestations et les ingérences nationales.

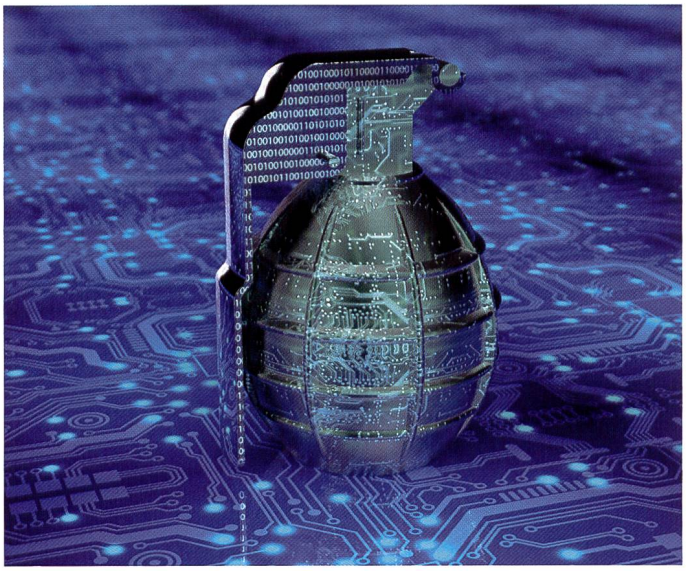
Ces phénomènes de cyber-espionnage sur les réseaux sociaux permettant ensuite de créer des faux contenus sont particulièrement menaçants pour le monde militaire et ses soldats. En effet, les troupes déployées dépendent des réseaux sociaux pour obtenir des informations du pays d'origine et rester en contact avec leur famille et leurs amis. Une étude de l'université d'Oxford a ainsi révélé comment des *hackers* ciblent les militaires et civils en déploiement, ainsi que leurs familles.

La recherche «a montré que des extrémistes, des théoriciens du complot et des acteurs étrangers utilisent déjà les médias sociaux pour diffuser une désinformation subversive afin d'influencer les opinions et les discussions au sein de la communauté militaire américaine».[11] Le moral et l'esprit de corps peuvent être fortement influencés et freinés, ainsi que la prise de décision et l'exécution des ordres destabilisées. Au niveau des

9 MAZZETTI Mark. «Killing C.I.A. Informants, China Crippled U.S. Spying Operations», *The New York Times*, May 20, 2017 https://www.nytimes.com/2017/05/20/world/asia/china-cia-spies-espionnage.html

10 *Ibid.*

11 KRULL Matthew. «Foreign Disinformation is a Threat to Military Readiness, too», *Defense One*, 16 Feb, 2018 http://www.defenseone.com/ideas/2018/02/foreign-disinformation-threat-military-readiness-too/146076/?oref=defenseone_today_nl



Tout logiciel comportant une vulnérabilité est une bombe numérique à retardement.

ambassades et les ministères, ces manipulations peuvent affecter négativement la productivité du personnel diplomatique et administratif.

Surveiller les citoyens

La politique intérieure du parti communiste chinois est obsédée par 3 éléments : le contrôle, le contrôle et le contrôle. Le parti essaie de contrôler la vie des citoyens de toutes les manières possibles afin d'éviter la liberté, la protestation, la pensée alternative, l'initiative ou l'imprévisibilité. La République populaire de Chine associe législation et actions technologiques de cyber-espionnage pour censurer et réglementer internet au niveau national. Par exemple, la nouvelle loi sur la cybersécurité entrée en vigueur en 2017 accorde au gouvernement chinois un contrôle accru sur l'architecture du cyberespace et les réseaux informatique des entreprises. Dans certains articles de la loi, le libellé est vague et imprécis et permet d'invoquer différentes excuses pour des inspections, ce qui peut compromettre des secrets commerciaux et des informations sensibles. La législation oblige l'utilisation de hardware et software chinois, ce qui prend toute son importance en période de discussions en Occident sur l'utilisation de matériel de la société technologique Huawei.

En plus du « Great Firewall » qui limite l'accès aux sites Web (comme Facebook ou Google) et du « Green Dam », un logiciel installé sur les ordinateurs personnels pour surveiller les activités en ligne, le gouvernement a mis au point un nouveau moyen de faire respecter l'obéissance parmi les citoyens: l'application Sesame Credit. Cette application est un système de crédit social qui collecte des données pour mesurer le degrée d'obédience de l'utilisateur à la politique du parti, permettant ainsi de le récompenser ou de le sanctionner. Tout comportement digital est collecté : sur les médias sociaux, les déplacements, ce qui est partagé ou publié, et une multitude d'autres données telles que les habitudes d'achat. [12]

Tout comportement est lié à des points et un score global est affiché. Par exemple, si vous achetez un article étranger, comme un manga japonais, votre score diminue. Par contre, si vous republiez des nouvelles de l'agence de presse du parti, il augmente. Plus le score est élevé, plus le citoyen a un « bon » comportement. Un bon score vous récompense avec des avantages : trouver un nouveau logement dans un quartier recherché, faciliter l'obtention d'un prêt hypothécaire, pouvoir inscrire vos enfants dans une école réputée, recevoir un visa pour voyager à l'étranger, bénéficier de réductions en ligne ou éviter les files d'attente pour des documents administratifs.[13] L'épisode « Nosedive » de la série *Black Mirror* n'est donc plus une fiction.

La fiction ne s'arrête pas là puisque l'Etat chinois a, depuis 2005, mis en place un système de surveillance intelligent nommée *Skynet* (la société ayant développé des robots tueurs dans les films de la franchise Terminator).[14] Les caméras et lunettes intelligentes de *Skynet* filment, reconnaissent les visages, collectent et stockent les données dans des bases de données exploitables. Officiellement, ce système de surveillance en temps réel permet de traquer et arrêter des fugitifs, criminels liés à des affaires de corruption mais aussi tout autre acte jugé illégal sur la voie publique (ex: traverser en dehors des passages cloutés). Les citoyens peuvent ensuite voir leur nom affichés sur des panneaux publics.

Utilisation opérationnelle

De 2014 à 2016, le groupe Fancy Bear, supposé être lié au gouvernement russe, a espionné l'armée ukrainienne. Un rapport de l'entreprise en cybersécurité CrowdStrike a révélé que les hackers espionnaient les forums militaires ukrainiens afin de propager un malware fonctionnant sur une application Android. Le logiciel malveillant a été ensuite déployé via une plateforme digitale développée à l'origine pour améliorer le temps de ciblage de l'artillerie. Environ 9'000 membres du personnel d'artillerie utilisaient cette boîte à outils légitime. Ensuite, les logiciels espions activés permettent de récupérer les données de communication et de localisation des périphériques infectés.[15]
Les données récupérées ont été utilisées efficacement car l'armée ukrainienne a subi une perte de 50 % de ses armes en deux ans et de 80 % de ses obusiers D-80 Howitzers.[16]

12 HATTON Celia. «China social credit: Beijing sets up huge system», *BBC*, Oct 26, 2015 http://www.bbc.com/news/world-asia-china-34592186

13 NOE Jean-Baptiste. «La Chine Big Brother: surveiller et punir», *Contrepoints*, Aug 3, 2019 https://www.contrepoints.org/2019/08/03/350491-la-chine-big-brother-surveiller-et-punir

14 SMITH Ms. «Skynet in China: Real-life Person of Interest spying in real time», *CSO Online*, Sep 26, 2017 https://www.csoonline.com/article/3228444/skynet-in-china-real-life-person-of-interest-spying-in-real-time.html

15 POPA Bogdan. «Fancy Bear Hackers Breached Ukrainian Artillery Using Android Malware», *Softpedia*, Dec 22, 2016 http://news.softpedia.com/news/fancy-bear-hackers-breached-ukrainian-artillery-using-android-malware-511208.shtml

16 *Ibid.*

Pénétrer les systèmes de défense

Combinés à la guerre électronique traditionnelle, qui consiste à utiliser des systèmes électromagnétiques pour perturber et obtenir un avantage sur l'ennemi, les *hackers* peuvent soutenir des opérations militaires.

Ainsi, les Etats lancent des campagnes de cyber-espionnage ou d'intrusion pour collecter des informations susceptibles d'être exploitées, tôt ou tard, pour se défendre. Le but est d'obtenir des informations utiles et exploitables en collectant, traitant et stockant des données. La NSA parle de «renseignement étranger à l'appui de la défense dynamique» («foreign intelligence in support of dynamic defense»)[17]. Dès lors, des Etats peuvent collecter des plans d'opérations ou d'armements pour augmenter leurs défenses et atténuer leurs effets en cas d'attaque, tout en permettant des options de contre-attaque grâce aux cyberattaques (comme le piratage des avions par des cyberattaques au lieu d'attaques conventionnelles).

Certains cyber-experts universitaires soutiennent que ces « intrusions de réseau axées sur la défensive...ne sont pas des invasions, mais des efforts de renseignement »[18]. Par conséquent, le renseignement fait partie de la politique internationale, que ce soit par l'espionnage traditionnel ou par le piratage. En fin de compte, « toutes les nations espionnent et toutes les nations le savent »[19]. La vraie question à laquelle il faut répondre est: à quel moment ces efforts représentent-ils une menace vitale nécessitant une réponse cinétique?
Une problématique ressort de ces différentes opérations de cyber-espionnage: elles créent un dilemme en matière de cybersécurité qui augmente les tensions.

Vers une cyber-course aux malwares

La situation actuelle conduit à une cyber-course aux malwares ressemblant à la course à l'armement du temps de la guerre froide. Durant ces années, un acte de guerre aurait signifié l'annihilation des deux opposants, en raison du nombre excessif et de la puissance des armes nucléaires à leur disposition. Pour cette raison, la guerre froide a abouti à la doctrine de destruction mutuelle assurée (Mutual Assured Destruction ou MAD). Reste à voir quel sera le résultat de la course aux *malwares*.

Cette course aux cyber armes se déroulera principalement entre les États-Unis et la Chine, avec quelques autres Etats profitant de l'asymmétrie qu'offre les cyberattaques. En septembre 2017, le président russe Vladimir Poutine a déclaré que l'intelligence artificielle (liée aux capacités cybernétiques) constituait « l'avenir, non seulement pour la Russie, mais pour l'humanité ».[20]

17 BUCHANAN Ben. «Prevalence and Dangers of Defensive Hacking», *Motherboard*, Feb 20, 2017 https://motherboard.vice.com/en_us/article/4xbv7j/the-cybersecurity-dilemma-the-prevalence-and-dangers-of-defensive-hacking

18 *Ibid.*

19 *Ibid.*

20 MEYER David. «Vladimir Putin Says Whoever Leads in Artificial

News

Les rançongiciels continuent de progresser

Berne, 29.10.2019 – Le 29e rapport semestriel de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) porte sur les principaux cyberincidents observés au cours du premier semestre 2019 en Suisse et à l'étranger. Il a pour thème prioritaire les rançongiciels, qui ont causé d'importants dommages dans le monde entier durant la première moitié de l'année.

Les chevaux de Troie verrouillant les données, appelés aussi rançongiciels, font partie actuellement des cybermenaces les plus graves pour les entreprises, les organisations et les administrations. En plus d'exiger du temps, du personnel et de l'argent pour le nettoyage des systèmes et la restauration des données perdues, une attaque qui réussit peut nuire à la réputation d'une entreprise ou entraîner une perte de productivité temporaire. Pour donner une idée concrète d'une attaque, la Ville de Berne explique dans le 29e rapport semestriel comment elle a géré un incident lié à un rançongiciel. En outre, la police cantonale zurichoise aborde le problème du point de vue des enquêteurs. Enfin, MELANI formule des recommandations sur la manière de se protéger contre de telles attaques.

Les petites et moyennes entreprises d'approvisionnement en électricité ont besoin de soutien dans le domaine de la cybersécurité

Les systèmes de contrôle industriels, notamment dans le secteur de l'approvisionnement en électricité, sont également dans le viseur des pirates informatiques. Aussi l'association faîtière Electrosuisse a-t-elle publié au printemps 2019 une étude sur la cybersécurité dans les petites et moyennes entreprises d'approvisionnement en électricité de Suisse. Il ressort de cette analyse que toutes les entreprises se préoccupent de cybersécurité. Cependant, des mesures supplémentaires s'imposent pour garantir la sûreté de l'information, dans les petites sociétés en particulier. Pour améliorer la sécurité informatique, une organisation de cybersécurité a été créée pour les services industriels. Grâce à cette plateforme, tous les partenaires pourront tirer parti de leurs expériences respectives et accroître progressivement ensemble le niveau de sûreté de l'information.

Le chantage par faux messages de sextorsion continue

Au cours du premier semestre 2019, on a observé une augmentation du nombre de faux messages de sextorsion dans lesquels les escrocs prétendent avoir piraté l'ordinateur de leur victime et détenir des images la montrant en train de consommer de la pornographie sur Internet. Malheureusement, beaucoup de gens continuent à payer la rançon exigée. Au printemps 2019, MELANI a donc lancé, en collaboration avec divers partenaires, le site Internet www.stop-sextortion.ch pour sensibiliser la population à cette imposture. Sur ce site, les personnes concernées trouvent des conseils sur la façon de procéder au cas où les maîtres chanteurs posséderaient réellement du matériel compromettant.

Unité de pilotage informatique
de la Confédération

La Chine a également reconnu le pouvoir du monde numérique. Selon le « Rapport sur la sécurité Internet : premier semestre 2017 » de l'entreprise Tencent, la Chine souffre d'une grave pénurie de professionnels de la cybersécurité. Ainsi, Beijing espère obtenir 1,4 million de diplômés en cybersécurité au cours de la prochaine décennie (une augmentation significative par rapport aux quelques 30'000 diplômés qu'elle produit aujourd'hui).[21] Pour ce faire, la Chine affirme qu'elle établira quatre à six écoles de cybersécurité de classe mondiale dans des universités chinoises afin de créer des « cyber-guerriers » d'ici 10 ans.[22]

Conclusion

En 2018, la première école de recrue cybernétique a permis de former 18 soldats de milice. [23] Les ambitions d'obtenir 600 cyber-spécialistes d'ici 2020 au DDPS, la mise en place d'un cyber-Defense Campus et d'un nouveau master en cybersécurité sont des mesures de rattrapage positifs, mais surtout nécessaires. En effet, la Suisse, n'est pas à la recherche de capacités offensives mais elle doit pouvoir détecter et analyser toutes intrusions suspectes et être capable de protéger ses infrastructures.

La SNPC 2018-2022[24] va clairement dans ce sens afin d'établir un *minima* et de limiter la surface d'attaque exploitable par des pirates informatiques. Néanmoins, la cybersécurité doit être comprise comme un effort général au niveau des individus, des entreprises et des administrations car la question n'est pas de savoir si nous sommes protégés mais si nous sommes prêts à répondre à toutes les cybermenaces.

J. C.

Intelligence Will Rule the World», *Fortune*, Sep 04, 2017 http://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/

21 TENCENT COMPUTER MANAGER. «2017 Internet security report in the first half of the year», *Tencent*, Aug 04, 2017 https://guanjia.qq.com/news/n1/2039.html

22 ZI Yang. «China Is Massively Expanding Its Cyber Capabilities"», *The National Interest*, Oct. 3, 2017 http://nationalinterest.org/blog/the-buzz/china-massively-expanding-its-cyber-capabilities-22577%22

23 Communication Défense. «Première experiences dans le domaine de l'instruction en cybernétique», *Armée Suisse, Sep 20, 2018* https://www.vtg.admin.ch/fr/armee.detail.news.html/vtg-internet/verwaltung/2018/18-09/erste-erfahrungen-mit-dem-cyber-lehrgang-der-armee.html

24 SN002 - Stratégie nationale de protection de la Suisse contre les cyber-risques (SNPC) 2018-2022, Avr 18, 2018 https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html