Observatoire du Monde Cybernétique

Lettre n°7 - Juillet 2012

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

[securitydefenceagenda] La Belgique exposée aux cyberattaques

La Belgique est particulièrement exposée aux cyberattaques, selon le rapport annuel du Comité R en charge de la surveillance de la sécurité des systèmes informatiques nationaux belges. En cause : une approche jugée incohérente et non-globale.

[BusinessDay] Les Jeux Olympiques font craindre une recrudescence des cyberattaques

Les autorités britanniques, qui craignent une recrudescence des cyberattaques en raison des Jeux Olympiques, ont annoncé la mise en place d'une Task Force capable de faire face, avec le CIO, aux éventuelles menaces.

En 2008, les Jeux de Pékin ont généré pas moins de 12 millions d'attaques potentielles ou avérées par jour. Atos, sponsor officiel des Jeux depuis 2002, table sur un risque de 14 millions d'attaques par jour.

[reuters] Le cyber, futur du marché de l'armement

Le marché de l'armement serait au point mort, à l'exception du cyber et du renseignement-surveillance-reconnaissance (*ISR*). C'est le constat issu du salon de Farnborough qui s'est déroulé durant le mois de juillet, au Royaume-Uni. Ces deux derniers segments sont en effet en forte croissance, incitant les grands groupes tels que Raytheon à acquérir de nombreuses sociétés spécialisées de petite taille afin de stimuler leur R&D.

[itespresso] Cybersécurité : remettre à plat la stratégie européenne

La Commission européenne lance une consultation sur la sécurité de l'information. Ce débat devrait contribuer à l'établissement d'un nouveau document sur la cybersécurité.

[Intelligence Online] Europe : Financement de programmes de protection contre les attaques électromagnétiques

La Commission européenne va financer à hauteur d'environ 3,5 millions d'euros les programmes de recherche Structures et Hipow. Ces deux projets devront évaluer les vulnérabilités des infrastructures critiques européennes face aux attaques électromagnétiques (EMP) et développer des capteurs de détection des menaces en temps réel, afin de mettre en place une stratégie de protection communautaire.

[Reuters] Le Conseil des droits de l'homme de l'ONU adopte sa première résolution sur le droit à la liberté d'expression sur Internet

Le Conseil des droits de l'homme de l'ONU a adopté le 5 juillet la première résolution sur le droit à la liberté d'expression sur Internet, malgré l'opposition de certains pays comme l'Inde et la Russie. Soutenu par 83 États, le texte affirme que *« les droits dont les personnes jouissent hors ligne doivent également être protégés en ligne »*. La résolution invite les pays membres à promouvoir et faciliter l'accès à Internet.

[defense.aol.com] Comment résoudre le problème de l'attribution des attaques ?

Lors d'une réunion de l'American Foreign Policy Council, l'expert Larry Wortzel s'est exprimé sur le problème de l'attribution des attaques. Selon lui, cette question pourrait être résolue grâce à un système de responsabilité étatique qui se dispenserait d'un dispositif formaliste de preuve. Il a rappelé que chacun des éléments physiques qui composent le cyberespace est soumis à la juridiction du lieu où il est situé.

[vpk] Un conseiller en cyberguerre américain veut louer les services de hackers

John Arquilla, expert américain, a appelé le gouvernement américain à louer les services de hackers. Selon lui, les Etats-Unis devraient s'inspirer de certains pays en passe de devenir des géants du monde cybernétique qui emploieraient déjà ce type de profils.

[wired] Le *Fog Computing* pour faire face aux fuites de secrets défense ?

Des recherches du Pentagone regroupées sous le concept de « *Fog Computing* » permettraient de répondre aux menaces internes, en dissimulant les fichiers classifiés dans un nombre incalculable de faux fichiers attirants. Des faux fichiers qui, attachés à des traceurs, permettraient de remonter à la source de la fuite.

[Intelligence Online] Développement d'une radio universelle par la Darpa

La Darpa a confié à l'université de Purdue, dans l'Indiana, le développement d'une radio logicielle qui, couvrant un large spectre de fréquences, pourrait se transformer en radio, en intercepteur GSM ou WiFi, en brouilleur d'ondes ou encore en récepteur GPS sur le champ de bataille. Objectif : combler le retard de la Darpa sur les hackers aujourd'hui capables de déployer des réseaux GSM artisanaux.

[wired] Le spoofing GPS de drones, simple prélude au hacking GPS généralisé ?

Lors d'un exercice récent, un drone civil aurait été *spoofé* avec 1000 $ de matériel par des chercheurs de l'université du Texas. L'utilisation très répandue du GPS est d'autant plus inquiétante que les signaux GPS ne sont aucunement protégés, même de techniques d'interférence simples.

[beyondbrics] La Russie souhaite renforcer son influence sur ses géants de l'Internet

Un projet de loi russe donnerait au Kremlin un droit de regard en cas de prise de participation significative d'une société ou d'un gouvernement étranger au capital de l'un des géants russes de l'Internet, comme Yandex ou Mail.ru.

[wired] Mahdi, un nouveau malware détecté en Iran et en Israël

Des chercheurs de Seculert et Kaspersky Lab ont découvert Mahdi, un cheval de Troie localisé principalement en Iran et en Israël. Le malware, au code relativement simple, a infecté près de 800 postes et permet de subtiliser des fichiers PDF, Word et Excel. Certaines lignes du code sont en farsi, évoquant une éventuelle origine iranienne. Aucune connexion n'a pu être établie entre Mahdi et Flame.

[TurkishWeekly] L'Iran se dote d'un SOC

L'Iran s'est récemment doté d'un Security Operation Center (SOC). Organisé par un groupe d'entreprises locales souhaitant se protéger de futures attaques telles que Stuxnet, ce centre veillera sur les réseaux, bases de données et sites web iraniens des secteurs financier, gouvernemental, militaire et industriel. Le groupe, opérationnel depuis le 18 juillet, emploierait près de 15 personnes.

[TurkishWeekly] L'Iran envisagerait la création d'un Cyber command

L'Iran envisagerait la création d'un Cyber Command afin de faire face à toutes sortes de menaces cybernétiques. Ce centre dédié à la cyberguerre accueillerait également un département de guerre psychologique.

[cyberlympics] Global CyberLympics : les premiers championnats internationaux de hack éthique

Pour la première fois, une compétition internationale en cybersécurité se déroulera simultanément sur les cinq continents durant l'année 2012.

L'événement permettra de découvrir de nouveaux talents, méthodes et idées ; d'encourager une prise de conscience au sein de la communauté internationale ; de renforcer la cohésion entre professionnels de la sécurité informatique ; et de travailler à la création d'un environnement assurant la protection et l'éducation des plus jeunes.

[isc.independant.gov.uk] Le rapport annuel du comité « renseignement et sécurité » britannique

Dans son rapport annuel, l'ISC détaille sa nouvelle cyberstratégie et englobe de nombreux concepts tels que le cyberespionnage, le cyberterrorisme ou encore la mise en place d'armes cybernétiques tels que Stuxnet. L'acquisition d'armes cybernétiques constitue donc un véritable enjeu pour le Royaume-Uni, souhaitant à la fois se protéger et être en mesure d'attaquer.

[Trendmicro et softpedia] « Blackhole Exploit Kit » ou comment Blackhole a changé le *phishing*

Trend Security analyse dans un rapport comment le *kit d'exploit Blackhole* a radicalement changé le *phishing* classique : alors que les spams avaient habituellement un caractère urgent et pouvaient facilement être détectés, *Blackhole* utilise une méthode « douce » qui, à l'aide de nombreuses redirections web, brouille les pistes et fait passer le spam comme légitime. Dans 66% des cas, le malware utilisé était *Zeus*.

[Marketresearch] Selon une étude, le budget des organisations de Défense dédié au cyber devrait continuer de croître

Selon l'étude de Market Research intitulée *« Global Defense Survey 2012: Cyber Warfare in the Defense Industry, Threats, Opportunities, Demand and Key Market »*, le budget des organisations de Défense dédié au cyber devrait continuer de croître. En effet, si près de la moitié des organisations interrogées ont indiqué ne pas changer leur budget cyber pour l'année à venir (dénonçant l'effet de mode ou le manque de moyens), seules 2% d'entre elles souhaitent réduire ce budget. L'autre moitié des participants à l'enquête a quant à elle prévu une augmentation franche de ce budget. En moyenne, les fonds dédiés à la cybersécurité devraient ainsi croître de 6% dans l'année à venir.

[Enisa] Recommandations sur la sécurité des smart grids

La mise en place de smart grids qui visent à réguler plus efficacement les réseaux électriques implique une plus grande interconnexion de ceux-ci, notamment via Internet.

L'ENISA prévient, dans un rapport publié le 10 juillet, qu'il faut donc y associer des mesures de cybersécurité (bonnes pratiques, meilleure coopération, amélioration du partage d'informations…). Un atelier conjoint Europe/Etats-Unis sur la cybersécurité des smart grids aura lieu le 15 octobre à Amsterdam.

[stefanomele.it] Le *Department of Defense* officialise sa stratégie d'adoption du Cloud

Le *Department of Defense* américain a officialisé sa stratégie d'adoption du Cloud le 12 juillet 2012. Elle repose sur deux grands piliers : d'abord, classiquement, l'adoption d'un Cloud qui faciliterait le transfert de données et réduirait les coûts. Ensuite, des besoins en sécurité accrus, ainsi que la nécessité d'un service ininterrompu et résilient.

[McAfee] Les gouvernements et criminels se cacheraient de plus en plus derrière la façade de l'hacktivisme

François Paget (McAfee) a récemment pubié un rapport faisant un état des lieux de l'hacktivisme. Selon lui, trois types de hacktivistes se distinguent : les médiatiques (à l'image des Anonymous), les « cyberguerriers » gouvernementaux et les « vrais activistes ». L'auteur dénonce également l'instrumentalisation de ces groupes de hacktivistes par des gouvernements ou des criminels.

Rapport Bockel sur la cyberdéfense française : quels enseignements ?

> ***« (...) un beau matin les hommes découvriront avec surprise que des objets aimables et pacifiques ont acquis des propriétés offensives et meurtrières »***
> Qiao Liang et Wang Xiangsui
> La guerre hors limites, Payot et Rivages, 1999, p.58.

La première véritable prise de conscience française en matière de cyberdéfense date de 2006 avec le rapport Lasbordes : organisation dispersée, moyens insuffisants, entreprises vulnérables, le rapporteur remémore le « constat sévère » du retard initial de la France dans ce domaine. Le constat est plus ou moins similaire dans le rapport Romani de 2008, mais la publication la même année du Livre blanc sur la défense et la sécurité nationale marque « *un véritable tournant* ». La protection des systèmes d'information est reconnue comme une « *composante à part entière de notre politique de défense et de sécurité* ». Outre la création de l'ANSSI, le Livre blanc préconisait la mise en place d'une défense active[1] en plus de la traditionnelle défense passive[2] et évoque pour la première fois le développement de capacités offensives.

La création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) le 7 juillet 2009[3] est le point de départ de l'organisation de la cyberdéfense française. Son champ de compétences est vaste : sensibilisation, assistance des administrations et des opérateurs d'importance vitale, prévention de la menace, formation, élaboration du référentiel général de sécurité (RGS), détection des attaques et réactions à ces dernières.

Rédigée par l'ANSSI et publiée le 15 février 2011, la stratégie française en matière de Défense et de sécurité des systèmes d'informations est organisée autour de quatre axes et a pour ambition de faire de la France une puissance mondiale de cyberdéfense, en lui garantissant une liberté de décision grâce à la protection des infrastructures vitales de la nation et à la sécurité dans le cyberespace. Depuis, les initiatives se multiplient et les capacités françaises se renforcent. Jean-Marie Bockel cite notamment la création d'un groupe d'intervention rapide de l'ANSSI, l'adoption d'une politique visant à homogénéiser le niveau de sécurité dans les systèmes d'information de l'Etat (notamment grâce à la création d'un réseau interministériel de l'Etat résilient) et le renforcement de la coopération avec les opérateurs d'infrastructures vitales.

C'est dans ce contexte que la commission des Affaires étrangères, de la Défense et des Forces armées du Sénat a confié en octobre 2011 à Jean-Marie Bockel la rédaction du présent rapport sur la cyberdéfense, publié le 19 juillet. En février 2012, le document préparatoire à l'actualisation du Livre blanc[4] expliquait que « les risques identifiés par le Livre blanc comme étant de long terme se sont donc en partie déjà concrétisés et la menace atteint désormais un niveau stratégique », renforçant l'intérêt autour de ce rapport. De l'aveu même de Jean-Marie Bockel, le rapport sur la cyberdéfense a été pensé *« dans l'optique de l'élaboration du nouveau Livre blanc* », qui devrait paraître au début de l'année 2013. C'est pour cette raison que le rapporteur a jugé utile de formuler 10 priorités, qui ont plutôt une portée programmatique, complémentées par 50 recommandations concrètes.

[1] « La défense active implique une véritable capacité de surveillance des frontières et l'aptitude à s'adapter en permanence à une menace qui évolue de manière quotidienne ».
[2] « La défense passive peut être définie comme un simple recours aux systèmes automatiques de protection des réseaux (pares-feux, antivirus), placés à la frontière entre ceux-ci et l'extérieur ».
[3] http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212
[4] http://www.sgdsn.gouv.fr/IMG/pdf/Doc_preparatoire_LBDSN-2012_.pdf

LES 10 PRIORITÉS DU RAPPORT

Priorité n°1 : Faire de la cyberdéfense et de la protection des systèmes d'information une priorité nationale, portée au plus haut niveau de l'Etat, notamment dans le contexte du nouveau Livre blanc et de la future loi de programmation militaire. S'interroger sur la pertinence de formuler une doctrine publique sur les capacités offensives ;

Priorité n°2 : Renforcer les effectifs, les moyens et les prérogatives de l'Agence nationale de sécurité des systèmes d'information, ainsi que les effectifs et les moyens dédiés au sein des armées, de la direction générale de l'armement et des services spécialisés, et développer une véritable politique des ressources humaines ;

Priorité n°3 : Introduire des modifications législatives pour donner les moyens à l'ANSSI d'exercer ses missions et instituer un pôle juridictionnel spécialisé à compétence nationale pour réprimer les atteintes graves aux systèmes d'information ;

Priorité n°4 : Améliorer la prise en compte de la protection des systèmes d'information dans l'action de chaque ministère, en renforçant la sensibilisation à tous les niveaux, en réduisant le nombre de passerelles entre les réseaux et l'Internet, en développant les systèmes d'analyse permettant de détecter les attaques, ainsi qu'en rehaussant l'autorité des fonctionnaires de sécurité des systèmes d'information ;

Priorité n°5 : Rendre obligatoire pour les entreprises et les opérateurs d'importance vitale une déclaration d'incident à l'ANSSI en cas d'attaque importante contre les systèmes d'information et encourager les mesures de protection par des mesures incitatives ;

Priorité n°6 : Renforcer la protection des systèmes d'information des opérateurs d'importance vitale, en réduisant le nombre de passerelles entre les réseaux et l'Internet, en développant les systèmes d'analyse, en généralisant les audits, en rendant obligatoire la déclaration des processus et automates industriels connectés à Internet et en favorisant la mise en place, de manière sectorielle, de centres de détection communs ;

Priorité n°7 : Soutenir par une politique industrielle volontariste, à l'échelle nationale et européenne, le tissu industriel des entreprises françaises, notamment des PME, spécialisées dans la conception de certains produits ou services importants pour la sécurité informatique et, plus largement, du secteur des technologies de l'information et de la communication, et renforcer la coopération entre l'Etat et le secteur privé ;

Priorité n°8 : Encourager la formation d'ingénieurs spécialisés dans la protection des systèmes d'information, développer la recherche et les activités de conseil, et accentuer la sensibilisation du public, notamment au moyen d'une campagne de communication inspirée de la prévention routière ;

Priorité n°9 : Poursuivre la coopération bilatérale avec nos principaux alliés, soutenir l'action de l'OTAN et de l'Union européenne, engager un dialogue avec la Chine et la Russie et promouvoir l'adoption au niveau international de mesures de confiance ;

Priorité n°10 : Interdire sur le territoire national et à l'échelle européenne le déploiement et l'utilisation de « routeurs » ou d'autres équipements de coeur de réseaux qui présentent un risque pour la sécurité nationale, en particulier les « routeurs » et certains équipements d'origine chinoise.

Des progrès encourageants, mais une situation encore insatisfaisante, selon le rapport

Un constat sans concessions

Face à une menace réelle et protéiforme, « le dispositif français connaît encore d'importantes lacunes ».

La première partie du rapport s'attache à identifier les différentes menaces et à les illustrer par différentes situations concrètes. Les exemples cités sont bien connus du lecteur averti (l'Estonie, Stuxnet, Flame), mais permettent aux nombreux autres lecteurs de ce rapport, pas forcément familiers de ce domaine, d'avoir une entrée en matière claire. Les attaques les plus courantes sont définies (attaques par déni de service, vol de données, types de vulnérabilités), une liste des cibles potentielles est dressée (sites publics, systèmes opérationnels et détenteurs d'informations sensibles) et un profil des attaquants établis (notamment par une distinction salutaire entre les différentes types de pirates informatiques). Dans une démarche de sensibilisation, le rapporteur évoque plusieurs attaques qui ont visé la France, de la perturbation du site du Sénat au vol de données dans les systèmes d'information du ministère de l'économie ou d'AREVA.

Malgré les nombreux efforts accomplis, « *la situation de la France (…) reste insatisfaisante* », surtout en comparaison avec ses voisins allemands ou britanniques. En ce qui concerne l'ANSSI, ses attributions sont larges mais se heurteraient à deux écueils majeurs. Tout d'abord, le rapport décèle un manque d'effectivité des pouvoirs de l'Agence car « les textes ne lui reconnaissent pas l'autorité nécessaire pour assurer l'application uniforme, au sein des administrations, des règles inhérentes à la sécurité des systèmes d'information ». Ensuite, les effectifs sont largement insuffisants pour lui permettre de remplir l'ensemble de ses missions. De 250 à la fin de l'année 2012, l'ANSSI devrait compter 360 agents d'ici 2013, ce qui reste toutefois deux fois inférieur aux effectifs de ses homologues en Allemagne et au Royaume-Uni. De même, le budget de 75 millions d'euros prévu pour 2012 est inférieur à l'objectif initialement fixé de 90 millions d'euros.

En matière de sécurité, les ministères sont loin d'être exemplaires. Peu d'entre eux ont mis en place une « *véritable politique de sécurité des systèmes d'information* ». Pire, « *de nombreux ministères ne connaissent même pas la cartographie de leurs propres réseaux et ignorent souvent la finalité de leurs propres systèmes d'information* ».

Le constat est également sévère concernant les acteurs privés. De manière générale, selon le rapport, les entreprises françaises ne sont pas assez sensibilisées aux risques d'attaques informatiques. La situation est plus contrastée en ce qui concerne les opérateurs d'importance vitale[5] : si les secteurs bancaire, nucléaire et de l'aviation civile font figure de bons élèves, ce n'est pas nécessairement le cas pour les autres secteurs. A la différence des Etats-Unis et de l'Allemagne, la protection de ces infrastructures ne serait pas perçue comme prioritaire en France. Ainsi, nous ne disposons ni d'un service de protection *ad hoc* comme les israéliens, ni de systèmes permanents de protection et de détection des attaques informatiques comme les britanniques. Les opérateurs d'importance vitale ne sont pas préparés à un incident majeur sur leurs réseaux, et leurs contacts

[5] Le rapport propose la définition de la communication de la Commission européenne sur la « protection des infrastructures critiques dans le cadre de la lutte contre le terrorisme » d'octobre 2004 : « Les infrastructures critiques sont les installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements des États membres. Les infrastructures critiques se trouvent dans de nombreux secteurs de l'économie, y compris le secteur bancaire et des finances, les transports et la distribution, l'énergie, les services de base, la santé, l'approvisionnement en denrées alimentaires et les communications, ainsi que certains services administratifs de base ».

avec l'ANSSI seraient encore insuffisants. Le rapporteur considère donc que la sécurité de ces réseaux constitue « la principale lacune du dispositif français et un véritable *Talon d'Achille* ».

Prise de conscience internationale mais absence de réelle coopération.

En matière de cybersécurité, le rapport identifie trois limites à la coopération internationale :

- Le manque de confiance. On entend souvent qu'« il n'y a pas d'alliés dans le cyberespace ».
- La volonté par les Etats de préserver leur souveraineté nationale, privilégiant ainsi les relations bilatérales au cadre multilatéral
- La différence des conceptions entre, schématiquement, les Etats défenseur de la liberté sur Internet et ceux partisans d'un contrôle gouvernemental.

Au niveau international, le débat oppose principalement les pays emmenés par la Russie et la Chine, souhaitant profiter d'un texte sur la sécurité pour réglementer également le contenu de l'information, et les pays « *libéraux* », comme les Pays-Bas ou la Suède, qui défendent la liberté du cyberespace. Le rapporteur situe la France « *dans une position médiane* », favorable à un minimum de régulation mais refusant le concept de « *sécurité de l'information* ». Ce débat se transpose à l'ONU[6] et dans son organisme spécialisé, l'Union Internationale des télécommunications[7].

La collaboration internationale semble être plus fructueuse lorsqu'elle porte sur des aspects plus précis, comme la mise en place d'un groupe international permettant aux différents CERT (Computer emergency response team) du monde entier d'échanger entre eux. Le FIRST (Forum of incident response and security teams) réuni à ce jour plus de 250 CERT. Une structure informelle similaire a été établie par certains pays européens, dont la France : l'EGC (European government computer security incident response team).

Au niveau militaire, l'OTAN s'est longtemps contentée de protéger ses systèmes. Mais l'épisode estonien l'a confrontée à une question très complexe : « *quelle attitude adopter pour répondre à des cyberattaques lancées contre l'un des Etats membres ?* ». La question n'a toujours pas de réponse claire, mais depuis l'OTAN s'est dotée d'une politique « *globale* » en matière de cyberdéfense, notamment en ce qui concerne l'assistance en cas d'attaque contre un allié, et organise des exercices. La création d'une nouvelle agence en charge de la sécurité des systèmes d'informations et des communications de l'OTAN est également d'actualité. Enfin, le rapporteur évoque la création d'un centre d'excellence sur la cyberdéfense, homologué par l'OTAN, auquel participent sept pays alliés, et regrette que la France n'en fasse pas partie.

Au niveau régional, le rapporteur a constaté l'adoption « *de nombreux documents d'orientations ou de programmes* », mais qui se contentent de fixer « *des objectifs très généraux* », ne paraissant pas « *en mesure de se traduire rapidement par des initiatives concrètes* ». Trois raisons sont identifiées : l'absence de stratégie globale à l'échelle européenne, la dispersion d'acteurs insuffisamment coordonnés, et un manque d'efficacité. En outre, si l'agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) s'est vue attribuée des missions « *très vastes* », une évaluation externe demandée par la Commission a souligné ses carences. Le constat du rapporteur est donc cinglant : « *à l'image de l'OTAN, l'Union européenne ne paraît pas encore en mesure d'assurer la protection de l'ensemble de ses propres réseaux et systèmes d'information* ».

[6] Avec les débats autour de l'adoption de mesures non-contraignantes sous formes de « bonnes pratiques ».

[7] A travers le souhait du secrétaire général de l'UIT, soutenu par la Russie et la Chine, d'accroître le rôle de l'organisation en matière de cybersécurité au niveau international.

Des perspectives d'amélioration

En plus d'établir un constat riche et varié de la situation française et internationale en matière de cyberdéfense, le rapport est force de propositions et formule cinquante recommandations.

Etat

Le maître mot du rapport au niveau national est la reconnaissance de la cyberdéfense comme « *priorité nationale, portée au plus haut niveau de l'Etat* » (recommandation n°1).

Aux dires du rapport, les capacités de l'ANSSI sont déjà très satisfaisantes au regard de ses moyens. Il s'agit désormais de renforcer ses pouvoirs quant aux acteurs publics et aux opérateurs d'importance vitale (recommandation n°4) et de « *donner à l'ANSSI (…) les moyens d'exercer [ses] missions » (recommandation n°3). La politique de sécurité doit essaimer au sein de l'Etat, en développant les pratiques de « labellisation* » et de « *certification* » (recommandation n°5) et en favorisant le recrutement de spécialistes de la sécurité informatique (recommandation n°6).

En ce qui concerne le ministère de la Défense, il s'agit de continuer le mouvement initié depuis le Livre blanc de 2008 : *« poursuivre et amplifier les moyens techniques et humains consacrés à la cyberdéfense au sein des armées, de la DGA et des services spécialisés* » (recommandation n°7), « *conforter et approfondir la nouvelle organisation de cybersécurité mise en place au sein du ministère de la défense* » (recommandation n°8) et « *poursuivre le développement de capacités offensives au sein des armées et des services spécialisés* », tout en s'interrogeant sur la « *pertinence d'un discours public, voire d'une doctrine publique* » sur ces capacités (recommandation n°10).

En revanche, le rapport appelle à une modification des pratiques en cours dans les autres ministères afin de faire de la protection des systèmes d'information une « *véritable priorité* » (recommandation n°11). Outre l'accroissement de la sensibilisation (recommandation n°15), la tenue d'une « *cartographie à jour de son propre réseau et de son système d'information* » devrait être obligatoire (recommandation n°12). Le rapport suggère également de « *rehausser l'autorité et le rôle des fonctionnaires de la sécurité des systèmes d'information* » afin de leur donner du poids dans les projets informatiques des administrations (recommandation n°13). Le rapporteur encourage la poursuite des efforts en matière de résilience, avec la poursuite de « *la mise en place du Réseau Interministériel de l'Etat* » (recommandation n°14) et la création d'un « *pôle juridictionnel spécialisé à compétence nationale* ».

Entreprises et opérateurs d'importance vitale

Pour les entreprises, le rapport recommande également que la sécurité devienne une priorité, en rendant obligatoire une « *déclaration d'incident à l'ANSSI en cas d'attaque importante* » (recommandation n°17), en incitant à rehausser « *le niveau hiérarchique et le rôle* » des RSSI (recommandation n°18) et en invitant les entreprises aux dialogues avec les compagnies d'assurance (recommandation n°19) et avec l'ANSSI (recommandation n°20). Le second volet vise à encourager le développement d'un tissu industriel (recommandation n°21), notamment à l'export (recommandation n°23), et les activités de conseil et d'assistance (recommandation n°22).

Dans le cas particulier des opérateurs d'importance vitale, les recommandations sont similaires mais beaucoup plus précises en ce qui concerne l'obligation de déclaration d'incident à l'ANSSI (recommandation n°24) et la coopération avec l'ANSSI : cartographie obligatoire, audit annuel, déclaration des SCADA connectés à Internet

auprès de l'ANSSI (recommandation n°26). Le rapport appelle à une sécurité très poussée pour ces opérateurs, suggérant notamment l'introduction d'un « *système de surveillance de flux permettant de déceler les attaques informatiques (…) et favoriser le [leur] groupement autour de système de détection partagés opérationnels 24/24* » (recommandation n°25).

Le renforcement des effectifs ne peut se faire sans l'augmentation du nombre de spécialistes en sécurité formés (recommandation n°27) et le renforcement des activités de recherche et développement (recommandation n°28). Plus généralement, la sécurité informatique doit faire l'objet d'un *« plan de communication inspiré du plan de prévention de la sécurité routière* » (recommandation n°29).

International

Outre une plus grande coopération bilatérale avec le Royaume-Uni (recommandation n°31) et l'Allemagne (recommandation n°32), le rapport recommande de développer des liens avec « *les CERT gouvernementaux et militaires* » (recommandation n°30), et plus largement avec tous les pays intéressés, que ce soit pour « *promouvoir le modèle français de gouvernance en matière de cybersécurité* » (recommandation n°33) ou « *mettre en place des dialogues stratégiques bilatéraux avec les pays pouvant jouer un rôle particulier en matière de cyberattaques à l'encontre de nos intérêts nationaux* » (recommandation n°34).

Au niveau des organisations internationales, le rapport appelle à la clarification de la doctrine de l'OTAN (recommandation n°37), recommande une présence française dans le centre d'excellence de Tallinn (recommandation n°38) et invite à une plus grande coopération avec l'UE (recommandation n°36). En ce qui concerne l'UE justement, une réforme de l'ENISA est primordiale « *pour en faire un outil efficace* » (recommandation n°40). La stratégie européenne se doit également d'être plus « *lisible* » (recommandation n°39) : le renforcement de la « *coopération industrielle européenne* » (recommandation n°42), ainsi que la réflexion autour de l'adoption de normes juridiques (recommandation n°43) et l'interdiction des équipements cœurs de réseaux « *à risque* » - notamment les composants chinois - (recommandation n°44) sont autant de pistes à explorer avec nos partenaires européens.

Tout en recommandant un dialogue « *franc et ouvert* » avec la Chine et la Russie (recommandation n°46), le rapport s'oppose à « *la reconnaissance d'un fondement juridiquement contraignant à l'action de l'UIT sur la cybersécurité (…) et à un rôle opérationnel en ce domaine* » (recommandation n°47). Idem devant l'ONU, la France doit « *défendre l'idée d'un code de bonne conduite (…) plutôt qu'un traité international ou un texte international juridiquement contraignant* » (recommandation n°45).

Le rapport de Jean-Marie Bockel "*La cyberdéfense : un enjeu mondial, une priorité nationale*" est disponible en PDF sur le site du Sénat.

Point juridique sur la publication de failles de sécurité

S'il est possible d'informer le public sur l'existence d'une vulnérabilité, il ne faut pas que cette information permette d'exploiter des failles de sécurité informatique, sauf motif légitime.

Fin avril 2012, un chercheur a révélé l'existence de portes dérobées[8] dans les produits de la société RuggedCom, utilisés dans les réseaux de systèmes critiques. Cet accès, laissé volontairement par le fabricant, aurait pu permettre à des hackers de s'introduire dans les systèmes, d'autant plus que les clients n'étaient pas informés de l'existence de cet accès. Le chercheur a diffusé publiquement l'information après avoir sollicité en vain RuggedCom et l'ICS-CERT (CERT des systèmes de contrôle industriel du *Department of Homeland Security* américain). Suite à ces révélations, la société RuggedCom a annoncé procéder rapidement à la correction des failles existantes[9].

Comme l'illustre cet exemple, la recherche de failles dans des systèmes informatiques est l'une des activités les plus appréciées parmi les communautés de hackers, de pentesteurs et autres experts de sécurité informatique. Mais qu'advient-il une fois que ces derniers ont trouvé des vulnérabilités dans les systèmes ?

« White Hat » : entre « full » et « responsible disclosure »

Il existe plusieurs chapelles parmi les passionnés de sécurité informatique. Certains vont informer le propriétaire du site internet, ou l'éditeur du logiciel, de l'existence de cette faille afin que ce dernier la corrige au plus vite : c'est ce qu'on appelle un « *white hat* »[10]. Parmi ceux-ci, certains sont partisans du « *full disclosure* » ou divulgation complète, alors que d'autres prônent le « *responsible disclosure* » ou divulgation responsable. La différence entre les deux positions tient à l'étendue des informations révélées. Dans le cas de la divulgation « complète », toutes les informations connues concernant la faille sont publiées, y compris les « *exploits* », c'est-à-dire les moyens d'exploiter la faille. L'idée est que la faille sera plus rapidement prise au sérieux et corrigée si toutes les données à son sujet sont rendues publiques. Les partisans de la divulgation « responsable » choisissent de laisser un certain temps à l'intéressé pour corriger la faille, et s'ils choisissent de divulguer l'existence d'une faille, ils ne fournissent en principe pas les « *exploits* ». D'autres enfin estiment qu'effectuer une divulgation complète mais dans un cercle d'initiés restreints constitue également une « *responsible disclosure* ».

Comment la loi appréhende-t-elle la publication de failles de sécurité informatique ?

Un texte ambigu

L'article 323-3-1[11] du Code pénal sanctionne *« le 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 ou plusieurs des infractions prévues par les articles 323-1 à 323-3 »*, c'est-à-dire le fait d'accéder, de se maintenir frauduleusement, d'entraver, de fausser le fonctionnement ou d'introduire des données dans un systèmes de traitement automatisé de données [STAD]. Ce comportement « *est puni des peines*

[8] http://seclists.org/fulldisclosure/2012/Apr/277

[9] http://www.wired.com/threatlevel/2012/04/ruggedcom-to-fix-vuln/

[10] Les « black hats » ne sont pas directement concernés par les problématiques de publication des failles. En effet, ces derniers ont tout intérêt à conserver les failles inconnues afin de pouvoir les exploiter en toute tranquillité.

[11] http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418323&cidTexte=LEGITEXT000006070719&dateTexte=20120601&oldAction=rechCodeArticle

prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée », c'est-à-dire au maximum 7 ans de prison et 100 000€ d'amende.

Introduit par la Loi pour la Confiance dans l'Economie Numérique (LCEN) du 21 juin 2004 afin de sanctionner la production et la détention de virus informatiques, ce texte transpose l'article 6[12] de la Convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001. En plus d'une dizaine d'année, ce texte a été ratifié par 33 pays et signé par 14 autres[13]. Au total, ce sont plus de 120 pays qui collaborent de près ou de loin avec le Conseil de l'Europe pour lutter contre la cybercriminalité.

Quels outils sont visés par le texte ?

De nombreuses inquiétudes ont traversé le milieu de la sécurité informatique à l'époque, car beaucoup se sont interrogés sur le champ d'application, assez large, de cet article. Par exemple, quels outils informatiques remplissent les conditions énumérées par les articles 323-1 et suivants ? Le texte évoque les outils *« conçus ou spécialement adaptés »* pour commettre des atteintes au STAD, critère qui, pour être apprécié, nécessiterait de se mettre à la place du concepteur du programme. A cette analyse subjective plutôt délicate, certains commentateurs, comme le professeur Agathe Lepage[14], proposent ainsi de substituer une analyse du potentiel du logiciel à porter atteinte au STAD. Ainsi, des informations d'ordre général, ne permettant pas de perturber le fonctionnement des systèmes, ne devrait pas en principe être visées par le texte : indiquer l'existence d'une faille n'est pas une infraction. En revanche si les informations sont « *accessibles à tous [et permettent] d'exploiter des failles de sécurité informatique* »[15], c'est-à-dire si l'on divulgue les « *exploits* », l'article 323-3-1 du Code pénal est applicable.

Quelle définition pour le « motif légitime » ?

La question de la définition du motif légitime se pose également. L'article 6 de la Convention sur la cybercriminalité exclut la responsabilité pénale en cas de diffusion ou de mise à disposition d'un dispositif permettant une infraction informatique lorsque ces dernières « *n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique* ». Pour le professeur Agathe Lepage, le motif légitime doit également être entendu de façon à « *tenir compte des nécessités de la recherche ou de la sécurité informatique* »[16].

On peut donc légitimement penser que la finalité de sécurité informatique entre dans la définition du motif légitime évoqué dans l'article 323-3-1 du Code pénal. Mais ce constat amène plusieurs interrogations :

- d'une part, est-ce que le motif légitime se limite à la sécurité informatique ? Ne peut-on pas imaginer que le droit à l'information constitue un motif légitime de possession ou de diffusion d'un des outils incriminés par

[12] Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesres législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit:
a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition:
i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus;
ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,
dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5; et
b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.
2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.
3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

[13] http://pvynckier.blog.estjob.com/index.php/post/2012/06/09/Convention-sur-la-cybercriminalit%C3%A9-%3A-une-protection-pour-vous-et-pour-vos-droits

[14] A. Lepage, La Semaine Juridique Edition Générale n°1, 11 janvier 2010, 19

[15] Cass. Crim, 27 octobre 2009, 09-82346

[16] Ibid.

l'article 323-3-1 du Code pénal ? Le fait d'être professionnel de la sécurité informatique dispense-t-il l'intéressé d'apporter la preuve de son motif légitime ?

- d'autre part, doit-on apprécier la « finalité de sécurité informatique » de façon directe ou indirecte ? En effet, le motif légitime ne manquera pas d'être invoqué de façon indirecte par certains « *white hat* » pour justifier des « *full disclosure* ». Leur raisonnement sera de justifier des divulgations complètes en expliquant que ces dernières placent les titulaires des droits sur les sites ou les logiciels vulnérables dos au mur, et les oblige à intervenir car la faille est accessible à n'importe quel « *script kiddies* »[17].

Une jurisprudence qui ne dissipe pas les interrogations

La Cour de cassation s'est pour la première fois prononcée sur l'appréciation de l'article 323-3-1 du Code pénal dans un arrêt du 27 octobre 2009, qui a largement fait parler de lui à l'époque. Les faits sont assez simples. Un professionnel de la sécurité informatique, gérant d'une société dans le domaine, avait publié sur son site internet « *des scripts permettant d'exploiter des failles de sécurité informatique, directement visibles sur le site et accessibles à tous* ». Les services de l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) avisent alors le parquet de Montpellier, qui décide d'engager des poursuites. Après une décision favorable en première instance, le professionnel est condamné le 12 mars 2009 par la Cour d'appel de Montpellier. Il forme alors un pourvoi qui est rejeté par la Cour de cassation.

Premier constat, l'article 323-3-1 du Code pénal peut s'appliquer à la publication de failles informatiques accompagnées de leur « *exploits* », c'est-à-dire du moyen d'exploiter la faille, et pas uniquement à la détention de virus. Pour autant, tous les experts en sécurité informatique, qui souvent possèdent et utilisent de tels outils, pourraient-ils être poursuivis sur le même fondement ?

Le cœur du débat était de déterminer ce qui constituait un motif légitime de diffusion de la vulnérabilité. Le professionnel expliquait en effet qu'il avait agi ainsi afin de « *remédier à une insécurité informatique* », et invoquait un « *motif légitime tiré de la volonté d'information* ». Il faisait sien l'adage selon lequel « la fin justifie les moyens », et estimait donc que le « *full disclosure* » était le meilleur moyen d'obtenir de bons résultats en matière de sécurité informatique. Avançant comme argument qu'il avait été remercié par MICROSOFT pour son travail, il omettait cependant de préciser que ces remerciements étaient intervenus à propos d'une autre faille, dont il avait averti la firme de Redmond par mail, sans divulguer d'information au public. En outre, dans l'affaire qui nous intéresse, il ne se contentait pas de signaler publiquement l'existence d'une vulnérabilité (ce que le site « Zataz » fait régulièrement), mais il mettait à disposition des visiteurs de son site les « *exploits* ». Il s'agissait donc d'un « *full disclosure* », car les informations permettait d'exploiter la faille et étaient « *directement visibles sur le site et accessibles à tous* ».

Et c'est sur ce point précis que la Cour fonde sa décision, car « *du fait de son expertise en la matière, il savait qu'il diffusait des informations présentant un risque d'utilisation à des fins de piratage par un public particulier en recherche de ce type de déviance* ».

C'est la position classique du droit français qui présume que les professionnels sont nécessairement des personnes averties de leurs obligations, de sorte que s'ils violent la loi, cette violation est nécessairement consciente. En aurait-il été autrement s'il ne s'était pas agi d'un professionnel ? Peut-être, mais qui d'autre qu'un professionnel, ou du moins un amateur éclairé, pourrait découvrir et mettre en ligne des vulnérabilités informatiques ?

[17] http://fr.wikipedia.org/wiki/Script_kiddie

Le portail OMC
La nouvelle plateforme de la DAS

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

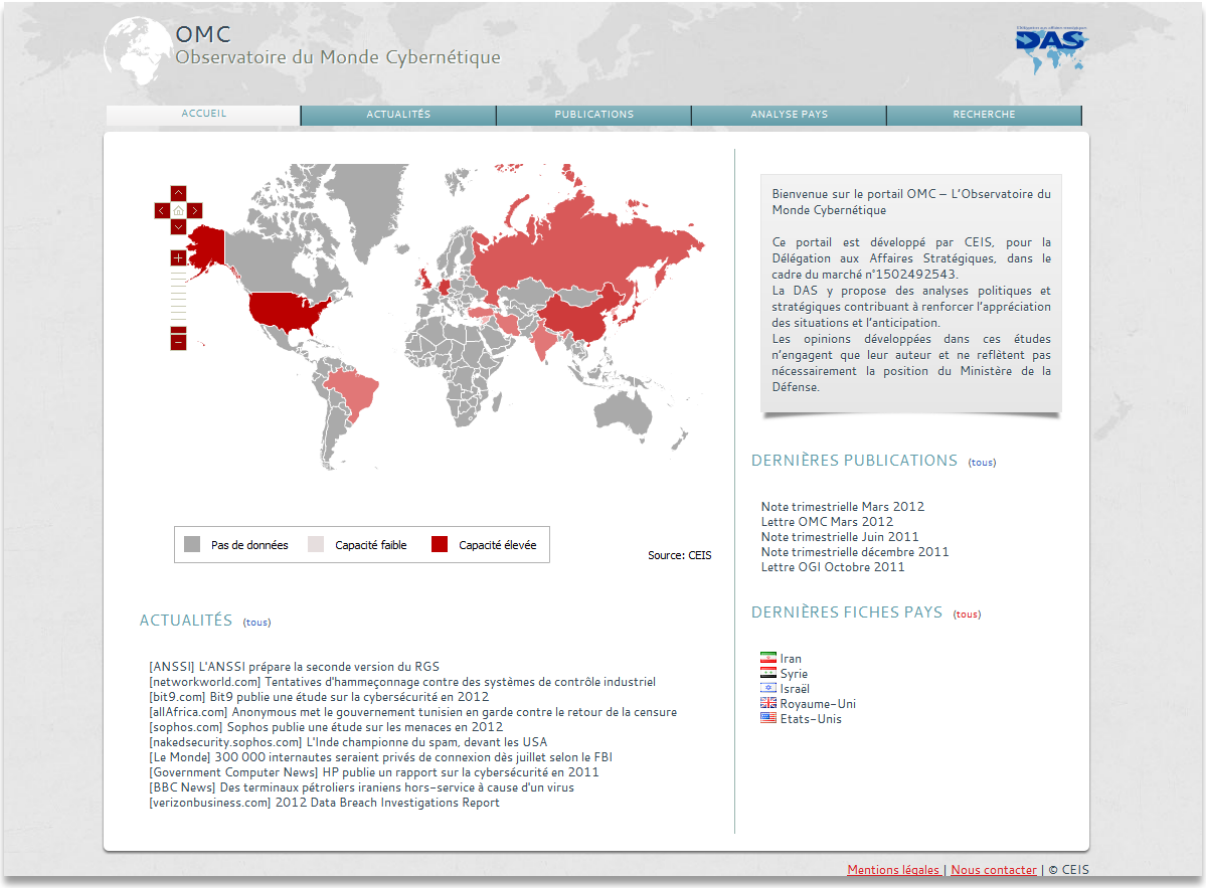

Figure 1 - Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Petit Déjeuner SecurityVibes	Paris (France)	20 septembre
ISC Cloud 12 Mannheim	Allemagne	24-25 septembre
InfoSecurity International Summit 2012	Shanghai (Chine)	25 – 26 septembre
Le futur de votre patrimoine applicatif, la nouvelle dimension GCOS 7	Paris (France)	27 septembre
VMworld EMEA	Barcelone (Espagne)	9-11 octobre
SC12	Salt Lake City (Etats-Unis)	10-16 Novembre
Forum pour la Gouvernance d'Internet	Bakou (Azerbaïdjan)	Novembre
Global CyberLympics	En ligne	Courant 2012 (non encore précisé)

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