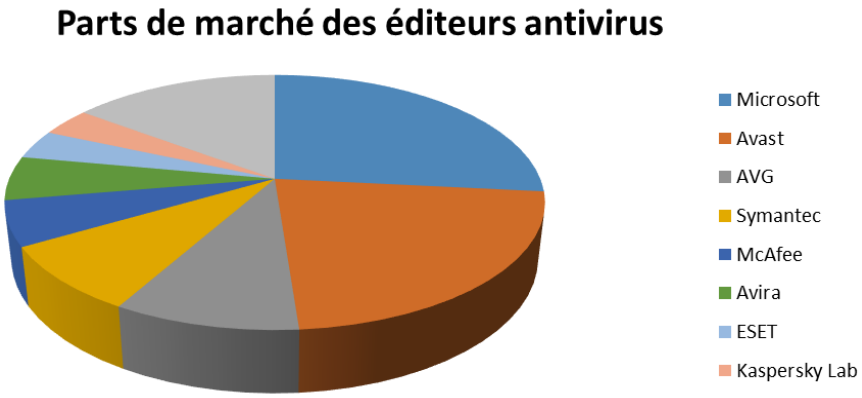
Lettre n°37 – avril 2015 – disponible sur omc.ceis.eu

Brève du mois

"*Adversaries should know that our preference for deterrence and our defensive posture don't diminish our willingness to use cyber options if necessary. (...) And when we do take action – defensive or otherwise, conventionally or in cyberspace – we operate under rules of engagement that comply with domestic and international law.*" **Ashton B.Carton, Secrétaire de la Défense américaine, le 24 Avril 2015, à l'Université de Stanford.**

LE ROLE STRATEGIQUE DES EDITEURS D'ANTIVIRUS



Source: OPSWAT, "Antivirus and Operating System Report", octobre 2014.

Acteurs majeurs et historiques du monde de la sécurité informatique, les éditeurs de logiciels antivirus prennent part à un marché dynamique devant réagir au plus vite pour détecter les menaces. L'implémentation de solutions antivirus apparaît rapidement comme l'une des premières étapes nécessaires pour la stratégie de protection du système d'information d'une entreprise ou d'une administration. Aujourd'hui, les éditeurs de programmes antivirus se comptent par dizaines. Pourtant, seuls quelques-uns coiffent un podium hautement concurrentiel et sans cesse bouleversé par l'arrivée de nouveaux acteurs.

Plus un antivirus dispose d'un parc important de machines sur lequel il est installé, plus il met en place une forme de souveraineté sur un ensemble d'appareils donné. Un récent rapport d'OPSWAT, s'intéressant à l'utilisation de chaque fournisseur de logiciels antivirus au niveau mondial sur les machines OPSWAT GEARS, nous renseigne un peu plus sur le marché de ces sociétés[1]. Trois d'entre elles occupent actuellement le podium en termes de parts de marché. Microsoft se hisse à la première marche avec 26,6% de parts de marché dont 62,9% se fait grâce à Microsoft Security Essential et 31,4% par Windows Defender. À la deuxième place, nous retrouvons AVAST qui en conquiert 22,2%. Quant à la troisième place, elle est occupée par AVG avec 9,4%. Suivent ensuite Symantec (8,4%), McAfee (5,7%), Avira (5,6%), ESET (3,7%) et Kaspersky Lab (3,6%). Un marché changeant puisqu'en 2010, OPSWAT publiait un rapport affichant un tout autre classement avec Avast en tête (19,14%), puis Avira (11,39%) et enfin Symantec (10,6%)[2]. Les résultats obtenus par OPSWAT démontrent également l'importance des solutions gratuites dans l'industrie de la sécurité informatique. Or, selon une étude d'AV-Comparative, ces solutions ne seraient pas les plus sûres[3]. Le spectre des vulnérabilités et des menaces traitées est en effet souvent moins large que pour des solutions payantes qui proposent des offres plus complètes incluant la protection des achats en ligne et de l'identité numérique. En revanche, si l'on considère les chiffres d'affaires générés dans ce marché de la sécurité informatique, on constate que les éditeurs commercialisant des versions payantes de leurs programmes se placent en tête du classement[4]. Ainsi selon un rapport d'IDC datant de 2010, Symantec devance de loin ses concurrents dans la vente de ces solutions aux consommateurs avec 45,6% des profits produits. L'entreprise américaine est suivie par McAfee (18%), Trend Micro (8,4%), Kaspersky Lab (6,7%), AVG (3,6%) et BitDefender (3,1%), etc.

Nombre de firmes coexistent donc dans ce secteur, secteur essentiel pour les gouvernements et les activités stratégiques. Alors que les menaces informatiques sont de plus en plus prégnantes, le secteur de la sécurité informatique est devenu une préoccupation pour les États. Dès 2001, le cas de Magic Lantern démontre la collaboration entre les éditeurs et certaines agences gouvernementales américaines[5]. En 2007, une enquête conduite par le magazine CNET s'intéressait aux demandes faites par l'administration à ces mêmes éditeurs pour mettre sur liste blanche les programmes développés par les autorités[6]. L'entreprise israélienne Check Point Software Technologies avait d'ailleurs fait savoir qu'elle répondrait avec la même courtoisie aux services de police qu'aux éditeurs logiciels qui demanderaient à être « whitelistés »[7]. À l'aune de ces éléments, on peut se questionner sur les enjeux économiques mais aussi stratégiques inhérents aux éditeurs de solutions antivirus.

Quelle neutralité pour les éditeurs d'antivirus ?

À l'heure où les menaces ne sont plus uniquement terrestres, navales ou aériennes, les éditeurs d'antivirus disposent, grâce à leur parc logiciel, d'un réseau de capteurs absolument unique au monde. Il est donc parfaitement logique qu'ils soient aux avant-postes dans la détection des activités malveillantes et des campagnes de cyber-espionnage, en particulier dû au fait qu'ils basent encore leurs technologies sur le principe de la signature.

Un antivirus a en effet la particularité « légitime » de pouvoir accéder à l'ensemble des informations du système sur lequel il est installé : messagerie, documents bureautiques, pages web visitées et même système d'exploitation. En

[1] https://www.opswat.com/resources/reports/antivirus-october-2014
[2] http://www.clubic.com/antivirus-securite-informatique/logiciel-antivirus/actualite-352666-avast-antivir-avg-marche-antivirus.html
[3] http://chart.av-comparatives.org/chart1.php
[4] Kolodgy Charles J., *Wordwide Endpoint Security 2010-2014 Forecast and 2009 Vendor Shares*, IDC, 2010.
[5] http://pqasb.pqarchiver.com/washingtonpost/doc/409229527.html?FMT=ABS&FMTS=ABS:FT&date=Nov+23%2C+2001&author=Bridis%2C+Ted&pub=The+Washington+Post&edition=&startpage=&desc=FBI+Is+Building+a+%27Magic+Lantern%27%3B+Software+Would+Allow+Agency+to+Monitor+Computer+Use
[6] http://news.cnet.com/2100-7348-6197020.html?tag=tb
[7] *Ibidem*.

complément, il échange avec les serveurs de l'éditeur (donc basés à l'étranger si l'on se place du point de vu français) d'une manière chiffrée, sans que l'on sache quelles informations sont envoyées ou reçues.

L'attribution des opérations de cyberespionnage par ces entités que sont les éditeurs de solutions antivirales soulève en revanche davantage de questions. Qu'il s'agisse de Regin mis au jour par Symantec, de Flame, de Babar, de Casper ou encore d'Equation Group par Kaspersky Lab, ces entreprises n'hésitent en effet pas à pointer du doigt les quelques États qui sont soupçonnés d'être à l'origine de ces campagnes. La plupart de ces entreprises ayant des liens avérés ou supposés avec leurs États respectifs, on peut dès lors légitimement s'interroger sur l'indépendance et la neutralité de leurs analyses qui incriminent rarement les États dont elles sont originaires.

Avant même la parution publique de rapports démontrant l'existence de telles campagnes de cyberespionnage, des entreprises comme FireEye auraient en effet pour habitude de transmettre ces documents aux gouvernements[8]. Certaines sont également consultées par leur État pour mener des investigations sur des actions de piratage ou entraîner des équipes spécialisées[9]. De fait, les autorités politiques privilégient souvent l'intervention de sociétés nationales jugées plus fiables. Dave DeWalt, le Président de FireEye, soulignait l'existence de tels liens lorsqu'il disait : *« tous [les États] ont des sociétés de sécurité nationales (…) On arrive, je pense, au développement de cyber-blocs de super puissances en compétition »*[10].

Ces connexions entre les pouvoirs publics et le secteur privé ne sont ni nouvelles ni surprenantes compte tenu du caractère éminemment stratégique de l'activité de ces éditeurs.

Ces liens sont en outre entretenus par la forte porosité entre les secteurs privés et public dans le domaine de la sécurité, du renseignement et de l'intelligence économique[11]. Le PDG de Kaspersky Lab, Eugene Kaspersky, a ainsi été formé dans un institut de cryptographie sponsorisé par le KGB, une biographie parfaitement assumée voire revendiquée par l'entreprise qui l'a d'ailleurs exploitée dans une campagne marketing destinée au Japon[12]. Même proximité avec le FSB, qui a d'ailleurs certifié sa solution, pour l'autre éditeur russe, Dr Web. FireEye aurait elle aussi des liens étroits avec le gouvernement américain. L'entreprise, dont le développement a été en partie financé par le fonds d'investissement de la CIA, In-Q-Tel, fournirait ses technologies à la NSA. La dimension stratégique de ces entreprises est apparue au grand jour en 2005 lorsque la Commission des investissements étrangers américaine (CFIUS), fondée sur l'avis du FBI et de la NSA, a empêché le rachat de Sourcefire par Check Point Software Technologies.

Vers l'émergence d'antivirus souverains

En 2013, les révélations d'Edward Snowden concernant le programme PRISM ont marqué une nouvelle étape dans la mise en lumière du rôle clé que peuvent jouer les grands éditeurs de logiciels dans les dispositifs de renseignement étatiques. Les chevaux de Troie, jadis totalement inavouables, sont même parfois officialisés et assumés. Le directeur de la NSA, l'Amiral Michael S. Rogers, s'est ainsi récemment prononcé en faveur de l'utilisation de portes dérobées[13]. En France la LOPPSI 2 (2001) a autorisé leur utilisation par certains services à des fins de lutte contre la criminalité et la délinquance organisée.

[8] http://blogs.wsj.com/digits/2015/03/23/when-cybersecurity-meets-geopolitics/
[9] *Ibidem*
[10] *Ibid*
[11] http://www.securite-strategie.fr/Enquete-Profils-et-trajectoires.html
[12] http://www.bloomberg.com/news/articles/2015-03-19/cybersecurity-kaspersky-has-close-ties-to-russian-spies
[13] http://www.numerama.com/magazine/32784-la-nsa-propose-d-avoir-juste-un-bout-de-votre-cle-de-securite.html

Face à ces pratiques et à la globalisation du marché de la sécurité, nombreux sont les États qui ont adopté une politique volontariste et émis des recommandations à l'attention de leurs citoyens et de leurs agences gouvernementales, voire de lancer des initiatives nationales. Depuis 2010, année de la découverte de Stuxnet, l'Iran développerait sa propre solution antivirale[14]. En 2014, les autorités chinoises ont publié une liste de cinq éditeurs de solutions antivirus chinois approuvés : Qihoo 360, Venustech, CAJinchen, Beijing Jiangmin et Rising[15]. En 2009, le Département de la défense américain avait adopté une politique similaire avec la mise à disposition au personnel d'éditions gratuites de programmes édités par Symantec et McAfee[16]. Certains pays ont donc pris le parti d'adopter une politique de préférence nationale ou de lancer des projets destinés à palier le manque d'éditeurs de confiance, non seulement pour des motivations économiques, mais également pour des raisons de sécurité et de souveraineté nationales.

L'émergence de ce concept de souveraineté numérique, c'est-à-dire de la prérogative de l'exercice, par l'État, d'une domination légitime et inaliénable sur son environnement numérique, a ainsi donné lieu au lancement de plusieurs initiatives nationales. En France, l'État, et en particulier le Ministère de la Défense, a soutenu dès 2011, à travers le Programme des Investissements d'Avenir, le projet de recherche et développement de « Démonstrateurs d'AntiVirus Français et Internationaux » (DAVFI)[17]. Ce projet, qui a réuni dans sa première phase (R&D) cinq acteurs français (Nov'IT, le laboratoire de cryptologie et de virologie opérationnelles de l'école d'ingénieurs ESIEA, Qosmos, Teclib' et DCNS Research) avait pour objectif de créer un antivirus français, de nouvelle génération et de confiance, destiné à un large marché incluant les opérateurs d'importance vitale, les entreprises et les particuliers. Après deux ans de développement (2012-2014), cette solution antivirus souveraine doit passer dorénavant du *démonstrateur* à son industrialisation par l'intermédiaire de Nov'It, le chef de file du projet. Il apparaît toutefois que la société rencontre les difficultés classiques de financement liées à cette étape d'industrialisation et qu'elle va devoir, par manque de moyens financiers donc, abandonner le projet, voire le transférer à des tiers qui pourraient prendre en charge cette étape.

Les politiques industrielles déployées par les États au nom de la sécurité nationale ne sauraient cependant faire fi des réalités économiques : le développement de produits souverains implique l'existence d'un marché dynamique et suffisamment vaste (330 millions d'euros pour la France en 2014), ainsi qu'un écosystème sachant favoriser le financement de solutions innovantes[18]. Et pour la France, ce marché passera nécessairement par la constitution progressive d'un marché numérique européen et par l'exportation.

[14] http://www.threatmetrix.com/whats-better-than-homemade-antivirus-a-ban-on-imported-software-means-iran-is-about-to-find-out/
[15] http://venturebeat.com/2014/08/04/chinese-government-curbs-use-of-u-s-anti-virus-software/
[16] http://www.stripes.com/news/dod-providing-free-anti-virus-for-home-computers-1.87750
[17] http://www.linformaticien.com/actualites/id/30700/davfi-l-antivirus-francais-lancera-bientot-un-appel-aux-hackers.aspx
[18] http://pro.clubic.com/it-business/securite-et-donnees/actualite-593458-davfi-nouvel-acteur-francais-securite.html

LES ETATS-UNIS DOMINENT-ILS TOUJOURS LE CYBERESPACE ?

Depuis la chute de l'Union soviétique, en décembre 1991, les Etats-Unis sont reconnus comme la première puissance mondiale. Certes, cette année les Etats-Unis ne sont plus la première puissance économique mondiale, mais force est de constater qu'en combinant les autres domaines (diplomatique, politique, militaire, technologique), les Etats-Unis surpassent les autres pays. Le cyberespace, qui constitue un vecteur de puissance essentiel pour les Etats-Unis mais également une source de vulnérabilités importantes, illustre parfaitement cette situation paradoxale.

Il est indiscutable qu'aux Etats-Unis, il y a eu un avant et un après Snowden. Un rappel des faits : Edward Snowden, employé de la *Central Intelligence Agency* (CIA) et de la *National Security Agency* (NSA) décide de rendre publique en Juin 2013, par l'intermédiaire de médias, des milliers de documents classifiés sur différents programmes de renseignements : PRISM, X-Keyscore, Tempora, GENIE, Bullrun, Quantum, etc. Ces documents permettent au monde de découvrir l'existence de nombreux programmes de surveillance de masse des citoyens américains et non américains, ainsi que des programmes d'espionnage économique et de personnalités politiques. Cet espionnage est réalisé par les Five Eyes, alliance des services de renseignements des Etats-Unis, Australie, Canada, Nouvelle-Zélande et Royaume Uni. Ces révélations créèrent une fissure dans les relations diplomatiques avec les autres pays. Au Brésil par exemple, suite aux révélations des interceptions des communications de Dilma Rousseff et de ses collaborateurs, la présidente brésilienne annule sa visite à Washington et annule sa commande de 36 F-18 Super Hornet de Boeing au profit du Gripen suédois de Saab. Officiellement "moins cher", mais moins performant.

Un élément intéressant à observer depuis les révélations d'Edward Snowden est l'implication des entreprises américaines à faire changer les pratiques du gouvernement américain. En effet, il est apparu que, suite à la mise en lumière du programme PRISM où l'on apprend que ce programme de surveillance électronique permettait la collecte de renseignements en accédant directement aux serveurs des fournisseurs de services électroniques (Facebook, Google, Apple, Microsoft, etc.), une forte chute du chiffre d'affaire est apparu pour ces sociétés. Selon une étude de Perspecsys[19] parue en 2014, 62% des personnes interrogées pensent que la négativité envers le cloud américain est justifiée. Lorsque le scandale de l'ampleur de la récupération de données par la NSA a été révélé, ces sociétés ont d'abord assuré qu'elles n'avaient pas eu d'autre choix que d'obéir. Mais au fur et à mesure des révélations sur l'étendue de l'espionnage, elles ont demandé au gouvernement une véritable réforme de ces systèmes de surveillance.

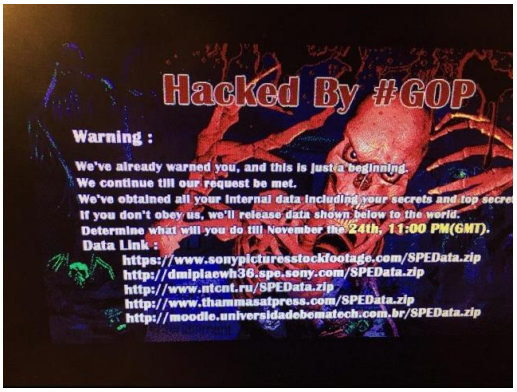
Le 26 mars 2015, les sociétés technologiques américaines (incluant Apple, Facebook, Google, Evernote, Twitter et Microsoft) ont appelé, dans une lettre ouverte, les Etats-Unis à ne pas renouveler la collecte en vrac des métadonnées[20], suite à l'expiration en Juin 2015 de la Section 215 du Patriot Act[21]. Des actions plus radicales ont été aussi mises en place par ces GAFA : Apple a voulu rebondir sur l'affaire PRISM, lors de la sortie de l'iPhone 6. En effet, pour le système d'exploitation du dernier iPhone, iOS8, Apple a mis en place un système de chiffrement des données qui empêche « techniquement » à la société californienne de répondre aux demandes des autorités souhaitant récupérer des informations d'appareils[22]. Cette nouvelle fonctionnalité n'a pas été appréciée par les autorités : le directeur du FBI, James Corney, voit cette fonctionnalité comme «(…) un moyen pour certaines personnes d'agir au-dessus des lois.», ainsi que John J. Escalante, chef du département d'enquête de la police de Chicago qui pense que

[19] http://perspecsys.com/cloud-trust/
[20] https://static.newamerica.org/attachments/2579-nsa-coalition-letter/NSA_coalition_letter_032515.pdf
[21] http://theoceancountylibrary.org/USPatriotActSection215.htm
[22] https://www.apple.com/privacy/government-information-requests/

«l'iPhone va devenir le téléphone préféré des pédophiles»[23]. Quant à Google, il a voulu faire comme son concurrent, mais a finalement cédé face aux pressions du gouvernement : le chiffrement ne sera pas activé par défaut[24] sur la dernière Android Lollipop, contrairement à leur déclaration initiale. C'est un choix qui devra être fait par le constructeur lui-même. Afin de faciliter le dialogue, le gouvernement Obama a décidé de se rapprocher de ces sociétés technologiques : ainsi, il a ainsi annoncé en avril 2015 l'ouverture dans la Silicon Valley d'un bureau de cybersécurité par le département de la sécurité intérieure[25].

Au sein du gouvernement américain, le cyber est devenu un sujet prioritaire. Le président Obama, lui-même, souligne que « les cyber-menaces représentent l'un des plus graves problèmes économiques et de sécurité nationale pour les Etats-Unis» et que lutter contre elles sont «une urgence nationale». Ces derniers mois, plusieurs mesures ont été prises par des décrets présidentiels afin d'améliorer la protection du pays sur ce sujet. Depuis le 30 mars 2015, un décret présidentiel[26] permet maintenant au Trésor américain de bloquer ou geler les avoirs des personnes impliquées dans des cyber-attaques sur les réseaux informatiques américaines « essentiels » et représentants «une menace importante pour la sécurité nationale, la politique étrangère, la santé économique ou la stabilité financière des Etats-Unis». Le 13 février dernier, deux nouvelles dispositions ont aussi été annoncées par le président Obama, lors du *Cybersecurity and Consumer Protection Summit* à l'Université de Stanford. La première incite les entreprises américaines à partager leurs informations classifiées sur les menaces informatiques avec le gouvernement[27]. La seconde est la création *du Cyber Threat Intelligence Integration Center* (CTIIC)[28] : ce centre sera chargé de coordonner et centraliser les informations relatives aux menaces dans le cyberespace.

Cette restructuration fait suite à l'affaire Sony qui révéla un manque de communication entre les différentes agences, chacune ayant un discours officiel différent sur les causes de cette attaque[29]. L'affaire Sony est un cas d'étude intéressant pour observer le comportement américain dans le cyberespace. Pour rappel, le 24 novembre 2014, suite à une demande de rançon non-payée par l'entreprise, le collectif *Guardians of Peace* diffuse plus de 11 To de données piratées chez Sony Pictures.



Message présent sur les postes de Sony après l'attaque.

[23] http://uk.businessinsider.com/police-apple-will-become-the-phone-of-choice-for-the-pedophile-2014-9?r=US
[24] http://arstechnica.com/gadgets/2015/03/02/google-quietly-backs-away-from-encrypting-new-lollipop-devices-by-default/
[25] https://www.hackread.com/homeland-cyber-security-silicon-valley/
[26] https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m
[27] https://www.whitehouse.gov/the-press-office/2015/02/12/fact-sheet-executive-order-promoting-private-sector-cybersecurity-inform
[28] https://www.whitehouse.gov/the-press-office/2015/02/25/fact-sheet-cyber-threat-intelligence-integration-center
[29] http://www.washingtonpost.com/world/national-security/white-house-to-create-national-center-to-counter-cyberspace-intrusions/2015/02/09/a312201e-afd0-11e4-827f-93f454140e2b_story.html

Des soupçons sont rapidement portés vers la Corée du Nord par le FBI, dû aux menaces émises par Pyongyang en cas de diffusion de *The Interview* par Sony Pictures, film parodiant le leader nord-coréen Kim Jong-Un. Or, cette théorie a été rapidement mise en doute par de nombreux experts : le groupe *Guardians of Peace* ne serait pas nord-coréen[30], une demande de rançon semble étrange pour une revendication par un Etat. De plus, il serait nécessaire d'avoir des complices à l'intérieur de l'entreprise pour pouvoir exfiltrer autant d'informations. Pour résumer, personne ne sait ce qu'il s'est réellement passé avec certitude. Or, en décembre 2014, la Corée du Nord se fait attaquer pendant une semaine, quelques heures après qu'Obama annonce qu'il fallait donner une réponse proportionnée à l'attaque de Sony[31]. Mi-mars 2015, le président de la commission de la sécurité intérieure américaine, Michael McCaul, annonce officiellement que les Etats-Unis sont responsables de ce black-out, en réponse au piratage de Sony[32]. Même si ce piratage n'a eu que très peu d'effet sur la Corée du Nord[33] (le pays possède seulement 1024 adresses IP et s'appuie sur son propre réseau national, Kwangmyong[34]), les Etats-Unis ont effectué une cyber-attaque afin de paralyser la connexion internet d'un pays sur la foi de renseignements gouvernementaux. Il s'agit là d'une application concrète d'un audit légal secret qui autoriserait le président des Etats-Unis à des cyber-attaques préemptives en cas de menaces venant de l'étranger fondées sur des preuves solides, en conformité avec la Constitution américaine et les lois internationales[35].

Cette posture politique et militaire est soutenue par un fort investissement au plan technologique qui constitue l'un des piliers du « soft power » américain. Selon le Financial Times[36], le montant des investissements dans la cybersécurité par les fonds capital-risque américains a augmenté de près de 100% en une année : 1,02 milliard de dollars sur les trois premiers mois de 2015 contre 540 millions de dollars à la même période l'année dernière. Et il en découle directement un autre type de domination, plus souterrain : les comités de normalisation et standardisation. Le sujet de la gouvernance est un domaine bien compris par les Etats-Unis : les instances de gouvernances techniques sont amenées à faire des choix, ayant des répercussions politiques, économiques et stratégiques. Ainsi, une norme d'une société américaine devenant un standard mondial est un net avantage pour la position et les intérêts de la société : elle possède un fort avantage face à ses concurrents. Les comités de standardisation sont aussi une cible pour les agences de renseignements américaines: le programme *Bullrun*[37] de la NSA, révélé par Snowden, en est un exemple flagrant. Le but de ce programme est, entre autres, de s'assurer le contrôle sur l'établissement de normes américaines et internationales de chiffrement (NIST, normes ISO) afin de faire intégrer, dès la conception, des affaiblissements de leurs solutions de chiffrement. Ainsi, le standard *Dual_EC_BG* (définissant la génération de nombres aléatoires) aurait été affaibli délibérément, afin de permettre de déchiffrer le contenu chiffré avec cet algorithme[38].

Les Etats-Unis poursuivent donc leur nouvelle « initiative de défense stratégique » destinée à leur assurer une entière liberté d'action dans le cyberespace. Ils n'hésitent désormais plus à faire usage, avec succès, de capacités offensives et même à revendiquer les actions menées, tant pour dissuader un éventuel agresseur que pour légitimer ce type d'opération aux yeux des opinions publiques mondiales. Toute la question est cependant de savoir si ces démonstrations de force constituent un signe extérieur de puissance ou bien traduisent au contraire une fragilisation progressive de la suprématie américaine sur cet environnement. Premier pays connecté au monde, les Etats-Unis restent aussi logiquement le plus vulnérable. Leur domination économique sur le cyberespace a par ailleurs été largement fragilisée par les révélations Snowden et par les stratégies de souveraineté numérique d'autres pays, avec la Chine et la Russie au premier rang.

---

[30] https://twitter.com/GuardiansGOP/status/545997922241085441
[31] http://www.telegraph.co.uk/news/worldnews/barackobama/11304729/Watch-live-Barack-Obamas-year-end-news-conference.html
[32] http://www.bloomberg.com/politics/articles/2015-03-17/north-korea-web-outage-was-response-to-sony-hack-lawmaker-says
[33] http://www.arbornetworks.com/asert/2014/12/north-korea-goes-offline/
[34] http://www.fastcolabs.com/3036049/what-its-like-to-use-north-koreas-internet
[35] http://www.nytimes.com/2013/02/04/us/broad-powers-seen-for-obama-in-cyberstrikes.html
[36] http://www.ft.com/intl/cms/s/0/5cfcbcbc-e692-11e4-afb7-00144feab7de.html
[37] http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html
[38] https://projectbullrun.org/dual-ec/

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