Lettre n°55-Octobre 2016-disponible sur omc.ceis.eu

Brève du mois

« L'échec quasi-systématique des responsables de l'implémentation [du protocole DSA] à utiliser des méthodes de génération de nombres premiers vérifiables signifie que l'utilisation de nombres premiers faibles serait en pratique indétectable et aurait peu de chance de susciter la suspicion. »[1], *A kilobit hidden SNFS discrete logarithm computation*[2].

TABLE DES MATIERES

[1] http://www.computerworld.com/article/3130244/security/encrypted-communications-could-have-an-undetectable-backdoor.html

[2] https://eprint.iacr.org/2016/961.pdf, Joshua Fried, Pierrick Gaudry, Nadia Heninger, Emmanuel Thomé, University of Pennsylvania, INRIA, CNRS, Université de Lorraine.

« GET OFF THE FIRING LINE, PIKACHU ! »
REVUE DES RISQUES ASSOCIES AUX PRATIQUES DE JEU « AUGMENTEES »

Sources Israel Navy et US Marines

Le 12 juillet, la Marine israélienne publiait sur son compte Facebook un montage photo (ci-dessus à gauche), dans lequel on aperçoit un officier en exercice tenir une « Pokéball » face à « Léviator », un monstre issu de l'univers Pokémon[3]. Cette franchise japonaise créée à la fin des années 1990, qui a connu un immense succès planétaire, notamment en France, au début des années 2000, vient de se refaire une jeunesse, avec le jeu mobile en réalité augmentée « Pokémon Go ». Le 10 août, le site Guiness des Records annonçait que cinq records du monde avaient été battus par l'application, dont celle du nombre de téléchargements en un mois pour un jeu sur mobile, soit 130 millions[4]. Le 11 juillet, les Marines américains avaient déjà profité du lancement en pleine fanfare du jeu aux Etats-Unis pour proposer leur propre montage photo « décalé » sur leur fil Twitter, visant sans doute un public relativement jeune. On pouvait lire en légende : « Ecarte-toi de la ligne de tir, Pikachu [monstre emblématique de la saga] ! C'est une violation des règles de sécurité ! »

Que les deux montages aient ou non produit l'effet escompté, à savoir surfer sur le « buzz » du moment, est somme toute anecdotique. Néanmoins, avec ces clichés, les forces de défense israéliennes et américaines ont mis en alerte leurs états-majors respectifs. L'objet de cette note est de comprendre à quels risques

[3] Le nom de ce monstre est dérivé d'une créature biblique, le Léviathan, qui a également donné son nom à un gisement de gaz majeur, objet d'un litige avec le Liban et Chypre. Le choix du montage n'est donc peut-être pas anodin.

[4] Guinness des Records, 10 août 2016.

concrets s'exposent les forces armées face à ces jeux en réalité augmentée, et quelles opportunités peuvent en naître.

Réalité augmentée vs. Réalité virtuelle dans le secteur du jeu

Si les deux concepts sont souvent présentés conjointement, la réalité virtuelle se distingue nettement de la réalité augmentée par l'impact du risque sur la sécurité physique. Alors que la réalité virtuelle (ou « VR » selon son acronyme anglais) s'applique à créer des mondes virtuels dans lesquels les joueurs peuvent évoluer et qu'ils peuvent observer par le biais de terminaux dédiés tels que des casques ou des lunettes, les développeurs de jeux à réalité augmentée (ou « AR ») « superposent » en quelque sorte le monde réel avec des « inputs » virtuels : par exemple le monde vu de la webcam d'un Smartphone avec des « monstres de poche » dans le cas de « Pokémon Go ». Ainsi, avec la réalité augmentée, le joueur peut clairement distinguer ce qui est réel (son environnement) de ce qui ne l'est pas (dans notre exemple, les monstres).

Source Super Reality Blog

De la simple distraction au risque pour l'ordre public…

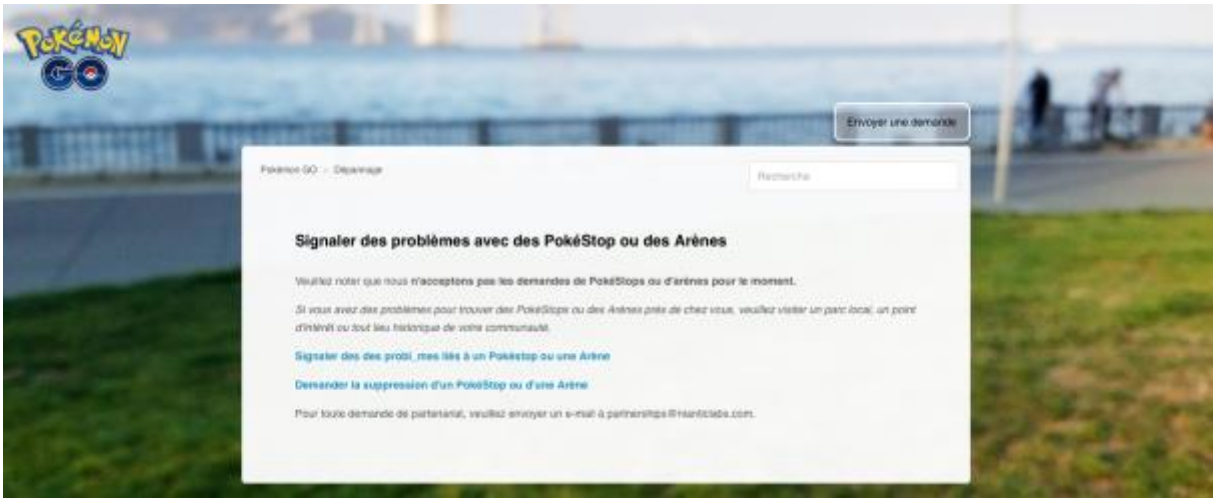
Cette distinction fondamentale permet de comprendre pourquoi le joueur est davantage « conscient » des risques qui l'entourent, même si les anecdotes mettant en lumière l'état de « distraction » des utilisateurs du jeu ont abondé dans les pages « faits divers » des médias cet été. En témoigne ce conducteur de New York qui a fini sa course en voiture dans un arbre, alors qu'il jouait au volant : les risques associés sont ici en réalité les mêmes que ceux de toute expérience immersive, que ce soit un SMS, un appel, etc. L'Armée indonésienne a d'ailleurs banni le jeu en invoquant un risque d'addiction pour ses soldats.

Outre ces risques individuels, le fait que de telles applications soient utilisées par un grand nombre de joueurs augmente le risque d'engorgement des voies : cela peut se traduire par un embouteillage, en raison de piétons traversant aléatoirement les routes, comme ce fut le cas à Central Park cet été, où a eu lieu un **regroupement de foule en un éclair**, ou « flash mob » en anglais, ce qui pose de sérieux risques en matière d'ordre public au vu du caractère spontané et imprévisible de la manifestation, à des points

sensibles des villes (les « Pokémons » apparaissent plus souvent en centre-ville ou près de monuments marquants qu'en rase campagne). Il est par conséquent tout à fait possible d'imaginer qu'un rassemblement spontané en lien avec ce type de jeux ait lieu à proximité de sites sensibles notamment ceux situés en ville près d'axes de transports majeurs. Le risque est avant tout d'ordre logistique, physique.

Source Sud Ouest

Face à la gronde rapidement apparue au niveau international, Niantic Labs a préféré jouer le jeu de la coopération, proposant aux joueurs ou autres riverains de contacter ses services pour demander la suppression d'un « Pokéstop » ou d'une « Arène », deux espaces virtuels du jeu correspondant à un emplacement géographique réel (et souvent associés à des lieux publics particulièrement fréquentés). Dans la banlieue de Sydney, en Australie, le conseil municipal de Canada Bay a réclamé à Niantic la suppression de deux des trois « Pokéstops » d'un parc local en invoquant la nécessité de rétablir l'ordre public : « Nous avons récemment rencontré de nombreuses anomalies par rapport à la normale, notamment en lien avec le trafic : un camion de pompiers a ainsi été retardé dans son intervention suite à un feu d'appartement en raison d'embouteillages causés par le jeu et les joueurs ». La municipalité a fait appel à ses habitants pour appuyer sa décision en les invitant à soumettre la même pétition à Niantic, ce qui souligne l'asymétrie qui peut exister dans les relations entre Niantic et certains acteurs, dont des collectivités locales de villes de petite et moyenne taille, de petites entreprises, etc.



Source : Niantic Labs

… au risque pour la sécurité nationale

La multiplication des exemples de risques physiques concrets a très certainement conduit les états-majors de plusieurs Etats à bannir tout ou partie de jeux en réalité augmentée. **Dès 2014 par exemple, l'Etat du Colorado aux Etats-Unis a interdit le jeu Ingress**[5] « et apparentés » d'une base aérienne, craignant que de tels jeux puissent être utilisés comme **couverture dans l'espionnage de ses sites militaires**. Une partie du jeu consiste en effet à « capturer » de manière virtuelle (à partir de son Smartphone géolocalisé) un ou plusieurs « objets » ou « monuments » du monde réel qui font l'objet de photographies partagées au sein du jeu. Si l'on ajoute à cela que les données de géolocalisation associées à ces photos sont également partagées avec d'autres joueurs anonymes (ainsi que l'éditeur Niantic, filiale de Google…), on comprend bien vite pourquoi les Forces Armées américaines ont très tôt décidé de bannir l'utilisation de ce type de jeux, quand bien même aucun exemple de détournement du jeu à des fins d'espionnage n'existe à notre connaissance. Devant le succès planétaire de « Pokémon Go », les forces de défense d'autres pays parmi lesquels la Malaisie, l'Indonésie et Israël ont suivi les pas précoces de l'armée américaine.

En Israël, précisons que les Forces Armées mènent un combat de manière plus globale contre **l'utilisation des applications et des réseaux sociaux qui entraînent la publication de photos sur le web**. Ainsi, des soldats ont déjà été punis pour avoir réalisé **un « check-in » depuis leurs bases sur Facebook**, partageant ainsi avec d'autres utilisateurs l'emplacement géographique de sites sensibles.

Avec « Pokémon Go » néanmoins, le simple bannissement du jeu ou la sanction d'utilisateurs ne suffisent pas : **Niantic génère l'apparition chronométrée de ses « monstres de poche » à partir d'un algorithme secret** qui les place aussi bien dans la rue du domicile du joueur que dans la résidence (privée) de son voisin. Cela génère des risques d'ordre stratégique voire vital lorsque des « Pokémons » surgissent dans l'enceinte d'OIV, de groupes industriels ou de bases militaires, attirant les joueurs de passage connectés. Si

[5] Ingress peut être présenté comme le prédécesseur de Pokémon Go, édité comme ce dernier par la compagnie Niantic Labs. Basé sur le même principe mais avec un contexte de jeu et un univers différents, il cible bien moins le « grand public » que son cadet.

Niantic ne propose pas aux joueurs de soumettre une requête en ligne pour suspendre la génération de ces monstres, l'éditeur semble avoir été contraint de filtrer certaines zones sensibles, dont les bases militaires américaines : dans un fil de discussion Reddit ouvert fin août par des officiers de l'armée américaine, plusieurs joueurs se plaignent de « ne plus rien voir apparaître une fois franchis les accès de la base ». Un utilisateur précise en revanche que des outils existent dans le jeu, des « encens », pour faire apparaître les « Pokémons ». De toute évidence, Niantic semble opérer au cas par cas et se soumettre uniquement aux demandes émanant d'organismes opérant des sites critiques. **L'opacité de l'éditeur**, de même que celle de son directeur John Hanke[6], ayant été soulignée de manière répétée dans la presse, il semble que le meilleur moyen de sécuriser ses actifs critiques (telles que la localisation de zones militaires secrètes) reste d'établir un **canal de communication direct**, non seulement avec Niantic mais d'autres sociétés vidéoludiques telles que Rovio, Machine Zone ou King. Ces dernières ont tout à perdre d'une exposition négative dans la presse, alors qu'elles évoluent sur un marché extrêmement concurrentiel.

Des risques associés à la protection de la vie privée

Parmi les « inputs » qui peuvent « augmenter » le monde qui nous entoure, les données privées, notamment de géolocalisation, figurent en première ligne. De nombreuses applications, ludiques ou non, se fondent sur ces dernières pour **enrichir la palette de services offerte par les terminaux mobiles**. C'est notamment le cas des applications de santé connectée visant à mesurer le nombre de kilomètres parcourus dans le courant de la journée par une personne. Reliées à un engagement dans un contrat d'assurance-vie, ces applications peuvent encourager l'utilisateur à faire davantage d'exercice en vue de réduire sa prime d'assurance. Mais ces applications ne sont pas que source d'opportunités.

Avec « Pokémon Go », les effets positifs, à savoir un divertissement ludique associé à une activité physique, semblent peser bien peu dans la balance face aux risques liés notamment aux **faibles garde-fous mis en place par les éditeurs**. Ainsi, lors du lancement du jeu, des dizaines de millions de personnes ont accepté de partager avec l'ensemble du réseau des données à caractère privé, dont certaines n'étaient pas du tout en lien avec l'objet de l'application. Par exemple, les joueurs ont consenti à Niantic un accès à leur compte de facturation Google Play. Si cette anomalie a par la suite été corrigée, elle témoigne bien de l'absence de « sécurité dès la conception » (ou « security by design » en anglais) chez ces développeurs. Ces derniers bénéficient également d'une méconnaissance des risques par le grand public. Une enquête réalisée par IDT911 a conclu que **la plupart de ces risques sont acceptés par les joueurs**, l'âge étant un facteur-clé pour comprendre cette acceptation du risque : en gros, les populations plus âgées seraient plus prudentes. Plus d'un tiers des 18-24 ans interrogés dans le cadre de cette enquête ne voyaient aucun inconvénient à ce qu'une application mobile ait accès aux données privées stockées sur leur Smartphone.[7]

Certains experts en sécurité se montrent pourtant très critiques à l'égard d'une solution qui est qualifiée de « **bracelet GPS virtuel** » par Andrew Brandt, expert Blue Coat (Symantec). Au-delà du fait que des agences de renseignement pourraient récupérer ces données, ce dernier a récemment souligné le **risque de**

[6] Avant de prendre la direction de Niantic, John Hanke a dirigé le département Geo de Google, chargé d'une grande partie des projets liés à la localisation. Fondateur de Keyhole, société d'imagerie satellitaire qui a bénéficié du soutien financier de la CIA, il était entré chez Google en 2004 après le rachat de sa société, rebaptisée Google Earth en 2005.

[7] Thirdcertainty.com.

« bullying » ou harcèlement moral et physique des joueurs par d'autres utilisateurs. Selon lui, le spoofing des données GPS sur les appareils mobiles[8], principale faille de « Pokémon Go », a entraîné un « jeu du chat et de la souris » entre Niantic et les tricheurs, le bannissement étant aisément contournable par des utilisateurs connaisseurs des nouvelles technologies, et un **déséquilibre entre ces derniers et les joueurs « intègres ».** De nombreuses menaces sur la sécurité physique des joueurs, soupçonnés de triche en particulier, auraient été proférées sur le web par des joueurs-hackers ayant mis la main sur des données telles que les « habitudes de promenade », conduisant certains utilisateurs du jeu à supprimer leur compte par peur de représailles physiques.

Ce problème technique du GPS-spoofing n'est cependant pas du ressort des éditeurs : il n'existerait à ce jour **aucun moyen pour une application mobile d'authentifier que les données GPS fournies par le système d'exploitation sont légitimes**. Face à cette situation, Niantic a vu se développer un « marché noir » de comptes frauduleusement farmés[9] qui viole les CGU du jeu, augmentant par là-même le ressentiment de joueurs s'estimant lésés, la progression dans le jeu d'un niveau à un autre étant particulièrement chronophage.

Signalons également les risques liés à la mise à disposition du jeu à des dates espacées : lancée avec retard sur le calendrier initial en France, à la suite de l'attentat de Nice, les joueurs se sont **exposés à des escroqueries**, n'acceptant pas d'attendre patiemment la sortie officielle du jeu. Une version « Pokémon Go » altérée et infectée avec un outil d'accès à distance, DroidJack, a ainsi été détectée sur des plateformes de stockage en ligne, hors Google Play Store. Une fois téléchargé, le malware permettait aux escrocs d'accéder aux informations personnelles du joueur. Les applis « tutoriels » seraient aussi touchées : ce sont souvent des fichiers APK (pour Android) qui modifient les paramètres de sécurité du Smartphone, les rendant plus vulnérables aux malwares.

Vers des applications ludiques dans le monde réel ?

Face au succès, même éphémère, de « Pokémon Go », le risque est grand que des développeurs souhaitent répliquer son succès, sans consentir les investissements nécessaires en matière de sécurité. Il semble urgent que les éditeurs de ce type d'applications ludiques mettent en place un niveau de sécurité et de confidentialité suffisants dès le développement des jeux.

Si les risques sont bien réels, certaines organisations, notamment les chaînes d'établissements de commerce au détail, voient déjà d'un bon œil leurs échoppes se transformer en lieux de rencontre pour les joueurs. Au-delà de l'aspect purement mercantile, les organisations du secteur de la défense pourraient utiliser ce type de jeux à des fins de divertissement associant le jeu à une pratique sportive : « Pokémon Go » n'est rien de plus qu'une « course au fanion planétaire ».

Enfin, pour donner une vision plus cynique, voire « retourner » le paradigme développé dans cet article, l'apparition d'outils d'analyse des données issues de ces applications de jeux en réalité augmentée pourrait

[8] La transmission de faux signaux GPS permet de contourner le principal obstacle au développement du compte joueur, à savoir une marche à pied « dans le monde réel » pour rechercher des Pokémons à capturer.

[9] Dans un jeu vidéo, le farming est une pratique qui consiste à récolter des « tokens » (que ces derniers soient des objets ou monnaies virtuelles ou de l'expérience) de manière répétée afin de monter rapidement d'un niveau à l'autre.

permettre de mieux détecter des agissements malveillants, dans des sociétés où les frontières entre le réel et le virtuel tendent à être de plus en plus brouillées. Pour les organisations qui les contrôlent, ces jeux constituent même un excellent outil de renseignement, voire de manipulation des individus.

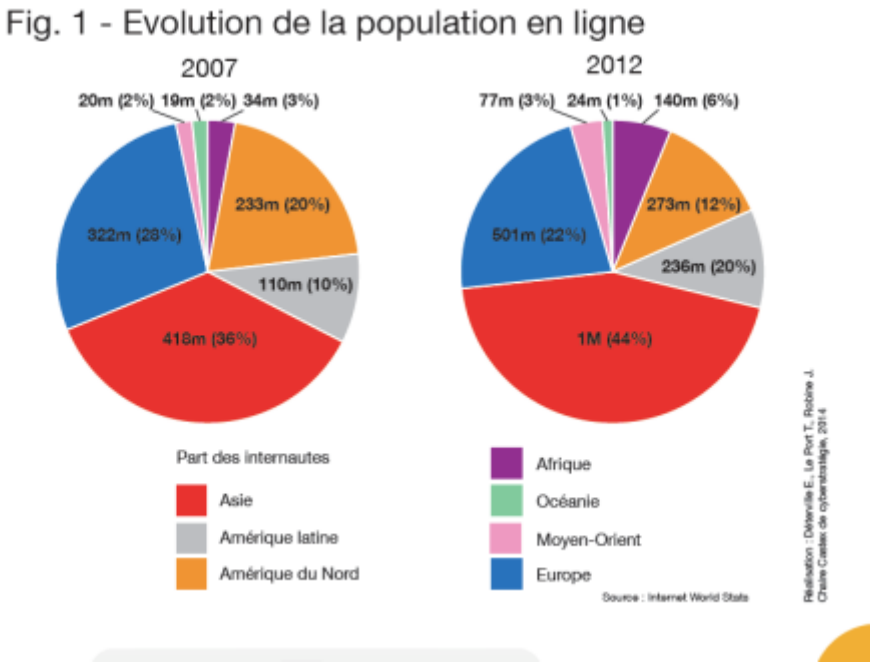
LE MARCHE DE LA CYBERSECURITE EN AUSTRALIE ET ASIE PACIFIQUE

Le secteur des nouvelles technologies de l'information et de la communication (NTIC) a connu au cours de ces dix dernières années une très forte croissante dans la zone Asie Pacifique. Pour beaucoup des pays de la région, l'innovation technologique a en effet constitué un véritable levier du développement économique, et le secteur des télécoms en particulier s'est imposé comme l'un de ses moteurs essentiels. Inévitablement, l'ouverture à ces nouvelles technologies de l'information et une pénétration croissante d'Internet dans ces économies les ont aussi rendues plus vulnérables, comme en témoignent la croissance exponentielle des cyber-attaques contre les infrastructures gouvernementales et les grands acteurs industriels de la région. Conscients des enjeux et des risques encourus, les Etats ont alors mis en place des politiques nationales de cybersécurité. Certains y ont aussi vu une opportunité de structurer une offre nationale de produits et de services de cybersécurité. L'Australie, la Malaisie et Singapour, qui figurent parmi les cinq états les plus « cyber matures » de la région selon le classement de l'Australian Strategic Policy Institute (ASPI), présentent des profils particulièrement intéressants.

Les TIC en Asie Pacifique : un développement rapide et diversifié

En même temps que son développement économique, l'Asie Pacifique a aussi rattrapé son retard en matière de technologies de l'information, un secteur qui présente une croissance forte et un développement rapide dans tous les secteurs industriels. L'Internet a connu un essor fulgurant dans la région au cours des dix dernières années, étant passé de 418 millions d'internautes en 2007 à plus d'un milliard en 2016, soit une augmentation de près de 150%.[10]

[10] « Géopolitique du Cyber en Asie », Asia Centre, septembre 2014



Source : Internet World Stats

Selon une étude Gartner[11] les pays de la région et notamment Singapour, la Malaisie, l'Indonésie et la Thaïlande, sont parmi les pays où l'investissement dans les technologies de l'information est le plus important. Onze pays de la région, dont les quatre cités plus haut, représentent également à eux seuls 80% des dépenses en technologies de l'information de la région avec une croissance de 6% jusqu'en 2015, année où les dépenses ont atteint 52 milliards de dollars. L'adoption pour ainsi dire généralisée d'applications web et surtout mobiles est sans doute la manifestation la plus notable de cette évolution. Une étude GfK du mois de décembre 2014[12] précise par exemple que la vente de téléphones mobiles en Asie Pacifique a augmenté de 61% au cours des 9 premiers mois de 2013 pour un total de 10,8 milliards de dollars pour Singapour, la Malaisie, la Thaïlande, l'Indonésie, le Vietnam, le Cambodge et les Philippines seulement. De même, la fréquentation des réseaux sociaux connaît une croissance exponentielle dans les pays de la région, non pas tellement via les lignes fixes que par les appareils mobiles, désormais principaux points d'accès à Internet. En termes de services, les possibilités offertes par le Big Data et le Cloud Computing constituent des moteurs essentiels dans des secteurs comme la banque, la santé, les télécoms ou la distribution. Il est fort probable que cette tendance à la croissance des technologies liées à Internet se poursuive, au moins à moyen terme. Pour ces pays, la poursuite des objectifs politiques, économiques et militaires est en effet étroitement liée au développement des connexions et à l'offre de services Internet essentiels.

[11] https://www.gartner.com/newsroom/id/3012117

[12] https://www.michaelbaileyassociates.com/news/it-and-ict-technology/the-changing-shape-of-se-asia-s-it-industry

Des Etats plus vulnérables et des cyberattaques en hausse

Conséquence de ce développement et de la pénétration d'Internet dans ces économies et industries qui reposent de plus en plus sur la technologie et un haut niveau de modernisation, les Etats et industries de la région sont aussi plus exposés et plus vulnérables aux cybermenaces.

La fréquence des cyberattaques enregistrées dans la région ne cesse ainsi de croître à un rythme soutenu. Un rapport FireEye estime par exemple que le nombre d'incidents de cybersécurité enregistrés dans les entreprises asiatiques aurait progressé de 17% entre 2012 et 2013, passant de 2444 à 2958.[13] L'impact financier de ces attaques n'est pas négligeable puisque selon une étude Grant Thorton elles auraient coûté 81 milliards de dollars américains aux entreprises d'Asie Pacifique entre septembre 2014 et septembre 2015, soit plus qu'à l'Europe et aux Etats-Unis réunis.[14] Outre le critère quantitatif, on remarque aussi que les incidents enregistrés deviennent de plus en plus graves à mesure que le volume des données potentiellement exposées augmente et que les attaques sont de plus en plus ciblées et sophistiquées, avec des modes opératoires de plus en plus variés.[15]

En Australie par exemple, le Centre de Cybersécurité Australien, estime que près de 2000 attaques ont ciblé les systèmes gouvernementaux entre le 1er janvier et le 30 juin 2016. Les attaques les plus impressionnantes ont pris pour cible le Bureau de Météorologie et le Bureau des Statistiques, où l'introduction de malwares a permis le vol de documents confidentiels. Si les autorités estiment le coût annuel direct des cyber-attaques à 1 milliard de dollars australiens, certaines estimations chiffrent leur coût réel à 1% du PIB, soit 17 milliards de dollars.[16] De même selon le Defence Outlook 2016[17], Singapour, avec son indicateur de vulnérabilité de 399 en 2014 contre 224 en 2008 fait même partie des Cyber Five, le top cinq des pays asiatiques les plus vulnérables, aux côtés de la Corée du Sud, l'Australie, la Nouvelle Zélande et le Japon. Les attaques qui ont visé le géant des télécoms M1 et la société de divertissement K Box Entertainment Group en 2014 illustrent bien cette situation. Dans les deux cas, elles mettaient en jeu les données personnelles de clients et utilisateurs, qui ont été manipulées ou divulguées.

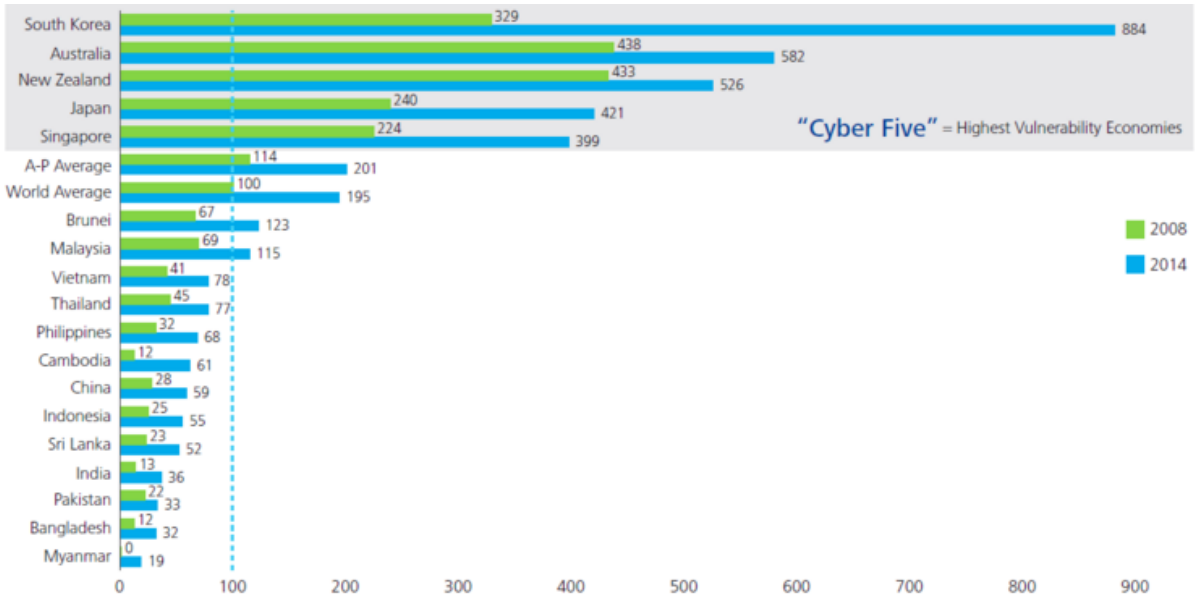
[13] « Géopolitique du Cyber en Asie », Asia Centre, septembre 2014

[14] http://www.hktdc.com/info/ms/a/fr/1X04CSJ5/1/French/Asie-Vers-Une-Cyberd%C3%A9fense-Renforc%C3%A9e.htm

[15] Targeted attacks in 2013 : Asia Pacific, Geok Meng Ong, Kenneth Geers, 2014 FireEye Blog

[16] http://www.bbc.com/news/technology-37163076

[17] http://www.channelnewsasia.com/news/singapore/singapore-one-of-5/2541456.html



Source : Asia-Pacific Defense Outlook 2016, Deloitte

Si la situation de la Malaisie semble moins impressionnante, le CERT national a cependant comptabilisé non moins de 9915 rapports d'incidents en 2016, soit une augmentation de 100% par rapport à 2007.[18] Selon son CEO les menaces concernent 65% des organisations publiques ou privées, les cibles les plus vulnérables restant dans l'ordre, les gouvernements, le secteur des télécommunications, et le secteur financier.[19]

Un constat qui peut être élargi à l'ensemble de la région et qui est partagé par FireEye dans son étude de mars 2015[20]. Celle-ci note que les attaques prennent de plus en plus la forme d'APT sophistiquées et cite parmi les secteurs les plus exposés dans la région les secteurs financiers et bancaires, mais aussi ceux de l'énergie, des télécoms et des transports. Ces attaques auraient des motivations financières ou viseraient le vol d'informations à des fins commerciales ou politiques, l'espionnage et la criminalité constituant les principaux facteurs d'instabilité dans le cyberespace régional. Les enjeux économiques liés au développement et à la prospérité des pays asiatiques représentent en effet un attrait non négligeable pour les criminels, et les tensions et disputes territoriales que connaît la région font du cyberespace un nouveau théâtre d'affrontements ou s'exprime les rivalités politiques et économiques.[21] Sans compter les acteurs privés et hacktivistes qui constituent une menace et un facteur d'instabilité sur lesquels les gouvernements de la région n'ont que peu de prise. [22]

[18] http://www.cybersecurity.my/en/media_centre/media_faqs/media_faqs/main/detail/1691/index.html

[19] http://www.ukm.my/news/Latest_News/malaysia-has-high-vurnerability-to-cyber-attacks-says-cyber-security-experts/

[20] https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Fireeye_rpt-southeast-asia-threat-landscape.pdf

[21] « Géopolitique du Cyber en Asie », Asia Centre, septembre 2014

[22] idem

Si les chiffres fournis par autorités nationales régionales ne sont pas suffisamment fiables pour identifier avec certitude les pays d'origine de ces attaques - et ce d'autant que les attaques originaires d'un pays peuvent transiter par les serveurs d'autres pays – toutes les études placent les Etats-Unis et la Chine en tête des actes de malveillance dans le cyberespace.

Or les pays ciblés sont d'autant plus vulnérables qu'ils sont insuffisamment équipés pour lutter contre des attaques plus fréquentes et plus sophistiquées, à la fois parce qu'ils ne possèdent pas pour la plupart de plans de réponse adaptés, d'outils de Threat Intelligence et d'expertise spécialisée, mais aussi en raison d'un déficit de ressources humaines et de formations adéquates, et de dispositifs de protection des données insu, de politiques d'évaluation du risque et de sensibilisation/formation des personnels insuffisants. Sans compter l'utilisation croissante de nouveaux outils et de nouveaux usages comme le BYOD ou le cloud, qui constituent un réel facteur d'instabilité et risquent d'accroître encore la vulnérabilité de ces Etats.

Le double constat d'une croissance forte et rapide des cyber-attaques et des risques qui en résultent d'une part, et de l'insuffisante protection des pays asiatiques de l'autre, a favorisé la prise de conscience des autorités nationales. Celle-ci s'est traduit, dans les années 2000, par la mise en place de politiques de cybersécurité et de structures dédiées chargées de leur mise en œuvre.

La mise en place de politiques de cybersécurité et de structures dédiées

Une étude réalisée par l'Australian Strategic Policy évalue la cyber maturité des pays asiatiques en prenant en compte une dizaine de critères intégrant à la fois l'existence d'infrastructures dédiées, les capacités militaires, le degré de sensibilisation et de compréhension des enjeux par les doctrines nationales, ou encore le niveau de développement des économies numériques et leur gouvernance. Les résultats de cette étude distinguent 4 géants : l'Australie, la Corée du Sud, le Japon et Singapour, suivis de près par la Malaisie. L'Australie, Singapour et la Malaisie présentent les profils les plus intéressants.

	Country	Weighted score
1	United States	90.7
2	Japan	85.1
3	South Korea	82.8
4	Singapore	81.8
5	Australia	79.9
6	New Zealand	72.8
7	Malaysia	68.3
8	China	64.0
9	Vietnam	53.6
10	Brunei	51.6
11	India	50.0
12	Thailand	49.1
13	Philippines	46.8
14	Indonesia	46.4
15	Fiji	30.7
16	Myanmar	26.9
17	Laos	23.3
18	Cambodia	20.7
19	Papua New Guinea	20.3
20	North Korea	16.4

Source : Australien Strategic Policy Institute [23]

Bien qu'issue d'une démarche volontariste, l'élaboration de politiques de cybersécurité dans les trois pays étudiés a pourtant été progressive, parfois lente, et les structures mises en place pour les soutenir ont parfois connu plusieurs évolutions successives avant d'atteindre leur forme actuelle – qui n'est sans doute pas définitive. Si toutes les politiques nationales s'appuient sur des stratégies de cybersécurité élaborées par les gouvernements concernés, elles se différencient non pas tellement par leur contenu que par la façon dont elles sont intégrées aux structures gouvernementales nationales et par les institutions qui ont la responsabilité de leur mise-en-œuvre.

Les politiques de cybersécurité dans les trois pays étudiés poursuivent dans les grandes lignes les mêmes objectifs : avancer et protéger les intérêts nationaux « en ligne », en travaillant au développement d'un environnement numérique et d'un cyberespace sûr et protégé et en favorisant l'émergence d'un écosystème national capable de soutenir leur développement économique. En Australie, les grandes orientations de la politique de cybersécurité ont d'abord été données par la *Cyber Strategy Policy* de 2009, complétée et précisée par la *Cyber Security Review* lancée en 2014 et par le Livre Blanc de la Défense de février 2016. De même, Singapour a publié le 10 octobre 2016 une stratégie nationale de cybersécurité qui repose sur

[23] Cyber maturity in the Asia–Pacific region 2015, Australien Strategic Policy Institute

quatre objectifs : renforcer la résilience des infrastructures stratégiques ; mobiliser l'industrie et les utilisateurs pour rendre le cyberespace plus sûr en luttant contre les cybermenaces et la cybercriminalité et en protégeant les données personnelles ; développer un écosystème de cybersécurité et une main d'œuvre qualifiée pour soutenir le développement économique national; et multiplier les partenariats internationaux pour lutter contre des menaces qui ne connaissent pas de frontières. La National Cyber Security Policy malaisienne lancée dès les années 2000 doit elle aussi permettre de garantir la sûreté, la résilience et l'autosuffisance en matière de systèmes d'informations, et est destinée à promouvoir la stabilité, le bien-être social et la création de richesses.

Des structures dédiées ont rapidement vu le jour à côté des institutions nationales pour mettre en œuvre ces politiques et ces stratégies. Intégrées aux organes gouvernementaux à très haut niveau mais de façons très différentes, elles se distinguent également par leur champ d'action et leurs compétence respectives. Ainsi l'Australie s'est dotée dès 2009 d'un Cyber Security Operations Centre (CSOC) opérant au sein de l'Australian Signals Directorate et chargé de centraliser les capacités opérationnelles des principaux acteurs publics concernés par les questions de cybersécurité. Le CSOC est devenu l'Australian Cyber Security Centre (ACSC) en 2014. En 2010, l'Australie a également mis en place son CERT national, « CERT Australia ». A côté de ces nouvelles structures, le ministère de la Défense australien joue un rôle clé dans la mise en œuvre de la politique de cybersécurité nationale. Il a développé dès 2009 des capacités adéquates, d'abord via une vaste réforme de rationalisation des systèmes d'information lui permettant d'intégrer ces nouvelles contraintes, ensuite via une série de programmes lui permettant de développer des solutions en interne en collaboration avec la Defence Science and Technology Organisation, chargée des sciences et technologies au sein du Ministère de la Défense. Au sein des forces armées, la Royal Australian Navy est aujourd'hui l'organisation qui semble prendre le mieux en compte la cybersécurité dans la conduite de ses opérations, notamment avec l'utilisation de systèmes de surveillance et de gestion reposant sur des solutions d'IBM.

En Malaisie au contraire, le ministère de la Défense est pour ainsi dire absent de la formulation et de la politique de cybersécurité nationale, la « National Cyber Security Policy », amorcée depuis les années 2000. Celle-ci est mise en œuvre le Conseil National de Sécurité (CNS) auquel participent à la fois le Ministère des Sciences, de la Technologie et de l'Innovation, le Ministère de l'Information, des Communications et de la Culture, et la Malaysian Administrative Modernisation and Management Planning Unit, en collaboration avec le Bureau du Procureur Général et le Bureau du Premier ministre. Un système particulièrement éclaté et coordonnée plutôt que centralisé par le CNS.[24] Le ministère de la Défense dispose également d'une politique de sécurité des systèmes d'information distincte, qui s'applique à l'ensemble du ministère et à ses fournisseurs.

Singapour présente un modèle encore différent, dans lequel les capacités de cybersécurité sont centralisées par la Cyber Security Authority[25] créée en 2015, rendant compte directement au Bureau du Premier Ministre

[24] NITC Malaisia : http://nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp

[25] Cyber Security Authority : https://www.csa.gov.sg/

et placée sous l'autorité du Ministère des Communications et de l'Information, du Ministères des Affaires Intérieures, de la Défense, des Finances, de la Recherche, de l'Agence pour les Sciences, la Technologie et la Recherche (A*STAR). Toutes ces structures sont membres du National Infocomm Security Committee (NISC), chargé de la definition du "*National Cyber Security Masterplan 2018*" qui s'échelonne sur 5 ans (2013 à 2018). Au sein de cette architecture, le Ministère de la Défense participe donc à la définition de la stratégie nationale à travers le NISC, et conduit des travaux de R&D dans ce domaine via la Defence Science Organisation et la DSTA Defence Science and Technology Agency. D'autre part, le Vice-secrétaire du ministère de la Défense en charge des technologies occupe également la fonction de directeur du CSA, une mesure qui donne au ministère de la Défense un poids et une influence non négligeables en matière de définition et de mise en œuvre de la politique de cybersécurité.

Pour mettre en œuvre leurs politiques nationales de cybersécurité, les trois pays étudiés s'appuient également sur les partenaires industriels locaux et étrangers qui contribuent à l'émergence d'un écosystème de cybersécurité.

L'émergence d'un écosystème de cybersécurité.

L'investissement dans les capacités de cybersécurité est non seulement un enjeu des compétitions économiques et commerciales régionales, mais aussi un enjeu de souveraineté car tous les pays cherchent à mieux contrôler l'environnement stratégique de leurs entreprises, et donc le leur en tant qu'Etat souverain. Ainsi dans les trois pays étudiés, le secteur de la cybersécurité comporte à la fois des acteurs locaux et mondiaux.

Si on compte encore peu d'acteurs locaux dans le domaine des systèmes d'information et de la cybersécurité australien, le gouvernement a mis en place début 2016 un « Cyber Security Growth Center » qui devrait être opérationnel d'ici la fin de l'année. Son objectif est de faire de l'Australie un leader en matière de cybersécurité en favorisant l'innovation, en encourageant les co-production public-privé, et en facilitant l'investissement étranger, le tout grâce à un budget de 30 millions de dollars australien d'ici 2019-2020. Les seuls acteurs nationaux de poids à ce jour sont CEA Technologies pour les communications navales, Aurecon, et Nuix. Le Ministère de la Défense a donc surtout recours à de grands groupes étrangers très bien implantés et notamment Selex ES Australia, Thales Australia, L-3 Communications, Lockheed Martin, Cisco Australia ou encore Northrop Grumman Australia. Le CIOG a par ailleurs sélectionné 5 « partenaires industriels privilégiés » que sont Accenture Australia, CSC Australia, IBM Australia, HP Australia, BAE Systems Australia. Ces acteurs étrangers disposent d'une forte implantation locale à travers la création de filiales, la mise en place de partenariats avec des acteurs publics ou encore le rachat de sociétés locales.

De même, la Malaisie fait état de capacités locales limitées mais vouées à se développer. On note d'abord une forte présence d'acteurs internationaux du secteur des technologies de l'information comme IBM, Cisco (via notamment e-Cop), Symantec et Deloitte. Dans le secteur de la défense, BAE Systems Applied Intelligence dispose d'un véritable ancrage local via la signature d'un protocole d'entente avec Cybersecurity Malaisia, ou le financement d'un programme postuniversitaire sur la cybersécurité à l'Université de Défense Nationale de Malaisie (UPNM). A côté de ces grands acteurs internationaux, il existe aussi des acteurs locaux spécialisés comme E-Spin, Heitech Padu ou AIMS Data Centre, dont les compétences et le nombre devraient croître en raison du dynamisme du marché.

Singapour présente une offre industrielle particulièrement dense qui s'appuie sur un écosystème très développé, porté notamment par un secteur des technologies de l'information très dynamique. ST Engineering, principal acteur local, combine à la fois des compétences dans la construction navale et dans la cybersécurité avec l'activité Infosecurity de sa branche ST Electronics. Le 18 mai 2016, le géant des telecoms de Singapour StarHub a annoncé la création de son Cyber Security Centre of Excellence (COE), dont l'objectif est le renforcement des capacités nationales en matière de cybersécurité à travers l' innovation et le développement de partenariats industriels. A ce jour quatre partenaires industriels, Blue Coat, Cyberbit, Fortinet et Wedge Networks, et quatre partenaires académiques, Nanyang Polytechnic (NYP), Republic Polytechnic, Temasek Polytechnic et Singapore University of Technology and Design, ont rejoint le COE. A cette occasion, StarHub a également annoncé son intention de désigner EY comme son fournisseur de conseils privilégié. On note toutefois également la présence de nombreuses entreprises étrangères dans le pays, à la fois des acteurs des technologies de l'information comme IBM, Microsoft ou Sopra Steria, de la Défense tel qu'Airbus, Rhode & Schwartz, BAE Systems, et Boeing. Les entreprises israéliennes comme IAI, Elbit Systems et Check Point sont particulièrement bien représentées.

Le renforcement des capacités et la structuration d'offres nationales sont donc un véritable enjeu à la fois politique, économique et commercial, pour ces trois pays. Cette démarche requiert un investissement financier et humain que les tous les états ne sont pas en mesure de fournir de façon continue, ce qui explique les disparités entre ces trois pays que l'on peut qualifier de « cyber matures » et d'autres moins avancés dans la région.

L'exemple de l'Asie Pacifique, et en particulier de trois pays déjà bien avancés en matière de cyber sécurité, montre bien que dans ce domaine plus que dans d'autres secteurs les aspects politiques, technologiques, économiques et commerciaux sont étroitement liés. L'impératif de protection et de lutte contre les cyber-attaques est indissociables des stratégies de promotion et de développement du secteur des TIC et de l'économie numérique : ces deux logiques se soutiennent mutuellement et prennent appui l'une sur l'autre. De même, du côté des attaques, criminalité, espionnage industriel ou politique et hostilités interétatique sont autant de manifestations d'une situation régionale marquée par l'augmentation des tensions, et l'expression de rivalités de natures variées.

La **Direction Générale des Relations Internationales et de la Stratégie (DGRIS)** propose les analyses politiques et stratégiques contribuant à renforcer l'appréciation des situations et l'anticipation. Elle soutient la réflexion stratégique indépendante, en particulier celle menée par les instituts de recherche et organismes académiques français et étrangers. Elle contribue au maintien d'une expertise extérieure de qualité sur les questions internationales et de défense.

A ce titre, la **DGRIS** a confié à **CEIS** la réalisation de cet **Observatoire du Monde Cybernétique**, sous le numéro de marché 1502492543. Les opinions développées dans cette étude n'engagent que leur auteur et ne reflètent pas nécessairement la position du Ministère de la Défense.

Ministère de la Défense et des Anciens combattants
Direction Générale des Relations Internationales et de la Stratégie
14 rue Saint-Dominique - 75700 – Paris SP 07

CEIS
280 Boulevard Saint-Germain - 75007 - Paris
Téléphone : 01 45 55 00 20
E-mail : omc@ceis-strat.com