World War C :
Comprendre les motifs des États-nations derrière les cyberattaques évoluées d'aujourd'hui

RÉSUMÉ

Le cyberespace est devenu une zone de guerre à part entière et les gouvernements du monde entier s'affrontent pour obtenir la suprématie numérique dans un nouveau théâtre des opérations dont la majeure partie est invisible. Autrefois l'apanage de criminels opportunistes, les cyberattaques deviennent une arme essentielle des gouvernements qui cherchent à défendre leur souveraineté et projeter la puissance de leur nation.

Des campagnes de cyberespionnage stratégique telles que Moonlight Maze et Titan Rain aux cyberfrappes militaires destructrices sur la Géorgie et l'Iran, les conflits humains et internationaux entrent dans une nouvelle phase de leur longue histoire. Sur ce champ de bataille indistinct, les victoires se gagnent avec des bits au lieu de balles, des logiciels malveillants au lieu de milices et des réseaux d'ordinateurs zombies au lieu de bombes.

Ces attaques secrètes sont pour la plupart invisibles au public. À la différence des guerres d'antan, cette cyberguerre ne produit aucune image spectaculaire de têtes explosives atteignant leur cible, d'immeubles effondrés ou de civils en fuite. Mais la liste des victimes comprend déjà quelques-uns des plus grands noms de la technologie, des finances, de la défense, des gouvernements, et s'allonge de jour en jour.

Il est plus facile de comprendre une cyberattaque non comme une fin en soi, mais comme un moyen potentiellement puissant d'atteindre divers objectifs politiques, militaires et économiques.

« Il est peu probable que les cyberattaques sérieuses soient sans motif, indique Martin Libicki, responsable scientifique de RAND Corp. Les pays les effectuent pour atteindre certains objectifs qui reflètent habituellement leurs grands objectifs stratégiques. Et si la relation entre les moyens choisis et les objectifs ne nous paraît pas rationnelle ou raisonnable, elle l'est pour eux. »

Tout comme chaque pays dispose d'un système politique, d'une histoire et d'une culture uniques, les attaques commanditées par les États présentent également des caractéristiques distinctives, de leur motivation au type d'attaque employé.

Ce document décrit les caractéristiques uniques des campagnes de cyberattaques menées par les gouvernements à travers le monde. Nous espérons qu'armés de ces connaissances, les

professionnels de la sécurité pourront mieux identifier leurs agresseurs et adapter leurs défenses en conséquence.

Voici un rapide aperçu :

- **Asie-Pacifique :** base de grands groupes de pirates structurés tels que le « Comment Crew » aux nombreux objectifs et dont les cibles multiples font l'objet d'attaques de force brute très fréquentes.
- **Russie/Europe de l'Est :** cyberattaques techniquement plus sophistiquées et échappant à la détection avec une grande efficacité.
- **Moyen-Orient :** pirates dynamiques utilisant souvent la créativité, la tromperie et l'ingénierie sociale pour inciter les utilisateurs à compromettre leurs propres ordinateurs.
- **États-Unis :** les campagnes de cyberattaques les plus complexes, les mieux ciblées et les plus rigoureusement conçues à ce jour.

INTRODUCTION

World War Z, best-seller porté à l'écran par Hollywood, raconte le détail d'une pandémie mondiale dans laquelle la politique et la culture influencent profondément la façon dont le public et par extension les gouvernements réagissent à une épidémie de zombies. Dans un passage, par exemple, un jeune Arabe refuse de croire que la maladie est réelle, et soupçonne Israël d'avoir inventé l'histoire. Les nations décrites dans World War Z, les États-Unis, la Chine, la Russie, la Corée du Sud, Israël, et bien d'autres, sont impliquées dans un tout autre type de conflit, mais dont l'impact sur la sécurité nationale est réel et croissant : World War C, où « C » signifie « Cyber » au lieu de « Zombie ». Toutefois, la même règle s'applique : chaque pays dispose d'un système politique, d'une histoire, d'une langue, d'une culture et d'une compréhension uniques des conflits humains et internationaux.

Les cyberconflits reflètent souvent les conflits traditionnels. Par exemple, la Chine utilise des cyberattaques de grand volume similaires à ses attaques d'infanterie au cours de la guerre de Corée. De nombreux soldats chinois furent alors envoyés au combat avec une poignée de balles seulement. La force de leur nombre les rendit pourtant capables de remporter des victoires sur le champ de bataille. À l'autre extrémité du spectre se trouvent la Russie, les États-Unis et Israël, dont les cybertactiques sont plus chirurgicales et font appel à des technologies de pointe et aux travaux de fournisseurs innovants mus par la concurrence et les stimulations financières.

Nous sommes encore à l'aube de l'ère de l'Internet. Mais les cyberattaques ont déjà fait leurs preuves en tant que moyen peu coûteux et hautement rentable de défendre la souveraineté et de projeter la puissance d'une nation. Nombre de gros titres d'aujourd'hui semblent être tirés des pages d'un roman de science-fiction. Un code sophistiqué détruit une centrifugeuse nucléaire à des milliers de kilomètres de distance. Des logiciels malveillants enregistrent secrètement tout ce que fait un utilisateur sur son ordinateur. Un logiciel vole les données de tout périphérique Bluetooth se trouvant à proximité. Un code chiffré se déchiffre uniquement sur un périphérique cible spécifique. Une telle sophistication en dit long sur la maturité, la taille et les ressources des organisations qui sont à l'origine de ces attaques. À quelques rares exceptions près, ces attaques font désormais partie de l'arsenal des États-nations.

« La communauté internationale a maintenant une bonne compréhension de la cybertechnologie, explique le professeur Michael N. Schmitt de l'U.S. Naval War College dans une interview par courriel. Ce qui manque, c'est la compréhension du contexte géopolitique dans lequel cette technologie fonctionne. Les attributions faites sans prise en compte de l'environnement géopolitique sont rarement raisonnables. »

Comme toute analogie, World War C a ses limites. La cyberguerre a été comparée aux forces d'opérations spéciales, à la guerre sous-marine, aux missiles, aux assassins, aux armes nucléaires, à Pearl Harbor, au 11 septembre, à Katrina et à d'autres. Même notre analogie avec les zombies n'est pas nouvelle. Souvent, un ordinateur infecté se trouvant sous le contrôle furtif d'un pirate est appelé un zombie, et les réseaux d'ordinateurs zombies sont parfois appelés des

armées de zombies. De plus, par comparaison aux mises en réserve de carburant et d'artillerie, écrire un code de cyberattaque et compromettre des milliers si ce n'est des millions d'ordinateurs est une chose facile. En outre, les logiciels malveillants se propagent souvent au rythme exponentiel d'une maladie infectieuse.

Ce document examine de nombreuses cyberattaques publiquement connues. En explorant quelques-unes des caractéristiques nationales ou régionales distinctives de ces attaques, les entreprises pourront mieux identifier leurs agresseurs, anticiper de futures attaques et mieux se défendre.

Avertissement

Les eaux de l'analyse de la cyberguerre sont troubles par nature. Au plan stratégique, les gouvernements désirent afficher un degré de démenti plausible. Au plan tactique, les organisations militaires et de renseignement enveloppent ces opérations de multiples couches de secret. Pour être efficaces, les opérations d'information reposent sur la tromperie, et l'Internet offre un contexte idéal pour les écrans de fumée et les jeux de miroir de l'espionnage. En termes pratiques, les pirates lancent souvent leurs attaques à travers un cyberterrain (tel que des réseaux tiers compromis) qui suscite des complications techniques et juridiques pour les enquêteurs. Et enfin, les outils, tactiques et procédures de piratage évoluent si rapidement que la cyberdéfense, la législation et l'application de la loi restent en retard par rapport aux actions de l'attaquant.

« La plus grande difficulté pour dissuader les cyberattaques, s'en défendre ou y répondre est d'identifier correctement leur auteur, explique le professeur John Arquilla de la Naval Postgraduate School dans une interview par courriel accordée à FireEye®. Les missiles balistiques sont livrés avec l'adresse de l'expéditeur. Mais les virus informatiques, les vers et les attaques par déni de service sont souvent envoyés de façon anonyme. La meilleure chance de percer cet anonymat provient du mélange habile de techniques de contre-piratage et d'une profonde connaissance des cultures stratégiques et des objectifs géopolitiques des protagonistes. »

La « cyberattribution », à savoir l'identification d'un coupable probable, qu'il s'agisse d'un individu, d'une entreprise ou d'un État-nation, est notoirement difficile, en particulier dans le cas d'une attaque isolée. Les États sont souvent identifiés à tort comme des acteurs non étatiques, et vice versa. Pour aggraver les choses, les liens entre les deux se renforcent en permanence. Tout d'abord, un nombre croissant de « pirates patriotes » mènent ostensiblement une cyberguerre pour le compte de gouvernements (par exemple, en Tchétchénie et au Kosovo dans les années 90, en Chine en 2001, en Estonie en 2007, en Géorgie en 2008, et chaque année au Moyen-Orient)[1]. Deuxièmement, les organisations cybercriminelles offrent à tous, y compris aux gouvernements, des services de cyberattaque comprenant des attaques par déni de service et l'accès à des réseaux déjà compromis.

Les chercheurs de FireEye ont même vu un État-nation élaborer et utiliser un cheval de Troie sophistiqué, et le vendre ensuite à des cybercriminels au marché noir (après avoir mis en place ses propres défenses). Ainsi, certaines campagnes de cyberattaques peuvent comporter les cachets d'acteurs étatiques et non étatiques, ce qui rend toute attribution certaine presque impossible. Enfin, les cyberopérations effectuées sous une fausse bannière impliquent un groupe de pirates se comportant comme un autre dans le but de tromper les membres de la cyberdéfense.

[1] Geers K. (2008) « Cyberspace and the Changing Nature of Warfare », e-book *Hakin9*, 19(3) No. 6 ; *SC Magazine* (27 août 2008) 1-12.

La perspective FireEye

FireEye occupe une position unique dans le monde indistinct de la cyberguerre. Tout d'abord, notre plateforme de protection contre les logiciels malveillants a été installée sur les réseaux informatiques sensibles de plus de 1 000 clients de premier plan à travers le monde. Cela donne à nos chercheurs une présence globale et intégrée dans le cyberespace. Deuxièmement, les dispositifs de FireEye sont généralement placés derrière les défenses de sécurité traditionnelles telles que les pare-feu, antivirus et systèmes de prévention des intrusions. Cela signifie que notre taux de « faux positif » est faible, et que les attaques que nous détectons ont déjà réussi à pénétrer les défenses externes d'un réseau.

ASIE-PACIFIQUE

Chine : un éléphant dans la pièce

La République populaire de Chine représente la menace la plus bruyante du cyberespace. Les raisons à cela comprennent son énorme population, son économie en expansion rapide et un manque de bonnes stratégies de prévention de la part de ses victimes.

Attaques chinoises sur les États-Unis

La liste des compromissions chinoises réussies est longue et couvre l'ensemble du globe. Voici quelques-uns des incidents les plus importants aux États-Unis :

- **Gouvernement :** en 1999, le Département américain de l'énergie croit que le cyberespionnage chinois représente une menace « grave » pour la sécurité nucléaire américaine[2]. En 2009, la Chine vole apparemment les plans de l'avion de combat le plus avancé des États-Unis, le F-35[3].
- **Technologie :** la Chine pirate la technologie d'authentification SecurID de Google, Intel, Adobe et RSA, au moyen de laquelle elle cible alors Lockheed Martin, Northrop Grumman et L-3 Communications[4].
- **Affaires :** Morgan Stanley, la Chambre de commerce américaine, et de nombreuses banques ont été piratées[5].
- **Médias :** le *New York Times*, le *Wall Street Journal*, le *Washington Post* et d'autres ont été la cible de cyberattaques évoluées et persistantes provenant de Chine[6].
- **Infrastructures critiques :** DHS signale en 2013 que 23 sociétés de gazoducs ont été piratées (éventuellement à des fins de sabotage)[7], et que des pirates chinois ont été vus à l'U.S. Army Corps of Engineers' National Inventory of Dams[8].

Certaines de ces cyberattaques ont permis à la Chine d'avoir accès à des informations confidentielles telles que des données de recherche et de développement. D'autres ont donné aux services de renseignement chinois l'accès à des communications sensibles de hauts responsables gouvernementaux ou de certains dissidents politiques chinois.

---

[2] Gerth, J. & Risen, J. (2 mai 1999) « 1998 Report Told of Lab Breaches and China Threat », *The New York Times*.
[3] Gorman, S., Cole, A. & Dreazen, Y. (21 avril 2009) « Computer Spies Breach Fighter-Jet Project », *The Wall Street Journal*.
[4] Gross, M.J. (1er septembre 2011) « Enter the Cyber-dragon », *Vanity Fair*.
[5] Gorman, S. (21 décembre 2011) « China Hackers Hit U.S. Chamber », *Wall Street Journal* et *Ibid*.
[6] Perlroth, N. (1er février 2013) « Washington Post Joins List of News Media Hacked by the Chinese » et « Wall Street Journal Announces That It, Too, Was Hacked by the Chinese », *The New York Times*.
[7] Clayton, M. (27 février 2013) « Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage », *The Christian Science Monitor*.
[8] Gertz, B. (1er mai 2013) « Dam! Sensitive Army database of U.S. dams compromised; Chinese hackers suspected », *The Washington Times*.

Attaques chinoises hors des États-Unis

Bien entendu, les États-Unis ne sont pas la seule cybercible de la Chine. Tous les conflits géopolitiques traditionnels se sont déplacés vers le cyberespace, et les compromissions chinoises englobent le monde entier. Mais de nombreuses disputes ont été des affaires unilatérales, toutes les attaques connues du public provenant de Chine.

- **Europe :** En 2006, les pirates chinois prennent pour cible la Chambre des communes britannique[9].En 2007, la chancelière allemande Angela Merkel évoque le problème de piratage des États-nations avec le président de la Chine[10].En 2010, le MI5 britannique signale que des agents de renseignements chinois en civil ont donné aux dirigeants d'entreprises britanniques des appareils photo numériques et des clés USB contenant des logiciels malveillants[11].
- **Inde :** Les autorités indiennes craignent que la Chine ne perturbe leurs réseaux informatiques lors d'un conflit. Un expert indique qu'une utilisation exclusive du matériel chinois pourrait donner à la Chine une capacité de déni de service « permanente »[12]. Une attaque sophistiquée sur un QG de la marine indienne aurait utilisé un vecteur USB pour combler le « vide » entre un réseau autonome compartimenté et l'Internet[13].
- **Corée du Sud :** Pendant plusieurs années, le gouvernement sud-coréen s'est plaint de l'activité chinoise sur ses ordinateurs officiels, y compris d'une compromission des ordinateurs et assistants personnels appartenant à une grande partie des membres du gouvernement en 2010[14] et d'un assaut sur un portail Internet contenant les informations personnelles de 35 millions de Coréens en 2011[15].
- **Japon :** La liste des cibles comprend le gouvernement, l'armée et les réseaux de haute technologie. Les pirates chinois ont même volé des documents secrets[16].
- **Australie :** La Chine aurait volé les plans du nouveau bâtiment de l'Australian Security Intelligence Organization valant 631 millions de dollars[17].
- **Dans le monde :** En 2009, des chercheurs canadiens ont découvert que la Chine contrôle un réseau de cyberespionnage dans plus de 100 pays[18]. En 2010, une entreprise de

[9] Warren, P. (18 janvier 2006) « Smash and grab, the hi-tech way », *The Guardian*.
[10] « Espionage Report: Merkel's China Visit Marred by Hacking Allegations » (27 août 2007) *Spiegel*.
[11] Leppard, D. (31 janvier 2010) « China bugs and burgles Britain », *The Sunday Times*.
[12] Exclusive cyber threat-related discussions with FireEye researchers.
[13] Pubby, M. (1er juillet 2012) « China hackers enter Navy computers, plant bug to extract sensitive data », *The Indian Express*.
[14] Ungerleider, N. (19 octobre 2010) « South Korea's Power Structure Hacked, Digital Trail Leads to China », *Fast Compan*y.
[15] Mick, J. (28 juillet 2011) « Chinese Hackers Score Heist of 35 Million South Koreans' Personal Info », *Daily Tech*.
[16] McCurry, J. (20 septembre2011) « Japan anxious over defence data as China denies hacking weapons maker », *The Guardian* et « China-based servers in Japan cyber attacks », (28 octobre 2011) *The Indian Express*.
[17] « Report: Plans for Australia spy HQ hacked by China », (28 mai 2013) Associated Press.
[18] « Tracking GhostNet: Investigating a Cyber Espionage Network », (29 mars 2009) Information Warfare Monitor.

télécommunications chinoise transmet des informations de routage erronées relatives à 37 000 réseaux informatiques, ce qui détourne une partie du trafic Internet via la Chine pendant 20 minutes. L'attaque expose les données de 8 000 réseaux américains, 1 100 réseaux australiens et 230 réseaux français[19].

Cybertactiques chinoises

La République populaire de Chine (RPC) compte 1,35 milliard de personnes, soit plus de quatre fois la population des États-Unis. Ainsi, la Chine a souvent la possibilité de submerger les cyberdéfenses par la quantité et non par la qualité, tout comme elle l'a fait pendant la guerre de Corée et comme elle pourrait le faire dans n'importe quel autre type de conflit.

Les logiciels malveillants chinois analysés par les chercheurs de FireEye ne sont pas les plus évolués ou les plus créatifs. Mais dans de nombreux cas, ils n'en ont pas été moins efficaces. La Chine utilise des attaques de force brute qui représentent souvent le moyen le plus économique d'atteindre ses objectifs. Ces attaques réussissent en raison de leur volume considérable, de la prévalence et de la persistance des vulnérabilités dans les réseaux modernes, et de l'apparente indifférence des pirates à se faire prendre.

Reconnaissance	Listes de diffusion, renseignements d'un point d'eau, analyse, exploration des données sur les réseaux sociaux
Militarisation	EXE déguisés en fichiers non exécutables, formats de fichiers non-EXE malveillants, arrosage attaques du point d'eau
Livraison	Compromissions Web stratégiques, URL de harponnage dans les courriers électroniques, pièces jointes utilisées comme des armes, compromission de serveurs Web par analyse
Exploitation	Vulnérabilités zero-day des navigateurs et des applications, ingénierie sociale
Installation	Outils d'accès à distance riches en fonctionnalités et compacts dotés de capacités de contournement minimales (nécessité d'un opérateur pour mouvement latéral)
Commandement et contrôle (CnC)	HTTP avec codage standard incorporé (XOR) et codages personnalisés
Actions sur les objectifs	Recueil de renseignements, espionnage économique, accès persistent
Modèles d'outils, tactiques et procédures	Comment Crew

Tableau 1 : Caractéristiques des cyberattaques chinoises

Le « Comment Crew »[20], un exemple connu de cybermenace chinoise, est soupçonné d'être un sous-traitant du gouvernement de la RPC. Le Comment Crew est à l'origine de nombreuses attaques notables, dont l'Opération Beebus, qui a ciblé l'aérospatiale et la défense américaines[21].

[19] Vijayan, J. (18 novembre 2010) « Update: Report sounds alarm on China's rerouting of U.S. Internet traffic », *Computerworld*.

[20] Sanger, D., Barboza, D. & Perlroth, N. (18 février 2013) « Chinese Army Unit is seen as tied to Hacking against U.S. » *The New York Times*.

[21] Pidathala, V., Kindlund, D. & Haq, T. (1er février 2013) « Operation Beebus », FireEye.

Une caractéristique importante du Comment Crew et qui le place définitivement dans la catégorie des acteurs de menaces persistantes avancées (MPA) est qu'il s'agit d'un groupe structuré. Une analyse approfondie révèle l'existence d'un petit groupe de penseurs créatifs et stratégiques au sommet de l'organisation. Une couche plus bas, un groupe plus important de spécialistes conçoit et produit des logiciels malveillants de façon industrielle. À la base de la pyramide se trouvent les soldats, des pirates de force brute qui exécutent les ordres et lancent des campagnes de cyberattaques prolongées, de la reconnaissance de réseaux au harponnage (spear phishing) et à l'exfiltration de données. Et ils obtiennent des résultats. Après avoir décodé une des mémoires caches d'informations volées par le groupe, le Federal Bureau of Investigation (FBI) a estimé qu'il aurait fallu une pile de papier plus haute qu'un ensemble d'encyclopédies pour en imprimer les données[22].

Un groupe d'une telle envergure permet d'expliquer le comportement parfois incongru des pirates. Par exemple, un logiciel malveillant donné peut avoir été écrit par un expert, mais plus tard être mal utilisé par un soldat inexpérimenté (un courriel de harponnage mal écrit). Comprendre le cycle de vie d'une cyberattaque et ses différentes phases peut aider les cyberdéfenseurs à la reconnaître et à la déjouer. Dans toute grande organisation, certains processus sont moins matures que d'autres, et donc plus faciles à reconnaître.

Cyberdéfense chinoise

Pour leur propre défense, les autorités chinoises affirment que leur pays est également la cible de cyberattaques. En 2006, la China Aerospace Science & Industry Corporation (CASIC) trouve des logiciels espions sur son réseau classé secret[23]. En 2007, le ministère chinois de la Sécurité de l'État déclare que des pirates étrangers ont volé des informations chinoises, avec 42 % des attaques provenant de Taïwan et 25 % des États-Unis[24]. En 2009, le premier ministre chinois Wen Jiabao annonce qu'un pirate de Taïwan a volé son prochain rapport à l'Assemblée populaire nationale[25]. En 2013, Edward Snowden, un ancien administrateur système de la National Security Agency (NSA), publie des documents suggérant que les États-Unis mènent des activités de cyberespionnage contre la Chine[26] et l'équipe d'intervention d'urgence informatique chinoise (CERT) déclare qu'elle possède des « montagnes de données » relatives aux cyberattaques effectuées par les États-Unis[27].

[22] Riley, M. & Lawrence, D. (26 juillet 2012) « Hackers Linked to China's Army Seen From EU to D.C. », Bloomberg.
[23] « Significant Cyber Incidents Since 2006 », Center for Strategic and International Studies.
[24] *Ibid*.
[25] *Ibid*.
[26] Rapoza, K. (22 juin 2013) « U.S. Hacked China Universities, Mobile Phones, Snowden Tells China Press », *Forbes*.
[27] Hille, K. (5 juin 2013) « China claims 'mountains of data' on cyber attacks by US », *Financial Times*.

Corée du Nord : le parvenu

La Corée du Nord et la Corée du Sud restent prisonnières de l'un des conflits les plus difficiles à résoudre de la planète. La Corée du Nord (soutenue par la Chine) semble encore au cyberâge de pierre, en particulier par rapport à la Corée du Sud (soutenue par les États-Unis), qui dispose des vitesses de téléchargement les plus rapides du monde[28], et dont les étudiants utiliseront des tablettes au lieu de livres d'ici à 2015[29]. Toutefois, l'Internet offre à toute personne et à toute nation un moyen asymétrique de recueillir des renseignements et de projeter sa puissance nationale dans le cyberespace, et la Corée du Nord semble avoir récemment intégré les cyberattaques à son arsenal.

En 2009, la Corée du Nord lance sa première attaque majeure connue contre la Corée du Sud et les sites Web du gouvernement américain. L'attaque provoque peu de dommages, mais l'incident bénéficie d'une large couverture médiatique[30]. En 2013, toutefois, les acteurs de la menace ont mûri. Un groupe surnommé le « DarkSeoul Gang » est responsable d'attaques de grande envergure contre la Corée du Sud lancées pendant au moins quatre années. Les attaques de ce groupe comprennent une attaque par déni de service distribué (DDoS) et du code malveillant qui efface le contenu des disques durs dans les banques, les médias, les FAI, les opérateurs de télécommunications et les sociétés financières, en remplaçant les données de travail par des messages politiques. Dans le conflit coréen, de tels incidents se produisent souvent à des dates d'importance historique, dont le 4 juillet, jour de l'indépendance américaine[31]. Les attaques nord-coréennes suspectées sur les institutions des États-Unis visent entre autres des installations militaires américaines basées en Corée du Sud, la commission américaine des droits de l'homme en Corée du Nord, et même la Maison-Blanche.

Des transfuges nord-coréens indiquent l'existence d'un service de cyberguerre en plein essor, comptant 3 000 personnes en grande partie formées en Chine et en Russie. Les transfuges soulignent que la Corée du Nord éprouve une fascination grandissante pour les cyberattaques en tant que moyen rentable de rivaliser avec un adversaire supérieur au plan conventionnel. Ils estiment que la Corée du Nord devient de plus en plus efficace et confiante dans ce nouveau domaine de la guerre, et que l'Internet n'est pas seulement vulnérable aux attaques, mais que cette stratégie est susceptible d'engendrer une pression psychologique sur l'Occident. Pour cela,

---

[28] McDonald, M. (21 février 2011) « Home Internet May Get Even Faster in South Korea », *The New York Times*.
[29] Gobry, P-E. (5 juillet 2011) « South Korea Will Replace All Paper With Tablets In Schools By 2015 », *Business Insider*.
[30] Choe Sang-Hun, C. & Markoff, J. (8 juillet 2009) « Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea », *The New York Times*.
[31] « Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War » (27 juin 2013) Symantec.

la Corée du Nord s'est employée à déconnecter ses serveurs importants de l'Internet tout en mettant en place un « réseau d'attaque » dédié[32].

Les chercheurs de FireEye ont constaté l'usage intensif du harponnage et de la mise en place d'un « point d'eau », dans lequel un important site Web est piraté dans l'espoir de compromettre les ordinateurs de ses visiteurs suivants, appartenant généralement à une catégorie VIP ciblée par l'attaquant. Certaines attaques nord-coréennes commencent à manipuler les paramètres du système d'exploitation de la victime et à désactiver ses logiciels antivirus, des techniques qui sont normalement caractéristiques des pirates russes. En d'autres termes, les pirates nord-coréens ont peut-être appris ou bénéficient du soutien de la Russie.

En dehors de toute éventuelle perturbation ou destruction résultant des cyberattaques, les opérations sur les réseaux informatiques sont un précieux outil de collecte d'informations sensibles, en particulier quand ce dernières se trouvent sur des réseaux gouvernementaux ou de réflexion normalement inaccessibles à partir de l'Internet. La Corée du Nord, la Chine et la Russie sont toutes naturellement intéressées par le recueil de cyberrenseignements qui leur permettrait d'accroître leur avantage comparatif en matière d'informations secrètes, de positions de négociation diplomatique ou de futurs changements de politique.

Simultanément, la Corée du Nord affirme être la cible de cyberattaques provenant de Corée du Sud et des États-Unis. En juin 2013, lorsque la Corée du Nord subit une panne de deux jours de l'ensemble de ses sites internes, son agence d'information officielle dénonce « les attaques de virus concentrées et persistantes » et proclame que « les États-Unis et la Corée du Sud devront assumer la responsabilité de toutes les conséquences ». La Corée du Nord fait remarquer que l'attaque a eu lieu parallèlement à Key Resolve (manœuvres conjointes américano-sud-coréennes), mais le Comité des chefs d'États-majors interarmées des États-Unis nie tout lien[33].

[32] Fisher, M. (20 mars 2013) « South Korea under cyber attack: Is North Korea secretly awesome at hacking? » *The Washington Post*.
[33] Herman, S. (15 mars 2013) « North Korea Blames US, South for 'Cyber Attack' », Voice of America.


Inde – Pakistan : anciens rivaux, nouvelles tactiques

Une frontière lourdement fortifiée sépare l'Inde et le Pakistan sur la carte. Mais la nature calme et sans frontières du cyberespace fait que les deux camps sont libres de s'affronter dans le domaine du piratage informatique, même en temps de paix.

En 2009, l'Inde annonce que les pirates pakistanais ont placé des logiciels malveillants sur des sites populaires de téléchargement de musique indienne en guise de manière intelligente et indirecte de compromettre les systèmes indiens[34]. En 2010, la « Pakistani Cyber Army » défigure puis arrête le site Web du Central Bureau of Investigation, la principale agence de police de l'Inde[35]. En 2012, plus de 100 sites Web du gouvernement indien sont compromis[36].

Afin de ne pas être surpassés, en 2013, les pirates indiens lancent l'« Opération Hangover », une campagne de cyberespionnage indien à grande échelle qui frappe les réseaux informatiques, miniers, automobiles, juridiques, d'ingénierie, de services alimentaires, militaires et financiers du Pakistan[37]. Bien que les chercheurs ne puissent lier les attaques au gouvernement indien avec certitude, nombre d'objectifs constituent des facteurs de sécurité nationale[38].

[34] « Significant Cyber Incidents Since 2006 », Center for Strategic and International Studies.
[35] « India and Pakistan in cyber war » (4 décembre 2010) Al-Jazeera.
[36] Muncaster, P. (16 mars 2012) « Hackers hit 112 Indian gov sites in three months », *The Register*.
[37] « Operation Hangover: Q&A on Attacks » (20 mai 2013) Symantec.
[38] Snorre Fagerland, et al. « Operation Hangover: Unveiling an Indian Cyberattack Infrastructure », mai 2013.

Association des nations de l'Asie du Sud-Est (ANASE) : économies émergentes et cibles vulnérables

Depuis 2010 au moins, de nombreux acteurs de MPA (probablement basés en Chine) ont ciblé les gouvernements, les structures militaires et les entreprises de l'ANASE, association géopolitique et économique de l'Asie du Sud-Est composée de Brunei, de la Birmanie (Myanmar), du Cambodge, de l'Indonésie, du Laos, de la Malaisie, des Philippines, de Singapour, de la Thaïlande et du Vietnam. Bien que les risques d'éclatement à court terme d'une guerre régionale soient faibles, les activités de cyberespionnage régional sont importantes et constantes. Les industries ciblées comprennent les télécommunications, les transports, le pétrole et le gaz, les banques, et les groupes de réflexion. La motivation habituelle est d'acquérir un avantage tactique ou stratégique au plan politique, militaire et économique[39].

Les chercheurs de FireEye suivent de nombreux acteurs MPA dans cette région, y compris BeeBus, Mirage, Check Command, Taidoor, Seinup et Naikon. Leur tactique la plus courante est le harponnage, souvent au moyen de documents de leurre légitimes relatifs à l'économie nationale ou à la politique de la cible, à des événements régionaux tels que les sommets de l'ANASE, aux sommets de la Coopération économique Asie-Pacifique (APEC), à l'exploration des sources d'énergie ou aux affaires militaires.

FireEye estime que nombre de ces organisations économiques régionales constituent des cibles attrayantes pour les campagnes de MPA, car les informations qu'elles détiennent sont précieuses et leur niveau de sensibilisation à la cybersécurité est faible. Souvent, ces organisations souffrent d'une administration système disparate, d'une gestion irrégulière des correctifs, d'un mauvais contrôle des stratégies ou d'une combinaison quelconque de ces problèmes. Ainsi, nombre de ces réseaux sont des « fruits mûrs » pour les attaquants. Et pour aggraver les choses, les systèmes compromis sont utilisés comme points de départ de nouvelles attaques sur des cibles régionales, par l'installation de serveurs de commandement illicites (CnC), le détournement de comptes de messagerie légitimes et la diffusion de documents volés en guise d'appât.

[39] Finkle, J. (4 août 2011) « 'State actor' behind slew of cyber attacks », Reuters.

RUSSIE/EUROPE DE L'EST

Russie : un peu *trop* calme ?

En 1939, Winston Churchill déclare que le comportement russe est un « rébus enveloppé de mystère au sein d'une énigme ». Sept décennies plus tard, les chercheurs en cyberdéfense diraient que rien n'a vraiment changé. Par comparaison avec les constantes attaques détectées à partir de la Chine, on peut presque entendre la neige tomber sur la Place Rouge. Une des principales questions de la cybersécurité d'aujourd'hui est « où sont les Russes ? » Peut-être sont-ils tout simplement d'excellents pirates. Peut-être ont-ils des renseignements humains suffisants. Quelle que soit l'explication, les analystes de cyberdéfense cherchent souvent en vain les traces de pirates russes. Afin de nous orienter vers quelques réponses, toutefois, souvenons-nous de la seconde moitié de la citation de Churchill : « ... mais il y a peut-être une clé, et cette clé est l'intérêt national russe ».[40] En d'autres termes, il n'y a pas de fumée sans feu.

Dans le milieu des années 90, à l'aube du World Wide Web, la Russie est engagée dans une lutte prolongée sur le sort de la Tchétchénie. Les Tchétchènes deviennent des pionniers en matière de cyberpropagande, et les Russes deviennent des pionniers en matière d'arrêt de leurs sites Web. En 1998, lorsque la Serbie, alliée de la Russie, fait l'objet d'attaques de l'OTAN, les pirates pro-serbes sautent dans la mêlée en ciblant l'OTAN avec des attaques par déni de service et au moins vingt-cinq souches de virus. En 2007, la Russie est le principal suspect dans la plus célèbre cyberattaque internationale à ce jour : les attaques par saturation punitives sur l'Estonie pour avoir déplacé une statue de l'ère soviétique[41].

En 2008, les chercheurs découvrent des preuves incontestables du rôle de soutien joué par les opérations de réseau informatique dans les avancées militaires russes lors de l'invasion de la Géorgie[42]. Toujours en 2008, la Russie est suspectée dans ce que le sous-secrétaire américain à la défense William Lynn appelle la « violation la plus importante des ordinateurs militaires américains », une attaque sur Central Command (CENTCOM) effectuée au moyen d'une clé USB infectée[43]. En 2009, des pirates russes sont accusés dans « Climategate », une violation de la recherche universitaire visant à saper les négociations internationales sur l'atténuation des changements climatiques[44]. En 2010, l'OTAN et l'Union européenne avertissent de

[40] « Winston Churchill », Wikiquote.
[41] Geers K. (2008) « Cyberspace and the Changing Nature of Warfare », e-book *Hakin9*, 19(3) No. 6 ; *SC Magazine* (27 août 2008) 1-12.
[42] « Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008 », (août 2009) U.S. Cyber Consequences Unit.
[43] Lynn, W.J. (2010) « Defending a New Domain: The Pentagon's Cyberstrategy », *Foreign Affairs* 89(5) 97-108.
[44] Stewart, W. & Delgado, M. (6 décembre 2009) « Were Russian security services behind the leak of 'Climategate' emails? » *Daily Mail* et « Global warning: New Climategate leaks », (23 novembre 2011) RT.

l'augmentation des cyberattaques russes, alors que le FBI arrête et expulse un agent de renseignements russe potentiel nommé Alexey Karetnikov, qui occupe un poste de testeur de logiciels chez Microsoft[45].

Un aspect ironique des cyberattaques des États-nations, en particulier dans les pays autoritaires, est que beaucoup d'entre elles sont orientées vers l'intérieur. En 2012, la société de sécurité russe Kaspersky Lab annonce la découverte d'« Octobre Rouge »[46], une campagne de cyberattaque qui espionne des millions de citoyens à travers le monde, mais surtout au sein de l'ex-Union soviétique. Les cibles comprennent des ambassades, des bureaux d'études, des bases militaires, des fournisseurs d'énergie, des agences nucléaires et des infrastructures critiques[47]. De même, en 2013, des chercheurs trouvent des logiciels malveillants sur des millions de périphériques Android en Russie et dans les pays russophones. Chacune de ces attaques (ou les deux) pourrait partiellement s'expliquer par la volonté du gouvernement russe de surveiller sa propre population et celle des pays voisins[48].

Sous un angle positif et en guise de pas vers la cyberdétente, en 2013, les États-Unis et la Russie signent un accord de mise en place d'une « cyber-hotline » similaire au téléphone rouge utilisé pour les crises nucléaires pendant la guerre froide, afin de désamorcer les crises informatiques dans le futur[49]. Mais par mesure de sécurité, la Russie prend la mesure de cyberdéfense extrême consistant à acheter des machines à écrire mécaniques[50] et l'armée russe (comme celle des États-Unis, de la Chine et d'Israël) crée des unités de cybercombat[51].

[45] Ustinova, A. (14 juillet 2010) « Microsoft Says 12th Alleged Russian Spy Was Employee », Bloomberg.
[46] « The 'Red October' Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies » (14 janvier 2013) GReAT, Kaspersky Lab.
[47] Lee, D. (14 janvier 2013) « 'Red October' cyber-attack found by Russian researchers », BBC News
[48] Jackson Higgins, K. (3 août 2013) « Anatomy of a Russian Cybercrime Ecosystem Targeting Android », Dark Reading.
[49] Gallagher, S. (18 juin 2013) « US, Russia to install 'cyber-hotline' to prevent accidental cyberwar », Ars Technica.
[50] Ingersoll, G. (11 juillet 2013) « Russia Turns to Typewriters to Protect against Cyber Espionage », *Business Insider*.
[51] Gorshenin, V. (29 août 2013) « Russia to create cyber-warfare units », *Pravda*.

Tactique pirate russe

La plupart des cyberattaques les plus complexes et les plus évoluées portées à la connaissance des chercheurs de FireEye semblent provenir de Russie. Plus précisément, le code malveillant russe peut être nettement plus furtif que son homologue chinois, ce qui peut aussi le rendre plus inquiétant. La campagne « Octobre Rouge », y compris son logiciel satellite baptisé « Spoutnik », est un exemple significatif de logiciels malveillants d'origine probablement russe.

Reconnaissance	Sources de renseignements probablement humaines
Militarisation	Formats de fichiers DOC/XLS malveillants
Livraison	Pièces jointes utilisées comme des armes
Exploitation	Vulnérabilités zero-day des applications
Installation	Outil d'accès à distance riche en fonctionnalités avec modules chiffrés
Commandement et contrôle (CnC)	HTTP avec chiffrement/déchiffrement personnalisé incorporé
Actions sur les objectifs	Recueil de renseignements (en relation avec les gouvernements)
Modèles d'outils, tactiques et procédures	Octobre Rouge

Tableau 2 : Caractéristiques des cyberattaques russes

Les outils, tactiques et procédures utilisés comprennent souvent la livraison de pièces jointes utilisées comme des armes, mais les pirates russes semblent être experts dans l'art de changer leurs modèles d'attaque, leurs codes malveillants et leurs méthodes d'exfiltration des données afin d'échapper à la détection. En fait, un aspect révélateur des pirates russes semble être que, contrairement aux Chinois, ils produisent des efforts extraordinaires pour dissimuler leur identité et leurs objectifs. Les analystes de FireEye ont même vu des exemples de cyberopérations sous une fausse bannière dont la conception semblait provenir d'Asie.

Autre problème pour les chercheurs en cyberdéfense, certaines portes dérobées russes dans les systèmes compromis sont difficiles à distinguer de violations criminelles avancées.

MOYEN-ORIENT

La région du Moyen-Orient ne possède sans doute pas l'arsenal de codes malveillants « zero-day » de la Russie ou la force brute de la Chine. Par conséquent, les pirates du Moyen-Orient doivent compter sur des cybertactiques qui tirent parti de l'innovation, de la créativité et de la tromperie.

Par exemple, la campagne Mahdi de 2012 utilise des fichiers Word, PowerPoint et PDF malveillants pour infecter ses cibles au Moyen-Orient. Cette approche est semblable à celle de beaucoup d'autres assaillants. Mais ces attaques de logiciels malveillants sont accompagnées d'éléments imaginatifs tels que des jeux, des images attrayantes et des animations personnalisées spécifiquement conçus pour favoriser l'attaque.

Reconnaissance	Listes de diffusion régionales, conférences
Militarisation	Fichiers PPT/PPS malveillants
Livraison	Pièces jointes utilisées comme des armes
Exploitation	Ingénierie sociale, clics de souris sur l'écran
Installation	Collection primitive d'outils et outils d'accès à distance personnalisés (nécessité d'un opérateur pour mouvement latéral)
Commandement et contrôle (CnC)	HTTP standard, dissimulation en pleine vue
Actions sur les objectifs	Recueil de renseignements (en relation avec le Moyen-Orient), déni de service
Modèles d'outils, tactiques et procédures	Mahdi, LV

Tableau 3 : Caractéristiques des cyberattaques du Moyen-Orient

Non seulement les utilisateurs ont-ils été incités à exécuter des commandes pour installer du code malveillant, mais leur attention a aussi été détournée des messages d'avertissement relatifs aux logiciels malveillants. En outre, les attaques Mahdi ont été adaptées à des publics cibles spécifiques, par exemple en proposant des variantes de jeux propres à chaque organisation visée. Des frappes aussi ponctuelles se fondent sur une reconnaissance préalable, permettent de contourner les mécanismes de détection comportementale de la cyberdéfense, et accroissent considérablement les chances de compromission. Ainsi, au Moyen-Orient, la relative sophistication d'une attaque se calcule moins d'après sa technologie, et plus d'après les moyens astucieux de livrer et d'installer les logiciels malveillants sur le réseau cible.

Iran : une cyberguerre « chaude »

Partout où une activité importante survient dans le monde réel (y compris en matière de crime, d'espionnage et de guerre), une activité parallèle se déroule dans le cyberespace. Il n'est donc pas surprenant que l'Iran, qui entretient des relations internationales tendues et est sur le point d'acquérir la bombe nucléaire, ait également subi les cyberattaques les plus sophistiquées à ce jour.

En 2010, Stuxnet est une sorte de « cybermissile » conçu avec une précision minutieuse pour s'enfoncer profondément dans le programme nucléaire iranien et en détruire l'infrastructure physique. Dans une certaine mesure, ce logiciel remplace un escadron d'avions de chasse qui auraient violé un espace aérien étranger, largué des bombes guidées par laser et laissé un cratère fumant à la surface de la Terre[52]. Au-delà de Stuxnet, d'autres attaques d'espionnage avancées ont inquiété les experts en sécurité, dont Duqu, Flame et Gauss, qui proviennent potentiellement du même acteur de menace[53]. Et même les amateurs ciblent l'Iran avec succès. Bien que le malware Mahdi soit beaucoup moins sophistiqué que Stuxnet et ses cousins, il a déjà réussi à compromettre des entreprises d'ingénierie, des organismes gouvernementaux, des établissements financiers et des universités dans tout le Moyen-Orient[54].

Alors, comment quelqu'un, y compris un État-nation, peut-il répondre à une cyberattaque ? La contre-attaque reste-t-elle limitée au cyberespace ou peut-elle prendre la forme d'une agression militaire traditionnelle (ou terroriste) ? En 2012, l'Iran semble avoir choisi la première option. Un groupe de pirates appelé « L'épée tranchante de la justice » utilise le virus « Shamoon » pour attaquer la compagnie pétrolière saoudienne Aramco, supprimant les données des trois quarts des PC d'Aramco (dont les documents, feuilles de calcul, courriels et fichiers) et les remplaçant par l'image d'un drapeau américain en flammes[55]. Au cours de l'année dernière, un autre groupe appelé *Izz ad-Din al-Qassam* lance l'« Opération Ababil », une série d'attaques par déni de service contre de nombreuses institutions financières américaines, y compris la Bourse de New York[56].

---

[52] Sanger, D. *Confront and Conceal*. (New York, 2012) pp. 188-225.
[53] Boldizsár Bencsáth. « Duqu, Flame, Gauss: Followers of Stuxnet », BME CrySyS Lab, RSA 2012.
[54] Simonite, T. (31 août 2012) « Bungling Cyber Spy Stalks Iran », *MIT Technology Review*.
[55] Perlroth, N. (23 octobre 2012) « In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back », *The New York Times*.
[56] Walker, D. (8 mars 2013) « Hacktivists plan to resume DDoS campaign against U.S. banks », *SC Magazine*.

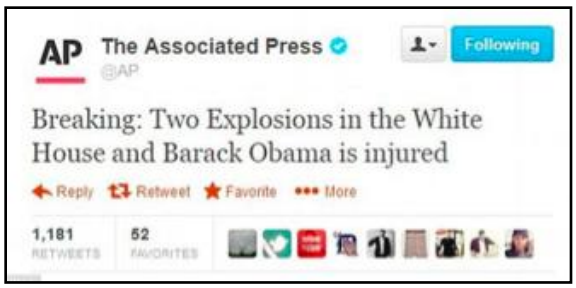
D'autres exemples de cyberattaques ne manquent pas. En 2009, les plans d'un nouvel hélicoptère présidentiel US Marine Corps 1 sont trouvés sur un réseau de partage de fichiers en Iran[57]. En 2010, l'« Iranian Cyber Army » perturbe Twitter et le moteur de recherche chinois Baidu en redirigeant les utilisateurs vers des messages politiques iraniens[58]. En 2011, des pirates iraniens compromettent une autorité de certification numérique néerlandaise et publient plus de 500 certificats frauduleux pour de grandes entreprises et des organismes gouvernementaux[59]. En 2012, l'Iran perturbe le service en langue persane de la BBC et les chercheurs de l'Université de Toronto signalent que certaines versions du logiciel « proxy » Simurgh (qui est populaire dans les pays comme l'Iran et anonymise le trafic Internet) installent également un cheval de Troie qui recueille les noms d'utilisateur et les séquences de touches frappées au clavier et les envoie probablement à un site de collecte de renseignements[60]. Enfin, en 2013, le *Wall Street Journal* signale que des acteurs iraniens ont intensifié leurs efforts pour compromettre les infrastructures critiques américaines[61].

Syrie : en quoi consiste l'armée électronique syrienne ?

La Syrie est en proie à une guerre civile, de sorte que les chercheurs ont une forte cyberactivité à analyser. Le groupe de pirates le plus connu est la Syrian Electronic Army (armée électronique syrienne, SEA), fidèle au président syrien Bashar al-Assad. La SEA effectue des attaques par déni de service, hameçonnage, dégradations pro-Assad et campagnes de pourriels contre les gouvernements, les services en ligne et les médias perçus comme hostiles au gouvernement syrien. La SEA a piraté *Al-Jazeera*, Anonymous, Associated Press (AP), la BBC, le *Daily Telegraph*, le *Financial Times*, le *Guardian*, Human Rights Watch, la National Public Radio, *The New York Times*, Twitter, et d'autres[62]. Son exploit le plus célèbre est une annonce canular passée au moyen du compte Twitter d'AP, informant du bombardement de la Maison-Blanche et des blessures du président Obama, qui provoque une brève plongée des marchés boursiers pour une valeur de 200 milliards de dollars[63].

---

[57] Borak, D. (3 mars 2009) « Source in Iran views Marine One blueprints », *Marine Corps Times*.
[58] Wai-yin Kwok, V. (13 janvier 2010) « Baidu Hijacked By Cyber Army », Forbes.
[59] Charette, R. (9 Sep 2011) « DigiNotar Certificate Authority Breach Crashes e-Government in the Netherlands », *IEEE Spectrum*.
[60] « Iranian anti-censorship software 'Simurgh' circulated with malicious backdoor » (25 mai 2012) Citizenlab.
[61] Gorman, S. & Yadron, D. (23 mai 2013) « Iran Hacks Energy Firms, U.S. Says », *Wall Street Journal*.
[62] Fisher, M. & Keller, J. (31 août 2011) « Syria's Digital Counter-Revolutionaries. » *The Atlantic* ; « Syrian Electronic Army », (accessed 25 juillet 2013) *Wikipedia*.
[63] Manzoor, S. (25 juillet 2013) « Slaves to the algorithm: Are stock market math geniuses, or quants, a force for good? » *The Sunday Telegraph*.



Pour le seul mois de juillet 2013, la SEA a compromis trois sites de communication en ligne largement utilisés : TrueCaller (le plus grand annuaire téléphonique de la planète)[64], Tango (un service de messagerie vidéo et texte)[65] et Viber (une application d'appel en ligne et de messagerie gratuite)[66]. Ces types de compromissions sont importants, car ils pourraient donner aux services de renseignement syriens l'accès aux communications de millions de personnes, dont des militants politiques se trouvant en Syrie qui pourraient ensuite être ciblés pour espionnage, intimidation et arrestation.

Afin de compromettre ses cibles, la SEA envoie souvent des courriels d'ingénierie sociale et de harponnage conçus pour pousser les militants de l'opposition à ouvrir des documents malveillants utilisés comme des armes. Si le destinataire se laisse tromper, un cheval de Troie, un outil d'accès à distance est installé sur son ordinateur et peut transmettre à l'attaquant des séquences clavier, des captures d'écran, des enregistrements effectués par le microphone et la webcam, des documents volés et des mots de passe. Et bien sûr, la SEA envoie probablement toutes ces informations à une adresse se trouvant à l'intérieur de l'espace IP contrôlé par le gouvernement syrien pour collecte et examen[67].

Israël : ancien conflit, nouvelles tactiques

Même pendant la guerre froide, le conflit israélo-arabe a connu de nombreuses phases chaudes, et a souvent été le banc d'essai de nouvelles armes et tactiques militaires. Rien n'a changé à l'ère de l'Internet. Depuis l'année 2000 au moins, les pirates pro-israéliens ont ciblé des sites

[64] Khare, A. (19 juillet 2013) « Syrian Electronic Army Hacks Truecaller Database, Gains Access Codes to Social Media Accounts », *iDigital Times*.
[65] Kastrenakes, J. (22 juillet 2013) « Syrian Electronic Army alleges stealing 'millions' of phone numbers from chat app Tango », *The Verge* ; Albanesius, C. (23 juillet 2013) « Tango Messaging App Targeted by Syrian Electronic Army », *PCMag*.
[66] Ashford, W. (24 juillet 2013) « Syrian hacktvists hit second mobile app in a week », *Computer Weekly*.
[67] Tsukayama, H. (28 août 2013) « Attacks like the one against the New York Times should put consumers on alert », *The Washington Post*.

d'importance politique et militaire au Moyen-Orient[68]. En 2007, Israël aurait perturbé les réseaux de défense aérienne syriens au moyen d'une cyberattaque (avec quelques dommages collatéraux infligés à ses propres réseaux domestiques) afin de faciliter la destruction d'une prétendue installation nucléaire syrienne par l'armée de l'air israélienne[69].

Mais en tant que nation industriellement évoluée, Israël dépend également de technologies de l'information. Le pays s'est avéré vulnérable aux cyberattaques qui visent souvent son économie. En 2009, lors de l'opération militaire israélienne à Gaza, des pirates paralysent brièvement de nombreux sites du gouvernement au moyen d'une attaque par déni de service lancée à partir d'au moins 500 000 ordinateurs. L'attaque de 2009 se compose de quatre vagues indépendantes, chacune plus puissante que la précédente, avec un pic à 15 millions de pourriels par seconde. Le site israélien du « Home Front Command », qui joue un rôle clé dans les communications nationales relatives à la défense avec le public, reste indisponible pendant trois heures. En raison de similarités techniques avec la cyberattaque de 2008 sur la Géorgie lors de la guerre avec la Russie, les responsables israéliens supposent que l'attaque elle-même aurait été menée par une organisation criminelle située dans l'ex-Union soviétique et payée par le Hamas ou le Hezbollah[70].

Le problème en ce qui concerne les cyberattaques est souvent qu'elles n'ont pas besoin d'être hautement sophistiquées pour réussir, même contre la méfiance d'Israël. En 2012, le logiciel malveillant Mahdi maladroitement écrit[71] compromet au moins 54 cibles en Israël[72]. Dernier point, mais non des moindres, en 2013, les médias iraniens signalent que l'armée syrienne a exécuté une cyberattaque contre l'approvisionnement en eau de la ville israélienne de Haïfa. Le professeur Isaac Ben-Israel, conseiller du premier ministre Benyamin Netanyahou en matière de cybersécurité, déclare que le rapport est faux, mais ajoute que les cyberattaques sur les infrastructures critiques constituent une « menace réelle et présente » contre Israël[73].

[68] Geers K. (2008) « Cyberspace and the Changing Nature of Warfare », e-book *Hakin9*, 19(3) No. 6 ; *SC Magazine* (27 août 2008) 1-12.
[69] Carroll, W. (26 novembre 2007) « Israel's Cyber Shot at Syria », *Defense Tech*.
[70] Pfeffer, A. (15 juin 2009) « Israel suffered massive cyber attack during Gaza offensive », *Haaretz*.
[71] Simonite, T. (31 août 2012) « Bungling Cyber Spy Stalks Iran », *MIT Technology Review*.
[72] Zetter, K. (17 juillet 2012) « Mahdi, the Messiah, Found Infecting Systems in Iran, Israel », *WIRED*.
[73] Yagna, Y. (26 mai 2013) « Ex-General denies statements regarding Syrian cyber attack », *Haaretz*.

L'OCCIDENT

États-Unis

Les analystes estiment que les États-Unis ont mené les cyberattaques les plus sophistiquées à ce jour, y compris Stuxnet[74], Duqu, Flame et Gauss[75]. Cette famille de logiciels malveillants est inégalée dans sa complexité et sa capacité de ciblage. Stuxnet en particulier a été développé avec un objectif unique (perturber le programme iranien d'enrichissement nucléaire). Il a été à la fois étroitement ciblé et capable d'offrir des gains stratégiques dans l'arène internationale. Contrairement aux vers informatiques tels que Slammer et Code Red, Stuxnet n'a pas cherché à compromettre autant d'ordinateurs que possible, mais *aussi peu* que possible. Fait encore plus étonnant, son comportement malveillant a été dissimulé sous une couche de données opérationnelles apparemment légitimes, mais en fin de compte, ce malware a détruit des centrifugeuses iraniennes.

Reconnaissance	Sources de renseignements probablement humaines
Militarisation	Médias amovibles auto-infectés
Livraison	Médias amovibles USB
Exploitation	Ingénierie sociale, utilisation des médias USB
Installation	Ver bien conçu et ciblé (crypto-clé, aucun opérateur requis, mouvement latéral automatique)
Commandement et contrôle (CnC)	Utilisation stratégique unique de nœuds CnC, cryptographie SSL complète
Actions sur les objectifs	Recueil de renseignements, perturbations subtiles des systèmes (en relation avec le Moyen-Orient)
Modèles d'outils, tactiques et procédures	Stuxnet, Flame, Duqu, Gauss

Tableau 4 : Caractéristiques des cyberattaques occidentales

Cette famille de logiciels malveillants a été superbement conçue. Par exemple, sa charge utile peut arriver à destination chiffrée et être déchiffrée et installée uniquement sur un périphérique cible. Cela permet au logiciel malveillant d'échapper aux regards inquisiteurs des cyberdéfenseurs et rend sa découverte et sa rétro-ingénierie beaucoup plus difficiles.

Ironiquement, cette famille de logiciels malveillants pourrait être un modèle d'hypercomplexité. Par exemple, elle utilise non seulement de multiples exploits « zero-day », mais aussi des premières informatiques mondiales telles que la « collision de hachage » forcée[76]. Dans le cas de l'Iran (actuellement soumis à un embargo commercial restreignant l'acquisition de haute technologie), on peut douter que beaucoup de logiciels iraniens soient actualisés ou

[74] Sanger, D. *Confront and Conceal*. (New York, 2012) pp. 188-225.
[75] Boldizsár Bencsáth. « Duqu, Flame, Gauss: Followers of Stuxnet », BME CrySyS Lab, RSA 2012.
[76] Goodin, Dan (7 juin 2012) « Crypto breakthrough shows Flame was designed by world-class scientists », *Ars Technica*.

correctement configurés. Ainsi, les auteurs de Stuxnet auraient pu utiliser des exploits plus classiques et néanmoins réussir.

Un des aspects possibles des cyberattaques américaines est le suivant : elles nécessitent de tels investissements financiers, une telle sophistication technique et une telle supervision juridique qu'elles se démarquent. Sur ce dernier point, Richard Clarke, fonctionnaire spécialisé en contre-terrorisme de trois présidents américains, fait valoir que Stuxnet était une opération américaine parce que le logiciel « semblait fortement avoir été écrit ou dirigé par une équipe d'avocats de Washington »[77]. Enfin, la quantité de travail fournie pour ces opérations suggère la participation d'un grand nombre de fournisseurs spécialisés dans les aspects particuliers d'une vaste et complexe entreprise de défense.

L'inconvénient (similaire au cas d'Israël) est que toute économie industriellement évoluée est vulnérable aux cybercontre-attaques. En 2008, un fonctionnaire de la CIA informe un groupe de fournisseurs d'infrastructures critiques que des pirates inconnus ont pu perturber à plusieurs reprises l'alimentation électrique de diverses villes étrangères[78]. Dans le domaine militaire, les insurgés irakiens utilisent un logiciel du commerce valant 26 dollars pour intercepter les flux vidéo en direct de drones américains Predator, ce qui peut leur donner la possibilité de surveiller les opérations militaires américaines et d'y échapper[79]. Dans le domaine économique, le Fonds monétaire international (FMI) basé aux États-Unis est victime d'une attaque d'hameçonnage en 2011, décrite comme une « violation très importante »[80].

Ainsi, les cyberattaques sont un phénomène nouveau et représentent un défi croissant pour la sécurité nationale. Dans le cadre d'un effort plus important visant à atténuer la menace, le président Obama signe en 2013 une directive selon laquelle les États-Unis doivent aider leurs alliés subissant des cyberattaques étrangères[81].

[77] Rosenbaum, R. (avril 2012) « Richard Clarke on Who Was Behind the Stuxnet Attack », *Smithsonian*.
[78] Nakashima, E. & Mufson, S. (19 janvier 2008) « Hackers Have Attacked Foreign Utilities, CIA Analyst Says », *Washington Post*.
[79] Gorman, S., Dreazen, Y. & Cole, A. (17 décembre 2009) « Insurgents Hack U.S. Drones », *Wall Street Journal*.
[80] Sanger, D. & Markoff, J. (11 juin 2011) « I.M.F. Reports Cyberattack Led to 'Very Major Breach' », *New York Times*.
[81] Shanker, T. & Sanger, D. (8 juin 2013) « U.S. Helps Allies Trying to Battle Iranian Hackers », *New York Times*.

Europe

Aucun exemple marquant de cyberattaque n'a été constaté en ce qui concerne l'Union européenne (UE) ou l'Organisation du traité de l'Atlantique nord (OTAN). Au contraire, leurs dirigeants y ont jusqu'ici renoncé[82]. Mais de nombreux exemples montrent que les réseaux européens sont piratés depuis d'autres parties du monde, la Chine et la Russie notamment.

En 2010, les cyberattaques lancées sur le ministère britannique des Affaires étrangères défient les défenses du réseau et prétendent provenir de la Maison-Blanche[83]. En 2011, la police allemande constate que les serveurs utilisés pour localiser les criminels et les personnes soupçonnées de terrorisme ont été pénétrés, initialement par une attaque d'hameçonnage[84]. Toujours en 2011, les fonctionnaires de la Commission européenne sont ciblés lors d'un Forum sur la gouvernance de l'Internet (FGI) en Azerbaïdjan[85].

Dans le domaine militaire, en 2009, des avions de la Marine française restent cloués au sol suite à une infection par le ver Conficker[86]. En 2012, le Royaume-Uni reconnaît que des pirates ont pénétré les réseaux de défense classés secrets[87].

Dans le domaine des affaires en 2011, le marché du carbone de l'Union européenne est piraté, avec pour conséquences le vol de plus de 7 millions de dollars en crédits et la fermeture temporaire du marché[88]. En 2012, l'European Aeronautic Defence and Space company (EADS) et le sidérurgiste allemand ThyssenKrupp sont victimes d'importantes attaques lancées par des pirates chinois[89].

Les professionnels de la sécurité doivent notamment être à l'affût des cybermenaces persistantes avancées immédiatement avant et pendant les négociations internationales. Pendant la seule année 2011, la Commission européenne s'est plainte d'un piratage généralisé avant un sommet de l'UE[90], le gouvernement français a été compromis avant une réunion du

---

[82] Leyden, J. (6 juin 2012) « Relax hackers! NATO has no cyber-attack plans - top brass », *The Register*.
[83] Arthur, C. (5 février 2011) « William Hague reveals hacker attack on Foreign Office in call for cyber rules », *The Observer*.
[84] « Hackers infiltrate German police and customs service computers », (18 juillet 2011) *Infosecurity Magazine*.
[85] Satter, R. (10 novembre 2012) « European Commission Officials Hacked At Internet Governance Forum », *Huffington Post*.
[86] Willsher, K. (7 février 2009) « French fighter planes grounded by computer virus », *The Telegraph*.
[87] Hopkins, N. (3 mai 2012) « Hackers have breached top secret MoD systems, cyber-security chief admits », *The Guardian*.
[88] Krukowska, E. & Carr, M. (20 janvier 2011), « EU Carbon Trading Declines After Alleged Hacking Suspends Spot Market », Bloomberg.
[89] Rochford, O. (24 février 2013) « European Space, Industrial Firms Breached in Cyber Attacks: Report », *Security Week*.
[90] « 'Serious' cyber attack on EU bodies before summit » (23 mars 2011) BBC.

G20[91], et au moins dix entreprises de défense et d'énergie norvégiennes ont été piratées à grande échelle pendant la négociation de contrats, par un hameçonnage conçu sur mesure pour chaque entreprise[92].

[91] Charette, R. (8 mars 2011) « 'Spectacular' Cyber Attack Gains Access to France's G20 Files », *IEEE Spectrum*.
[92] Albanesius, C. (18 novembre 2011) « Norway Cyber Attack Targets Country's Oil, Gas Systems », *PCMag*.

CONCLUSION

World War Z raconte l'histoire de comportements nationaux idiosyncrasiques en réponse à une crise internationale majeure. Le présent document cherche à mettre en évidence le même phénomène en ce qui concerne les défis posés par la cyberinsécurité nationale et les cyberattaques internationales. Derrière chaque incident se cache une intention et des individus, tous uniques et finalement identifiables. Plus une cybercampagne est importante, plus elle génère de données utilisables par les chercheurs en sécurité, et plus il est difficile pour les attaquants de rester anonymes et de cacher leurs intentions.

En ce qui concerne les prédictions, personne ne sait à quoi ressemblera la prochaine cyberattaque. Mais compte tenu des tendances récentes, nous pouvons faire quelques suppositions éclairées.

Voici cinq facteurs qui pourraient changer le paysage de la cybersécurité dans le monde à court et à moyen terme :

1. **Panne des infrastructures critiques nationales :** nous savons que les cyberattaques peuvent perturber les réseaux gouvernementaux, mais la plupart des cas les plus courants n'atteignent tout simplement pas le niveau de menace à la sécurité nationale. Stuxnet et les représailles présumées de l'Iran contre Saudi Aramco ont fait passer la réflexion sur la cyberguerre de la théorie à quelque chose de plus proche de la réalité. Mais avons-nous vu la limite des cyberattaques ou les pirates pourraient-ils menacer la sécurité publique en arrêtant un réseau électrique ou un marché financier ?
2. **Traité sur les cyberarmes :** si les dirigeants mondiaux commencent à voir les cyberattaques plus comme un handicap qu'une opportunité, ils peuvent convenir d'un régime de contrôle des cyberarmes ou signer un pacte de non-agression dans le cyberespace. Toutefois, le contrôle des armes nécessite la capacité de vérifier l'absence d'un objet interdit. Le proverbe russe préféré du président Reagan était « доверяй, но проверяй » (aie confiance, mais vérifie). Étant donné qu'une seule clé USB peut maintenant contenir des milliards de bits d'information, la vérification est plus facile à dire qu'à faire.
3. **PRISM, liberté d'expression et vie privée :** nous sommes encore à l'aube de l'ère de l'Internet et cette conversation ne fait que commencer. Elle englobe Daniel Ellsberg, Chelsea Manning et Edward Snowden, ainsi que la Déclaration d'Indépendance, Enigma, et The Onion Router. Aujourd'hui, les politiciens, les espions et les hippies sont tous conscients du débat critique qui se profile à l'horizon : quel degré de vie privée devons-nous avoir en ligne ?
4. **Nouveaux acteurs sur la cyberscène :** le caractère révolutionnaire de l'informatique et la puissance d'amplification des réseaux ne sont pas le seul apanage des plus grandes nations du monde. L'Iran, la Syrie, la Corée du Nord, et même des acteurs non étatiques tels qu'Anonymous ont utilisé des cyberattaques pour diriger leur diplomatie et faire la guerre par d'autres moyens. Les chercheurs ont peu de raisons de penser que d'autres gouvernements ne sont pas actifs dans ce domaine. Les candidats possibles pourraient être :
    - **la Pologne :** ce sont les Polonais qui ont décrypté le chiffre allemand Enigma… en 1932 ! Aujourd'hui, étant donné son talent en programmation et sa rivalité bien connue avec la Russie, c'est une possibilité.

- **le Brésil :** base de certains cybercriminels les plus prolifiques au monde, le gouvernement brésilien en colère suite aux récentes révélations de cyberespionnage américain exploitera-t-il ces talents à des fins géopolitiques ?
- **Taïwan :** au vu des cyberattaques constantes provenant de la Chine continentale, Taïpei n'a guère d'autre choix que réagir.

5. **Mettre l'accent sur les contournements :** comme nous l'avons vu, certains États-nations savent lancer des cyberattaques furtives. Alors que l'art de la cyberdéfense arrive à maturité et que le grand public est de plus en plus conscient du phénomène *World War C*, certains cyberattaquants « bruyants » tels que la Chine peuvent être contraints de placer la barre plus haut en essayant de rester sous un radar mieux réglé.

L'analyse et les conclusions du présent document relèvent du domaine de la conjecture. La cybersécurité, le cyberespionnage et la cyberguerre sont des concepts nouveaux et en évolution rapide. En outre, la plupart des opérations de réseaux informatiques sont voilées par le secret et la tromperie est un fait établi.

« Une cyberattaque vue hors de son contexte géopolitique ne permet qu'une très mince marge de manœuvre juridique à l'État qui s'en défend, explique le professeur Thomas Wingfield du Marshall Center dans une récente interview par courriel accordée à FireEye. Les opérations effectuées sous une fausse bannière et la nature même de l'Internet font de l'attribution tactique un jeu où l'on perd à chaque fois. »

Mais Wingfield ajoute que l'attribution stratégique, par fusion de toutes les sources de renseignements sur une menace potentielle, permet d'obtenir un niveau de confiance beaucoup plus élevé et offre davantage de possibilités aux décideurs gouvernementaux.

« Et l'attribution stratégique commence et se termine par l'analyse géopolitique », ajoute-t-il.

Dans cet esprit, nous espérons que la prise de conscience de la dynamique de World War C aidera les professionnels de la cybersécurité à mieux comprendre, identifier et combattre les cyberattaques futures.

À PROPOS DE FIREEYE

FireEye est l'inventeur d'une plateforme de sécurité à base de machines virtuelles qui offre une protection en temps réel contre les menaces et la prochaine génération de cyberattaques visant les entreprises et les gouvernements du monde entier. Ces cyberattaques hautement sophistiquées contournent facilement les défenses traditionnelles basées sur les signatures, telles que les pare-feu de nouvelle génération, les solutions IPS, les logiciels antivirus et les passerelles. La plateforme FireEye offre une protection dynamique et en temps réel contre les menaces sans utiliser de signatures et permet de protéger toute organisation sur les principaux vecteurs de menaces, y compris le Web, le courrier électronique et les fichiers, tout au long des différentes étapes du cycle de vie d'une attaque. La plateforme FireEye est articulée autour d'un moteur d'exécution virtuelle complété par des informations dynamiques relatives aux menaces et permet d'identifier et de bloquer les cyberattaques en temps réel. FireEye compte plus de

1 000 clients dans plus de 40 pays, dont plus de 100 entreprises inscrites au classement Fortune 500.

Pour plus d'informations sur la protection contre les menaces de nouvelle génération, visitez www.FireEye.com.