Observatoire du Monde Cybernétique

Lettre n°15 – Mars 2013

Cette note est disponible sur le portail OMC. Pour y accéder, rendez-vous sur : https://omc.ceis.eu/

[NetSecurity] Le forum Infosecurity Europe de 2013 en réponse aux cybermenaces

Le Forum InfoSecurity Europe se tiendra à Londres du 23 au 25 avril 2013. Pour cette 18ème édition, plus de 350 exposants seront présenteront les dernières innovations en matière de cyberdéfense.

[01Net] Exercice grandeur nature de cyberdéfense en Grande-Bretagne

Le samedi 9 mars s'est déroulée, à Newport au Royaume-Uni, la version européenne du Cyber Defence Challenge. L'édition regroupait experts civils et militaires en sécurité informatique – fournisseurs de matériels, éditeurs de logiciels, consultants, développeurs, étudiants, universitaires – pour un exercice de cyberdéfense grandeur nature. Il s'agissait de voir si la coordination d'actions entre plusieurs pays au moyen d'une plate-forme d'information et de communication commune était possible ; et de dénicher quelques nouveaux talents susceptibles de rejoindre les équipes des industriels présents.

[LeMonde] Cyberattaque sans précédent contre une entreprise de lutte contre le spam

La société de lutte contre le spam Spamhaus, basée à Genève a annoncé avoir été victime d'une importante attaque DDoS. Si l'origine de l'attaque n'a pas été clairement identifiée, Spamhaus a mis en cause Cyberbunker et des pirates d'Europe de l'est. L'attaque a été revendiquée par Sven Olaf Kamphuis, porte-parole des attaquants. L'attaque aurait eu des répercussions dans toute l'Europe et aurait touché des millions de personnes. Cette information a toutefois été démentie par des sociétés et organismes de surveillance du trafic Internet.

[MagSecurs] Le futur de la sécurité informatique vu par un investisseur en capital-risque

Selon l'avis d'un investisseur en capital-risque de la société KPC&B, l'avenir de la sécurité en ligne exigera un réajustement des offres. Symantec ou McAfee sont par exemple invités à revoir leur stratégie, le marché de l'antivirus étant voué à disparaître. Selon l'expert, l'objectif de la sécurité ne doit plus être d'empêcher les intrusions, mais de protéger les données. La dépendance à un actionnariat est quant à elle vue comme un handicap au développement de l'offre. Enfin, il prédit le remplacement des attaques de type DDOS par des ADOS (Application Denial of Service).

[LeMondeInformatique] MiniDuke : une campagne mondiale de cyberespionnage utilisant Twitter

Kaspersky Lab et le Crysys de l'université d'économie de technologie de Budapest ont découvert une campagne globale de cyberespionnage utilisant Twitter. Baptisée MiniDuke, cette opération diffuse des fichiers .PDF corrompus, cible des organisations stratégiques et communique avec ses serveurs C&C via Twitter. L'attaque utilise également un ensemble complexe de solutions de backdoor et d'anonymat. Ses victimes sont diverses, tant en profil qu'en répartition géographique, puisque l'opération a touché des sociétés, des administrations et des laboratoires de recherches en Europe, en Amérique et en Asie.

[Guardian] La Reserve Bank of Australia attaquée

La Banque Centrale Australienne a subi une attaque ayant pour finalité de récupérer des données sensibles sur les négociations du G20, entre autres. Un email corrompu aurait été envoyé de manière ciblée à plusieurs employés de la banque, et ouvert par six d'entre eux. La propagation du virus a pu être contrôlée.

[WahingtonPost] Le Pentagone crée des équipes en charge de lancer des cyberattaques

Le général Keith Alexander a annoncé au Congrès américain la création de 13 équipes d'attaque au sein du Cyber Command. Le directeur de la NSA et du Cyber Command craint cependant de voir ces efforts compromis par les restrictions budgétaires à venir.

[Af.mil] PACOM encourage le développement de capacités cyberdéfensives régionales

PACOM (U.S. Pacific Command) souhaite capitaliser les cybercapacités des entreprises et des organismes publics. Et puisque les cybermenaces sont internationales, il estime nécessaire de développer des outils entre partenaires afin de protéger les communications et de mieux comprendre la menace. En ce sens, PACOM lance un nouveau programme de workshops et de conférences bilatérales et multilatérales afin de promouvoir un engagement de la cybersécurité à l'échelle régionale.

[AllAfrica] Le Nigeria au top du classement mondial des cybercrimes, décide de réagir

Selon le colonel Sambo Dasuki du National Security Advisor, le Nigeria fait partie des pays perpétrant le plus d'actes cybercriminels au monde. En réaction, les autorités nigérianes souhaitent développer leurs infrastructures de cybersécurité, avec notamment la création d'un CERT national. La cybercriminalité est perçue comme une menace sérieuse au développement économique du pays et pousse les autorités et renforcer la protection de leurs infrastructures critiques.

[Computing] La Chine favorable à des discussions avec les Etats-Unis à propos de la cybersécurité

Suite aux propos tenus par le conseiller à la Sécurité nationale américain Thomas Donilon, la Chine a accepté d'entamer des discussions avec les Etats-Unis sur la cybersécurité. Lors d'une conférence, ce dernier demandait à la Chine trois choses : i) la reconnaissance de l'urgence et de l'ampleur du problème posé par la cybercriminalité ; ii) la mise en œuvre d'actions afin de limiter la cybercriminalité sur son territoire ; iii) le lancement d'un dialogue afin de définir des règles de bonne conduite.

[Haaretz] L'armée israélienne forme un service spécialisé pour renforcer sa cyberdéfense

Les forces de défense israéliennes (FDI) ont créé un service spécialisé pour diriger les opérations de cyberdéfense du pays. Le personnel de ce service sera chargé de surveiller et de neutraliser les tentatives de perturbation ou de piratage des systèmes informatiques israéliens. Il sera assigné au quartier-général cybernétique de l'armée. La constitution de ce service marque une nouvelle étape dans le renforcement des capacités de cyberdéfense israéliennes.

[TheStar] Selon le NSC malaisien, « la cyberguerre est un crime »

Faisant suite aux cyberattaques réciproques entre des pirates malaisiens et philippins entre le 1er et le 4 mars 2013, le Conseil National de Sécurité (NSC) malaisien a réaffirmé par la voix de son secrétaire général l'illégalité de toute cyberattaque, fut-elle perpétrée par des étrangers ou des nationaux - même au nom de la Malaisie. Au cours de cet épisode, des dizaines de sites malaisiens avaient été défacés.

[LeMonde] La cyberattaque qui a touché Séoul ne serait « pas spécialement sophistiquée »

Si les autorités sud-coréennes n'ont toujours pas identifié les auteurs de la cyberattaque qui a touché leurs réseaux informatiques, les méthodes d'attaque ont, elles, été analysées. Elles révèleraient la relative simplicité de l'attaque : les pirates auraient utilisé un virus connu depuis un an, rebaptisé « DarkSeoul », et n'auraient même pas assombri les commandes insérées dans la partie malveillante du code.

[CAS] Cybersécurité, l'urgence d'agir

Le Centre d'Analyse Stratégique, dépendant du premier ministre, a récemment publié une note intitulée « Cybersécurité, l'urgence d'agir » dans laquelle sont formulées quatre recommandations, toutes centrées sur l'ANSSI. La proposition n°3 envisage notamment un élargissement des missions de l'agence. Cette note propose de renforcer les exigences de sécurité imposées aux opérateurs d'importance vitale, de soutenir les PME dans la gestion des risques et de revoir le cadre juridique afférant à la cybersécurité.

[ReportersSansFrontieres] Rapport spécial sur la surveillance, « Ennemis d'Internet »

Reporters Sans Frontières a publié son rapport spécial sur la surveillance 2013 dans lequel sont recensés les Etats « ennemis d'Internet » (à savoir ceux menant une politique de surveillance en ligne systématique avec de graves violations des droits de l'homme). Sont cités : la Syrie, la Chine, l'Iran, le Bahreïn et le Vietnam. Cette année, le rapport va plus loin en proposant une liste de cinq entreprises fournissant des solutions de surveillance violant les droits de l'homme : Gamma, Trovicor, Hacking Team, Amesys et Blue Coat.

[ForeignPolicy] Combien de cybersoldats ont les Etats-Unis?

Après l'annonce du Pentagone de vouloir augmenter les effectifs du Cyber Command de 900 à 4 900 employés, des questions ont émergé quant au nombre réel d'individus américains au service des capacités cyber du pays. D'autant que le gouvernement chinois a évoqué, en réponse au rapport Mandiant, une unité d'une centaine de milliers de cybersoldats américains. S'appuyant sur les données publiquement disponibles et excluant donc les contractants civils des services de renseignement, Foreign Policy a recensé les individus appartenant à des services dédiés à l'armement cyber dans les diverses armées américaines (Air Force, Navy, Marine), pour un total entre 53 000 et 58 000 cybersoldats américains.

[ForeignPolicy] Le Defense Science Board recommande la création d'une force de dissuasion cybernétique

Le Defense Science Board (organisme indépendant de l'armée américaine mais qui conseille celle-ci) recommande au Pentagone dans son dernier rapport de développer une force armée à même de contrer toute cyberattaque de grande ampleur par une frappe cybernétique dévastatrice. Cette force armée viendrait se placer en alternative au recours nucléaire, mais aurait les mêmes objectifs de dissuasion. Des responsables du Pentagone ont affirmé travailler sur le développement de cyberarmes et prendre en compte ce rapport, envisageant même l'application de certaines de ses recommandations.

[CCDCOE] L'OTAN publie son manuel de législation des cyberconflits

L'OTAN a publié le manuel de Tallinn qui propose de définir les règles de droit international applicables aux cyberconflits. Parmi celles-ci, l'OTAN prévoit l'interdiction d'attaquer des hôpitaux ou des centrales nucléaires, mais légitime l'attaque contre des civils participant à des actes de cyberguerre. Ecrit par des experts juridiques du Comité International de la Croix Rouge (CICR) et du Cyber Command américain, ce manuel est une première tentative de codification du droit des cyberconflits. Le manuel autorise notamment les répliques proportionnées en cas de cyberattaque étatique. La contre-mesure ne peut cependant pas inclure l'usage de la force, à moins que l'attaque initiale n'ait causé de graves dommages ou la mort.

[MarketWatch] Un rapport sur les tendances et opportunités du marché de la défense 2013

La plate-forme d'informations business Strategic Defence Intelligence a publié un nouveau rapport intitulé « Global Defense Survey 2013 : Business Outlook, Key markets and Opportunities ». Le document revient sur les dynamiques industrielles de ce secteur et anticipe les transformations à venir pour la période 2013-2017.

Le marché des 0-day – Entre rentabilité, éthique et souveraineté nationale

Alors qu'un véritable marché noir des failles zero-day s'est développé, les chercheurs en vulnérabilités se sont longtemps contentés d'assurer un « responsible » ou « full » disclosure (alerter le développeur du logiciel de la faille découverte afin qu'il propose les patchs adéquats). La question de la vente « légitime » de ces « exploits » se pose depuis peu, la demande sur ce marché ayant explosé depuis 2011.

Focus : la faille zero-day

« *Il existe des lacunes dans la sécurité des logiciels depuis que les logiciels existent, mais elles ont depuis le développement des cyber-armes un impact beaucoup plus important* »[1]. Les attaques contre les logiciels peuvent résulter d'un schéma classique visant à casser les mesures de sécurité instaurées pour les protéger. Mais les logiciels et leurs fournisseurs sont désormais la cible d'une menace bien plus pernicieuse : les « vulnérabilités 0-day » ou « Zero-day Exploits ». Ces dernières sont en réalité des défauts que l'on retrouve dans la conception des codes des logiciels, et que les hackers peuvent d'une part trouver – que ce soit par hasard ou en cherchant volontairement – et d'autre part exploiter, et ce avant que l'entreprise qui a conçu le logiciel ne se rende compte de l'existence du défaut en question.

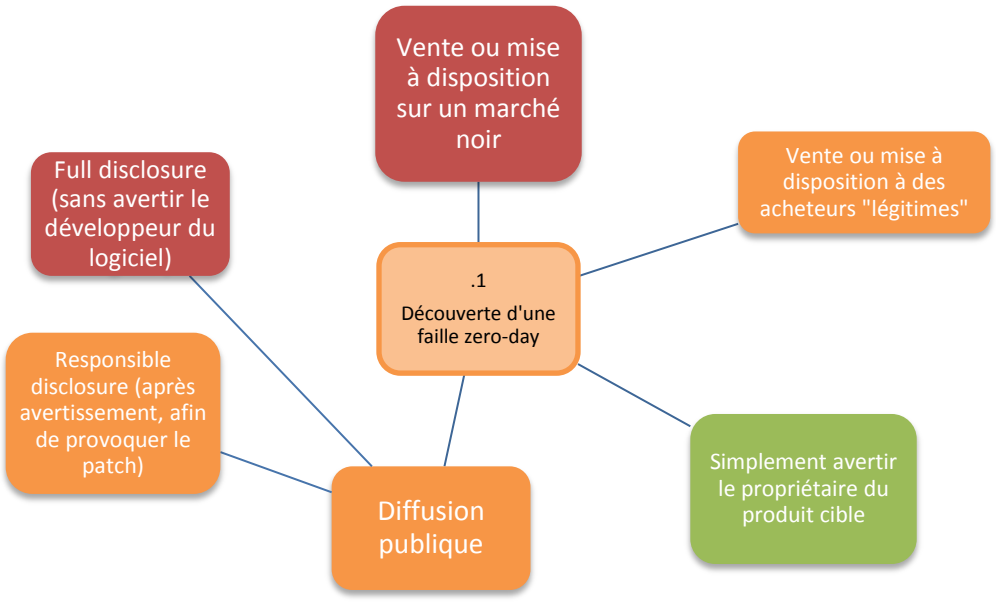

Figure 1. Schéma récapitulant les actions possibles suite à la découverte d'une faille zero-day (rouge : explicitement illégal – orange : incertitudes, tolérance ou source de débats – vert : légal)

[1] NPR, « In cyberwar, Software Flaws Are a Hot Commodity », http://www.npr.org/2013/02/12/171737191/in-cyberwar-software-flaws-are-a-hot-commodity

Le débat full/responsible disclosure

Face à l'extension de ce business qui se développe en sous-terrain, la question de la découverte des vulnérabilités zero-day et de leur diffusion gratuite fait toujours débat. Puisqu'il est avéré que le nombre d'attaques explose dès lors que la vulnérabilité est rendue publique, certains experts estiment qu'il est nécessaire de ne pas dévoiler cette faille au grand public, mais d'en avertir uniquement le fournisseur du logiciel affecté par l'une de ces vulnérabilités. Une autre position consiste à vouloir communiquer le plus possible sur ces failles une fois découvertes, ceci étant l'unique moyen de forcer l'entreprise à trouver puis à fournir aux utilisateurs un patch de sécurité adapté à la faille. Il en résulte un vrai questionnement, opéré par ceux qui découvrent les failles zero-day, quant à l'intérêt ou non pour eux d'avertir les fournisseurs des logiciels défaillants.

Le marché des zero-day

Le marché des zero-day est discret et relativement secret. Les relations entre les différents acteurs sont encadrées par des accords de confidentialité stricts et les listes de clients bien gardées. C'est un marché également très complexe en raison de l'encadrement incertain et du débat éthique qu'il soulève.[2]

Les **entreprises proposant ces services** sont connues mais ne communiquent que très peu sur leurs activités sur le marché des zero-day. Il n'existe pas de « place de marché » officielle permettant, pour un chercheur, d'identifier clairement un acheteur ou, pour un acheteur, de faire « son marché » parmi les dernières failles découvertes. Ces entreprises (ou les chercheurs proposant de vendre le fruit de leurs recherches) sont également confrontées aux difficultés de vente inhérentes au produit proposé : difficile en effet de prouver la réelle détention d'un exploit zero-day sans le dévoiler totalement à l'acheteur, et difficile, de l'autre côté, de faire confiance.

Si les listes de **clients** sont bien gardées, la plupart des entreprises indiquent ne vendre leurs exploits qu'à des agences du gouvernement ou des contractants militaires. Elles ne sont toutefois pas à l'abri d'un glissement vers un acheteur moins « légitime », comme le souligne le dirigeant de Vupen, société française positionnée sur ce marché[3].

Les prix d'une faille zero-day varient entre 20 000 et 500 000 $. Mais ces montants sont essentiellement fixés par le bon vouloir des acheteurs finaux. Si peu de règles semblent établies sur ce marché, le montant d'une transaction peut varier du fait de plusieurs facteurs[4]. Par exemple, la vente d'un exploit issu d'un logiciel utilisé à grande échelle sera plus importante que celle d'un exploit provenant d'un logiciel peu connu. De même, le prix sera plus conséquent si la vulnérabilité concerne la mise à jour la plus récente d'un logiciel. Selon Andy Greenberg de Forbes, la liste des prix de vente est actuellement la suivante :

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

[2] http://securityevaluators.com/files/papers/0daymarket.pdf

[3] http://www.washingtonpost.com/world/national-security/secrecy-surrounding-zero-day-exploits-industry-spurs-calls-for-government-oversight/2012/09/01/46d664a6-edf7-11e1-afd6-f55f84bc0c41_story.html

[4] NetSecurity, « How much does a 0-day vulnerability cost ? », http://www.net-security.org/secworld.php?id=12652

La recherche de la rentabilité primerait-elle sur l'éthique et la sécurité des produits ?

La rentabilité au cœur du débat

La vente de failles zero-day est rapidement apparue comme le moyen de rémunérer une activité de recherche avancée. Les chercheurs émettent en effet parfois des réticences à diffuser « gratuitement » le résultat de leurs travaux dans le cadre de full ou responsible disclosures, lorsqu'ils peuvent le vendre pour un prix important.

> ***"We wouldn't share this with Google for even $1 million," Vupen chief executive and head of research Chaouki Bekrar told Forbes. "We don't want to give them any knowledge that can help them in fixing this exploit or other similar exploits. We want to keep this for our customers."***

Cette volonté de reconnaissance mais surtout de rémunération s'oppose aux considérations éthiques développées par d'autres acteurs, tels que l'EFF[5]. Le fait de ne pas révéler la faille, mais de la vendre, aurait un effet contreproductif pour la sécurité[6]. La conséquence directe est en effet de priver le développeur du logiciel vulnérable de l'opportunité de patcher/corriger cette vulnérabilité, donc d'améliorer la qualité de son produit. La conséquence indirecte étant de « flouer » le consommateur, en conservant des failles de sécurité au détriment de la fiabilité des produits présentés comme sécurisés.

Le marché des failles zero-day : la mise à disposition de vulnérabilités critiques au plus offrant

Une étude réalisée par deux chercheurs de la société Symantec, Leyla Bilge et Tudor Dumita, a démontré que ces failles existaient en moyenne trois cents jours avant d'être corrigées ou sécurisées. Plus précisément, les attaques sur les vulnérabilités Zero-Day durent entre 19 jours et 30 mois. Une durée relativement longue, surtout lorsque l'on sait qu'une fois connues du grand public, le nombre d'attaques reçues par les vulnérabilités zero-day est multiplié par 100 000.

Les deux chercheurs ont réalisé une étude à partir des données provenant de plusieurs millions d'ordinateurs opérant avec les systèmes antivirus Symantec. Ils ont analysé ces données avec un catalogue de « Zero day Exploits » connus et un autre répertoriant des logiciels malveillants plus courants, installés sur les ordinateurs. Au total, les analystes ont découvert dix-huit vulnérabilités Zero-Day : 3 divulguées en 2008, 7 en 2009, 6 en 2010 et 2 en 2011[7]. Une fois divulguées, l'étude démontre que le nombre de variantes (ou de fichiers qui exploitent les vulnérabilités), augmente considérablement de 183 000 fichiers chaque jour[8]. Enfin, ce que l'étude souligne, c'est que les professionnels de la sécurité informatique et ceux chargés des logiciels antivirus, découvrent parfois ce type de vulnérabilités bien après sa première exploitation par des hackers. Ainsi chaque année, en moyenne, 8 vulnérabilités Zero-day échappent au contrôle et au radar des entreprises de sécurité informatique. D'où la difficulté de lutter contre ce phénomène.

Les analystes confirment que les utilisations de ces exploits sont, la plupart du temps, ciblées et mettent en œuvre des techniques d'espionnage d'une grande complexité. C'est le cas par exemple, à un niveau étatique,

[5] https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate

[6] Certains pensent toutefois le contraire : http://pentest.netragard.com/2012/08/13/selling-zero-days-doesnt-increase-your-risk-heres-why/

[7] Leyla Bilge, Tudor Dimitras, « Before We Knew It. An Empirical Study of Zero-day Attacks In The Real World », http://www.scribd.com/fullscreen/110211403?access_key=key-16cjr3zsofvp0t5kwbd9

[8] *Ibid*., p. 9

de l'attaque Stuxnet, qui était elle-même basée sur plusieurs vulnérabilités Zero-day[9]. Ainsi en théorie, chacun peut, s'il possède les moyens suffisants, s'offrir une vulnérabilité Zero-Day découverte sur un logiciel et s'en servir ensuite pour une durée suffisamment longue pour en profiter.

Le marché des zero-day, un atout pour la cybersécurité nationale ?

Pour un encadrement raisonnable et profitable de la vente de zero-day

L'idée d'un encadrement juridique du marché des zero-day n'est pas nouvelle. Si son effectivité est souvent remise en cause (analogie avec le contrôle impossible des armes à feu), cette régulation juridique pourrait, en fait, permettre un usage plus transparent et assumé de ces failles zero-day.

Trois visions s'opposent en la matière : l'interdiction, la libéralisation ou l'encadrement. L'encadrement (autorisation sous conditions) présente le double avantage de permettre à la fois l'usage de ces failles zero-day pour la LIO nationale par les agences gouvernementales, et l'interdiction de l'exportation de tels produits afin de ne pas les mettre à disposition de pays hostiles. Cette distinction entre marché interne et marché externe va de pair avec la notion d'indépendance nationale développée par certains auteurs.

Elle exige aussi, dans certains cas, une clarification des textes. Clarification nécessaire en France par exemple, de l'article 323-3-1 du Code pénal fortement décrié. L'article prévoit en effet la répression du fait, « sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre » une atteinte à un système de traitement automatisé de données, sans proposer de définition claire de ce « motif légitime ».

Les chercheurs et professionnels de la sécurité et de la cyberdéfense plaident pour la mention claire et explicite des besoins de la recherche comme « motif légitime ». La vente d'exploits aux agences gouvernementales à des fins de lutte informatique pourrait-elle, à terme, être visée comme « motif légitime » ?

La recherche de vulnérabilités, source d'indépendance nationale en matière de LIO

Face aux critiques dont a fait l'objet la société Vupen[10], le chercheur Eric Filiol a émis un avis tranché sur la question. Il souligne dans sa tribune[11] l'importance, pour un pays, de bénéficier sur son territoire des travaux d'une telle entreprise. Source d'indépendance nationale en matière de recherche de vulnérabilités, cela permet tant d'améliorer les capacités cyberdéfensives et cyberoffensives d'un pays, que d'assurer une dissuasion efficace. La recherche de vulnérabilités nouvelles serait, en somme, le pivot d'une cybersécurité efficace. Le développement du marché correspondant et la tolérance des Etats en dépit d'une législation souvent hostile, confirme que la course au cyber armement est aujourd'hui un enjeu national prioritaire pour les Etats.

[9] ArsTechnica, « Zero-day attacks are meaner, more rampant than we ever thought », http://arstechnica.com/security/2012/10/zero-day-attacks-are-meaner-and-more-plentiful-than-thought/

[10] http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/

[11] http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221164714/affaire-vupen-quand-competence-francaise-fai

Feuille de route numérique du Gouvernement : quelles opportunités en matière de cybersécurité ?

Certains ont pu regretter l'apparente timidité de la feuille de route numérique gouvernementale en matière de cybersécurité. De fait, parmi les 18 mesures annoncées, aucune n'est dédiée spécifiquement à la sécurité des réseaux et systèmes informatiques. La cybersécurité apparait pourtant en filigrane dans de nombreux objectifs et mesures annoncées. Analyse de la feuille de route à travers le prisme de la cybersécurité.

Le numérique est un levier de transformation global. Il est à la fois un atout pour la compétitivité des entreprises, un outil de promotion des valeurs fondatrices de la République et une chance pour la jeunesse. Tels sont en substance les trois axes de la stratégie numérique du Gouvernement qui propose également 18 mesures (cf. tableau ci-dessous), dont certaines constituent de vraies opportunités pour le renforcement de la cybersécurité en France.

Premier axe, la jeunesse

Le premier axe, consacré à la jeunesse, a ainsi pour objectif de faire entrer le numérique dans le scolaire et de renforcer la formation aux métiers du numérique. L'occasion d'une part d'intégrer aux programmes scolaires une initiation à « l'hygiène numérique », d'autre part de renforcer l'enseignement des différentes disciplines connexes ou spécifiques à la cybersécurité. Cette action devra cependant aller de pair avec l'élaboration d'un référentiel des métiers de la cybersécurité détaillant pour chaque type de poste, les compétences principales ou secondaires requises, les certifications et les formations existantes. Il n'existe en effet pas un mais des métiers de la cybersécurité. On peut par exemple citer l'architecte, l'auditeur, le développeur, l'analyste, le juriste ou l'enquêteur.

Deuxième axe : la compétitivité des entreprises

Le deuxième axe (« renforcer la compétitivité de nos entreprises grâce au numérique ») présente quant à lui plusieurs intérêts. Avec la création de démonstrateurs dédiés au numériques (les 15 quartiers numériques, dont le premier sera prochainement lancé en région parisienne) sur le modèle du Tech City londonien, il offre aux industriels, dont ceux de la confiance numérique, la possibilité de déployer « in vivo » leurs solutions. La R&D n'est pas en reste avec 150 millions d'aides mobilisés dans le cadre du programme Investissements d'avenir sur 5 technologies clés : les objets connectés et logiciels embarqués, le calcul intensif, le cloud computing « maîtrisé », le « big data » et la sécurité des systèmes d'information. Il parait en effet fondamental de concentrer les budgets sur quelques domaines clés, transversaux et sur lesquels nous disposons de compétences reconnues et de technologies matures. Troisième priorité annoncée, les infrastructures, avec trois mesures : le déploiement des technologies « smart grid » destinées à faciliter la transition énergétique, la mise à niveau de nos capacités de cyberdéfense et le soutien au développement de filières françaises pour la fourniture de « services numériques stratégiques ». Un appel à projet devrait ainsi être lancé avant l'été par le Commissariat général à l'investissement pour la sécurisation des systèmes d'information mobile (tablettes et téléphones).

Troisième axe : la promotion des valeurs

Le troisième axe (« promouvoir nos valeurs dans la société et l'économie numériques ») a une portée plus politique. Il s'agit de renforcer la lutte contre la cybercriminalité (création récente du groupe de travail interministériel), de moderniser l'action publique et l'offre de soins grâce au numérique, mais aussi de refonder la stratégie de l'Etat en matière d'identité numérique. Le Secrétariat général pour la mobilisation de l'action publique (SGMAP) est ainsi chargé de formuler des propositions d'ici l'été 2013, puis des plans d'actions pour la fin 2013, l'objectif étant de disposer de solutions d'identification et d'authentification déployables en 2014. Dernière priorité : répondre aux enjeux internationaux du cyberespace en soutenant un rééquilibrage de la gouvernance mondiale (le sens du rééquilibrage reste cependant à définir…), en développant les coopérations avec les pays en développement et en contrôlant l'exportation des technologies de surveillance de l'Internet. Le Gouvernement entend ainsi intégrer ces dernières dans la liste des biens et technologies à usage dual des Accords de Wassenaar, ce qui suppose de définir au préalable la liste de ces technologies (difficile puisque la plupart sont parfaitement « réversibles ») et de mettre d'accord l'ensemble des partenaires. Le Quai d'Orsay a cependant fait part de réserves sur l'application d'une telle mesure, estimant que les systèmes informatiques en question n'entrent pas la catégorie des matériels de guerre ni dans celle des biens à double usage, et n'ont pas vocation à en faire partie, malgré la réflexion entamée en ce sens par le gouvernement[12].

Reconnaissant les défis nouvellement présentés par la diffusion massive des technologies numériques dans la vie des citoyens français et le manque de prise en compte de son impact sur la vie privée des utilisateurs, le gouvernement entend également développer la législation protégeant la vie privée. Elle fera notamment l'objet d'un plan d'action pour le développement de services d'identité numérique sécurisés et respectueux de la vie privée, mais également d'une campagne de sensibilisation dès l'enseignement primaire à la protection de la vie privée. Fleur Pellerin a affirmé souhaiter répondre aux attentes des citoyens en matière de vie privée en proposant une loi sur la protection des droits et des libertés numériques, mais également en pesant sur les discussions européennes. Les ambitions françaises en termes de protection de la vie privée ne se limitent donc pas à la législation nationale mais souhaitent influencer l'orientation européenne donnée aux débats sur cette thématique[13].

Objectifs	Mesures	Quelles opportunités en matière de cybersécurité ?
Axe 1 : faire du numérique une chance pour la jeunesse	Mesure n°1 : entrée du numérique dans les enseignements scolaires.	Proposer une sensibilisation à « l'hygiène numérique ».
	Mesure n°2 : formation de 150 000 enseignants en 2 ans.	Proposer une sensibilisation à « l'hygiène numérique ».
	Mesure n°3 : lancement du Projet France Universités Numériques lancé avant l'été 2013.	Proposer un « e-learning » de sensibilisation à la sécurité des systèmes d'information ainsi qu'un programme de formation dédié à la

[12] http://www.nosdeputes.fr/14/question/QE/15634
[13] http://www.gouvernement.fr/gouvernement/feuille-de-route-pour-le-numerique-3-questions-a-fleur-pellerin

		cybersécurité.
	Mesure n°4 : renforcement des formations aux métiers du numérique.	Etablir un référentiel global sur les métiers de la cybersécurité et développer les filières correspondantes. Evaluer, aux plans quantitatifs et qualitatifs, les besoins RH en matière de cybersécurité.
	Mesure n°5 : faire du numérique une chance pour les jeunes peu qualifiés.	Organiser des challenges informatiques afin de déceler des potentiels.
Axe 2 : renforcer la compétitivité de nos entreprises grâce au numérique	Mesure n°6 : création de quartiers numériques (dont un premier à Paris ou en IDF en 2013). Création de « French digital houses », vitrine du numérique français à l'étranger.	Intégrer la SSI au cœur de ces projets. Participation des acteurs de la confiance numérique à ces démonstrateurs.
	Mesure n°7 : 150 millions d'aides à la R&D mobilisés dans le cadre du programme d'investissements d'avenir sur les 5 technologies stratégiques identifiées : objets connectés et logiciels embarqués, calcul intensif, cloud computing « maîtrisé », technologies « big data », sécurité des systèmes d'information.	Futurs appels à projets de R&D orientés « sécurité » ou comprenant une brique « sécurité ».
	Mesure n°8 : financement de la numérisation des PME et ETI grâce à une enveloppe de prêts de 300 millions d'euros (BPI).	Intégrer la SSI dans les programmes de diagnostic et de formation
	Mesure n°9 : couverture intégrale de la France en très haut débit d'ici 10 ans.	
Axe 3 : promouvoir nos valeurs dans la société et l'économie numérique	Mesure n°10 : développer les Espaces Publics Numériques pour faciliter l'accès aux outils numériques.	
	Mesure n°11 : généralisation de la délivrance de certificats diplômants sur l'utilisation des outils numériques pour les demandeurs d'emploi et les personnes en emploi les moins diplômées.	
	Mesure n°12 : rétablir notre souveraineté fiscale. Soutien au concept d'établissement stable virtuel dans les conventions OCDE, promotion à l'échelle européenne d'une assiette consolidée d'impôts sur les sociétés pour les prestataires de services électroniques, étude sur l'opportunité d'introduire des dispositions relatives à la fiscalité du numérique dans le PLF 2014.	

	Mesure n°13 : une loi sur la protection des droits et des libertés numériques.	
	Mesure n°14 : numérisation du patrimoine culturel.	
	Mesure n°15 : faire de l'ouverture des données publiques le levier de la modernisation de l'action publique.	
	Mesure n°16 : refonder la stratégie de l'Etat en matière d'identité numérique.	
	Mesure n°17 : territoires de soins numériques : moderniser l'offre de soins en mobilisant les technologies numériques.	Renforcer la prise en compte de la SSI dans le secteur de la santé.
	Mesure n°18 : contrôle de l'exportation des technologies de surveillance de l'internet.	

Le portail OMC
La nouvelle plateforme de la DAS

Découvrez le nouveau portail OMC. Pour y accéder, rendez-vous sur : https://omc.ceis.eu/

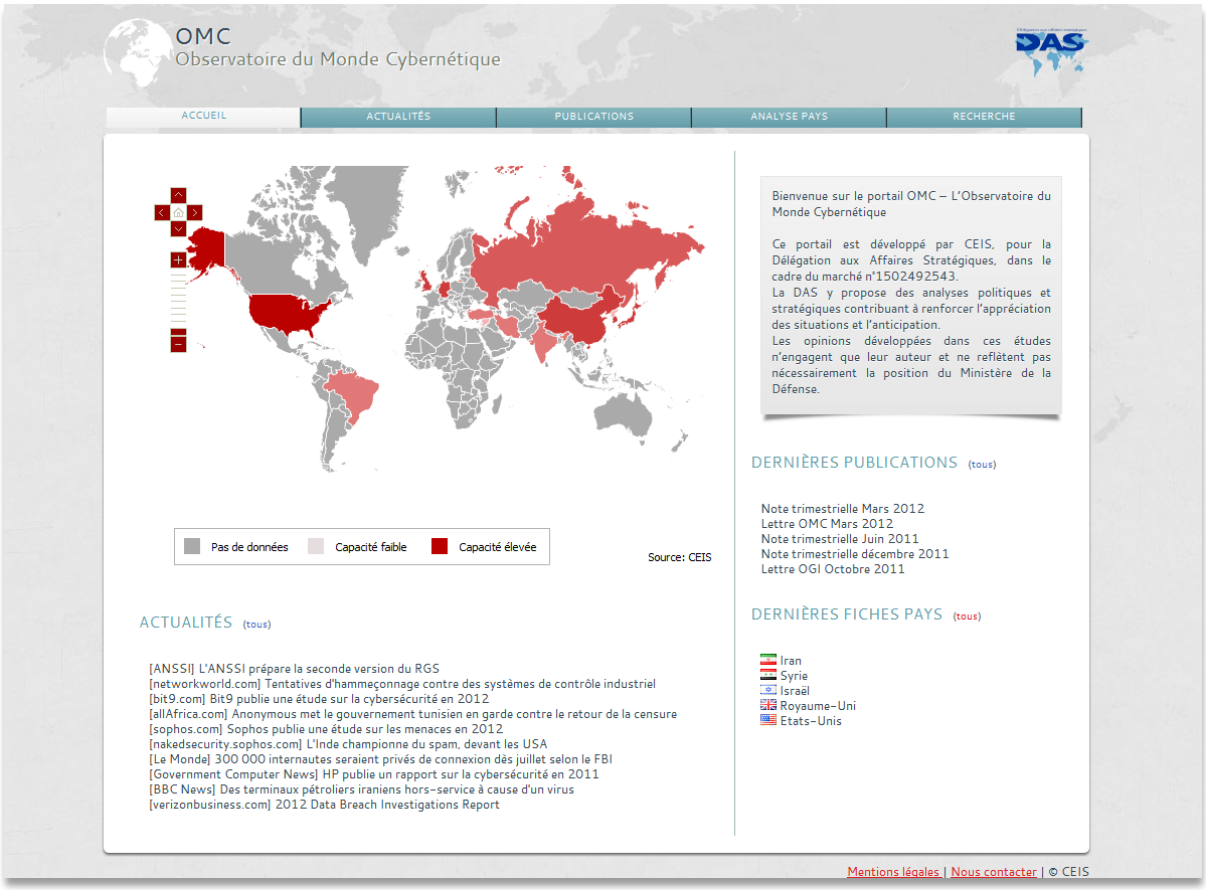

Figure 2. Page d'accueil du portail OMC - https://omc.ceis.eu/

Pour vous y connecter, n'hésitez pas à demander vos identifiants à CEIS.

Contact : Barbara Louis-Sidney - blouis@ceis.eu et omc@ceis.eu

International Forensic Sciences, Cyber Security and Surveillance Technologies	Istanbul, Turquie	27 – 29 mars
Cyber Security for the Chemical Industry Europe	Francfort, Allemagne	26 – 27 mars
Global Security Asia	Singapour	2 – 4 avril
GS Days	Paris	4 avril
ROOMn, les Rendez-vous One-to-One de la Mobilité Numérique	Deauville	10 – 11 avril
International Forensic Technologie Fair	Varsovie	10 - 12 avril
Forum InfoSecurity Europe	Londres	23 – 25 avril
Cyber Security Forum	Dubai	29 – 30 avril
3rd Annual Cyber Security Summit Prague 2013	Prague	11 – 12 avril
The Commonwealth Cybersecurity Forum of the CTO	Yaoundé	22 – 26 avril
SSTIC 2013	Rennes	5 – 7 juin
NSC – No Such Conference (Hacking éthique)	Paris	15 – 17 mai
ACM Workshop on Information Hiding and Multimedia Security	Montpellier	17 – 19 juin
Hack in Paris	Paris	17 – 21 juin
La Nuit du Hack	Marne La Vallée	22 – 23 juin
Les Assises de la Sécurité et des Systèmes d'Information	Monaco	2 – 5 octobre

CEIS

Compagnie Européenne
d'Intelligence Stratégique

Téléphone : 01 45 55 00 20
Télécopie : 01 45 55 00 60
E-mail : gtissier@ceis.eu

Les opinions exprimées dans cette lettre n'engagent que la responsabilité de leurs auteurs.

Retrouvez cette lettre et l'ensemble des articles cités sur le portail
https://omc.ceis.eu/
(Accès soumis à authentification)

La Délégation aux Affaires Stratégiques 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 DAS a confié à la **Compagnie Européenne d'Intelligence Stratégique (CEIS)** 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
Délégation aux Affaires Stratégiques
Sous-direction Politique et Prospective de Défense
14 rue St Dominique 75700 PARIS SP 07