Observatoire du Monde Cybernétique

Lettre n°19 – Juillet 2013

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

[Assemblée Nationale] Audition de M. Patrick Pailloux (directeur général de l'ANSSI) sur la cyberdéfense

M. Patrick Pailloux a été auditionné à l'Assemblée Nationale, le mardi 16 juillet, par la Commission de la défense nationale et des forces armées, sur les questions de cyberdéfense. Le directeur général de l'ANSSI a rappelé aux députés les trois principales menaces « cyber » (espionnage, déstabilisation et cybersabotage). Il a également dressé les grands enjeux des travaux préparatoires au livre blanc, rappelant la nécessité d'accroître les prérogatives étatiques en la matière.

[Rennes Atalante] DGA Maîtrise de l'information : 200 nouveaux postes « cyberdéfense » d'ici à 2017

DGA Maîtrise de l'information verra ses effectifs renforcés de 200 personnes au cours des 5 prochaines années grâce aux nouveaux investissements de l'État français dans la cyberdéfense. Les crédits d'étude alloués par la DGA en cybersécurité seront eux aussi fortement augmentés. Ils permettront de renforcer les partenariats avec les laboratoires de recherche et les entreprises de défense et de sécurité du domaine « cyber », avec un soutien accru aux PME innovantes.

[Europa] Adoption d'une directive renforçant la protection contre les cyberattaques

Le Conseil de l'Europe a adopté un nouveau texte afin de renforcer la lutte contre la cybercriminalité. De nouvelles infractions ciblent spécifiquement les cyberattaques à grande échelle. Le texte souhaite également améliorer la coopération entre les Etats membres en les obligeant à traiter les demandes urgentes dans les huit heures.

[ENISA] Accord de collaboration entre l'ENISA et les corps de standardisation européens CEN et CENELEC

L'ENISA a signé un accord de coopération avec le Comité Européen de Normalisation (CEN) et le Comité Européen de Normalisation en Electronique et en éLECtrotechnique (CENELEC). Objectif : mieux comprendre les enjeux liés à la standardisation afin d'améliorer la compétitivité des produits et services de cybersécurité européens.

[Reuters] Mise en accusation de hackers dans la plus grande affaire de fraude sur Internet

Cinq hackers ont été mis en accusation pour leur responsabilité présumée dans des fraudes aux cartes bancaires qui auraient coûté plus de 300 millions de dollars aux banques, ainsi que pour avoir décelé une faille de sécurité considérable dans le Nasdaq. Cette affaire est décrite comme « la plus grande affaire de fraude sur Internet ».

[LeFigaro] L'hébergeur français OVH victime d'un piratage

L'hébergeur français OVH a été victime d'un piratage majeur ayant exposé les données de ses clients européens. L'hébergeur a notamment invité ses clients à modifier leur mot de passe. Pour arriver à ses fins, un pirate aurait obtenu le mot de passe d'un employé d'OVH, se serait introduit dans le réseau privé virtuel d'OVH et aurait pu ainsi accéder aux dossiers internes, se procurant les données des clients européens de la société (près de 700.000 clients à travers le monde). Aucune donnée bancaire n'a cependant été volée.

[LesEchos] Comment le cloud français compte tirer profit du scandale Prism

L'affaire Prism risque de renforcer les craintes des entreprises européennes à l'égard des hébergeurs de données américains, bien que les géants américains aient tenté de rassurer leurs clients. Nombre d'entreprises s'inquiètent désormais de savoir comment sont gérées leurs données informatiques, qu'elles travaillent avec des entreprises américaines ou non.

Les opérateurs de cloud français espèrent tirer profit de la situation. Ils y voient un nouveau

moyen de justifier leur positionnement, basé sur l'argument de « souveraineté des données ».

[GOV.uk] Royaume-Uni : un partenariat de défense s'occupe des risques de cybersécurité

Le ministère de la Défense britannique s'associe au secteur privé pour créer un partenariat de cybersécurité censé renforcer la protection nationale contre les cyberattaques. Baptisé Defence Cyber Protection Partnership (DCPP), sa mission première sera de réduire les menaces pesant sur les fournisseurs du ministère de la Défense.

[InfosDefense] Le Pentagone va recruter 4 000 cyber-spécialistes

Le secrétaire d'Etat adjoint américain à la Défense, Ashton Carter, a annoncé une nouvelle vague de recrutement de spécialistes informatiques pour le DoD. 4 000 cyber-spécialistes vont ainsi être recrutés au sein du cybercommand et de la NSA. Au total, 40 cyber-équipes seront créées dont 13 dédiées à la mise au point de nouveaux outils et 27 à la défense des structures informatiques américaines.

[Defense Systems] L'US Navy consacre 900 M$ pour la cyberdéfense

Booz Allen Hamilton, CACI Technologies, IncComputer Sciences, General Dynamics, Honeywell Technology Solutions, IncEngility, Lockheed Martin, Science Applications International, Scientific Research, Secure Mission Solutions, STG, Systems Research and Applications and URS Federal Services ont remporté un contrat pour un montant de 900 millions $ en vue de mettre en place des solutions de cyberdéfense au sein du Naval Warfare Systems Center.

[Homeland Security News Wire] La Maison Blanche veut jouer sur les assurances pour encourager le respect des règles en matière de cybersécurité

La Maison Blanche élabore des règles visant à réduire le montant des assurances payées par les opérateurs d'importance vitale afin d'encourager le respect des futures règles relatives à la cybersécurité des entreprises.

[RTNews] Anonymous annonce une opération globale le 5 novembre 2013

Le groupe Anonymous a publié une vidéo appelant les citoyens du monde entier à un jour de désobéissance civile générale, le 5 novembre prochain (anniversaire du jour où Guy Fawkes a tenté de faire exploser la Chambre des Lords en 1605). Le groupe encourage à une vague de cyberattaques sur tous les gouvernements du monde. Le même appel il y a un an avait généré plusieurs cyberattaques.

[AgenceEcofin] Rwanda : Le gouvernement démarre une campagne de sensibilisation sur la cybercriminalité

Le Rwanda a lancé une campagne de sensibilisation des populations quant aux délits commis en ligne. Près de 6,7 millions € ont été alloués pour cette opération de sensibilisation pour l'année 2013/2014.

[Telecompaper] L'Ouganda et la Corée du Sud signent un pacte de régulation internet

Les gouvernements ougandais et sud-coréen ont signé un accord de coopération pour aider l'Ouganda à développer des politiques de gestion de sécurité de l'information. L'Agence coréenne d'Internet et de Sécurité (KISA) apportera son expérience en la matière pour permettre à l'Autorité Nationale ougandaise des Technologies de l'Information (NITA) de développer son CERT et son infrastructure à clés publiques (PKI). En avril 2013, la Corée du sud avait signé un accord similaire avec le Rwanda.

[Bloomberg] Les Emirats Arabes Unis déjouent une série d'attaques contre des sites gouvernementaux

Les Emirats Arabes Unis ont subi le 19 juillet une série de cyberattaques contre des sites gouvernementaux. Lancées depuis l'Egypte, les attaques n'auraient fait que peu de dégâts. Le pays s'est dit prêt à collaborer avec les autorités égyptiennes pour identifier les assaillants, grâce une liste d'adresse IP identifiées.

[Intelligence Online] Les Emirats Arabes Unis investissent dans une capacité industrielle locale en matière de cybersécurité

Les Emirats veulent développer une capacité industrielle locale en matière de cybersécurité et de renseignement électronique. Dans ce but, Mubadala ICT, la branche « technologie » du fonds souverain d'Abou Dhabi, ainsi qu'Invest AD, un autre fonds de l'émirat, se sont associés au fonds américain Paladin Capital Group pour prendre des participations dans des sociétés de sécurité informatique. Le principal responsable des investissements technologiques chez Paladin est l'ancien directeur de la NSA, Kenneth Minihan.

[The Voice of Russia] La Russie adoptera un nouveau "concept" de cybersécurité

La Russie prévoit d'établir et ratifier un document fondateur qui constituera la base des politiques publiques du pays en matière de cybersécurité. Le Président russe Vladimir Poutine avait récemment exprimé la nécessité pour la Russie d'éradiquer les cybermenaces. Ce document sera intitulé "Les Fondations de la Politique de l'Etat russe dans la Sphère de la Sécurité Internationale de l'Information".

[Dawn] Pakistan : un plan d'action de cybersécurité en 7 points

Le Comité de Défense et de Production de Défense du Sénat pakistanais a élaboré et proposé, en partenariat avec l'Association Pakistanaise de Sécurité de l'Information (PISA), un plan d'action de cybersécurité en 7 points. Il est notamment proposé d'adopter un corpus législatif de cybersécurité et d'établir un CERT pakistanais. Une entité joignant les forces des ministères de la Défense, des Technologies de l'Information, de l'Intérieur, des Affaires Etrangères et de professionnels de la sécurité privée sera créée, ainsi qu'un CyberCommand interservices pour les forces armées pakistanaises. Des pourparlers doivent également être engagés avec les huit pays de l'Association sud-asiatique pour la coopération régionale (SAARC), particulièrement l'Inde.

[Reuters] Taiwan : un terrain d'essai pour la cyberarmée chinoise

La quantité et la diversité des cyberattaques subies par Taïwan depuis une dizaine d'années laissent penser à leurs experts que l'île est devenue un terrain d'essai pour la Chine. Les signatures d'attaques subies se retrouvent notamment quelques mois après dans des offensives menées contre les Etats-Unis, confirmant l'idée de phases de tests contre Taïwan. Les dégâts restent les mêmes et la perte de données subie par Taïwan serait considérable.

[Channel News Asia] Singapour lance un plan quinquennal de cybersécurité

Singapour a lancé un plan de cybersécurité sur cinq ans, pour faire du pays un carrefour informatique de confiance d'ici 2018. Les secteurs privés et publics (mais aussi les citoyens) collaboreront pour gérer les cybermenaces. La base de spécialistes en cybersécurité à Singapour devrait dépasser les 1 500. Ce plan a été annoncé à l'occasion de la journée nationale de sensibilisation à la cybersécurité.

[01Net] Japon : des documents « sensibles » publiés par erreur sur Google Groupes

Des responsables du ministère nippon de l'Environnement ont utilisé les paramètres par défaut de Google Groupes, permettant ainsi au public d'accéder à des documents internes, relatifs à des négociations internationales sur le commerce du mercure avec leurs partenaires suisses et

norvégiens. Ils n'étaient pas top-secret, mais n'auraient pas du être publiés.

[InfoWorld] McAfee découvre une campagne de cyberespionnage contre la Corée du Sud

Les attaques remarquées en mars 2013 contre des banques et média sud-coréens n'auraient été que le point culminant d'une plus large campagne de cyberespionnage, baptisée Operation Troy. C'est la société McAfee qui en a fait la découverte. Depuis 2009, les attaquants utilisaient un réseau d'espionnage militaire sophistiqué pour dérober des documents tagués des mots « U.S. army », « nord », « arme » ou « défense ». McAfee n'a pas pu déterminer si les deux groupes à l'origine des attaques les plus récentes, New Romantic Cyber Army Team and the Whois Hacking Team, étaient affiliés à un quelconque Etat.

[Assemblée Nationale] Audition de l'ingénieur en chef de l'armement Guillaume Poupard, responsable du pôle de sécurité des systèmes d'information de la DGA

Dans le cadre de la préparation de la prochaine Loi de Programmation Militaire, la Commission de la Défense de l'Assemblée nationale a procédé le 10 juillet dernier à l'audition de Guillaume Poupard, responsable du pôle de sécurité des systèmes d'information à la DGA. Cette audition portait sur le rôle et l'organisation de la DGA en matière de cyberdéfense ainsi que sur les perspectives ouvertes en la matière par le Livre blanc.

Guillaume Poupard a présenté aux députés l'organisation de la DGA en matière de cyberdéfense, les liens de la DGA avec l'ANSSI, la coordination de la DGA avec des laboratoires de recherche et les activités de la DGA en matière de sécurité des systèmes d'information. Il a ensuite énoncé les besoins de la DGA en matière de cyberdéfense : disposer d'industriels de confiance capables de réaliser les systèmes de la DGA, d'experts très pointus et de formation de niveau inférieur à ce qui existe aujourd'hui. Les députés ont enfin interrogé Guillaume Poupard sur la possibilité de construire une Europe de la cyberdéfense, sur la protection des données et la sécurité des systèmes d'information des entreprises.

[ANSSI] L'observatoire de la résilience de l'Internet français publie son rapport annuel

L'observatoire de la résilience de l'Internet français vient de publier son rapport annuel. Concernant BGP, l'étude des 1270 acteurs français identifiés a mis en évidence une forte diversité. Il existe par conséquent peu d'opérateurs dont la panne affecterait une part significative de l'Internet français. Les analyses concernant DNS révèlent en revanche une concentration importante au niveau des hébergeurs et des résolveurs des FAI. Cette double concentration laisse à penser qu'une défaillance d'un acteur important de la communauté DNS pourrait avoir un impact significatif sur le fonctionnement de l'Internet français.

[CSO] Les places financières exposées aux cyberattaques

Un rapport du Research Department of the International Organization of Securities Commissions (IOSCO) et de la World Federation of Exchanges (WFE) révèle que 53% des places d'échanges mondiales ont subi une cyberattaque l'année passée. 93% des 46 places d'échanges interrogées confirment discuter de cybersécurité et en faire une priorité au sein du top-management. Leur capacité de détection et de réaction est estimée à 48 heures.

[Lloyd] La cybercriminalité est la 3ème priorité des PDG

Selon une étude menée par Lloyd sur 588 professionnels, les menaces que représentent la cybersécurité sont passées à la troisième position dans les préoccupations des dirigeants en 2013, alors qu'en 2009 et 2011, ces menaces occupaient respectivement la vingtième et douzième place.

[McAfee] La cybercriminalité coûterait jusqu'à 500 milliards de dollars par an à l'économie globale

McAfee estime le coût annuel de la cybercriminalité pour l'économie globale à entre 100 et 500 milliards de dollars. A titre de comparaison, cette fourchette haute est le coût estimé du trafic de drogue. Ne serait-ce qu'aux Etats-Unis, 500 000 pertes d'emploi seraient des conséquences indirectes de la cybercriminalité, en raison des pertes causées par le vol de propriété intellectuelle, par la divulgation de stratégies confidentielles et par des conséquences réputationnelles.

[Akamai] L'Indonésie rejoint la Chine en tête des foyers de cyberattaques

Selon un rapport d'Akamai Technologies, l'Indonésie était à l'origine de 21% des cyberattaques mondiales au cours du premier trimestre de l'année 2013, prenant la deuxième place derrière la Chine (34%). Ce chiffre intrigue puisqu'il était seulement d'un pour cent au dernier trimestre 2012. L'explication résiderait dans le type d'activité observée, suggérant une attaque agressive par botnet, englobant un nombre conséquent d'ordinateurs. Les Etats-Unis occupent la troisième place (8,3%) suivis de la Turquie et la Russie.

[OCDE] L'OCDE publie un rapport sur la déclaration de Séoul sur le futur de l'économie Internet

L'OCDE a publié un rapport portant sur l'examen de la déclaration ministérielle de Séoul de 2008 sur le futur de l'économie Internet dans l'ensemble des sept thématiques identifiées dans la proposition sur les « Suites à donner à la Déclaration ministérielle de Séoul sur le futur de l'économie Internet ».

.

Amérique latine et Caraïbes : une dynamique de cybersécurité enclenchée

Dans un rapport intitulé *« Latin American and Caribbean Cybersecurity Trends and Government Responses »*, Trend Micro, en collaboration avec l'Organisation des Etats Américains (OAS), réalise un état des lieux du traitement des cyber-risques par les Etats de l'OAS. Parfois sous-estimés, ces Etats semblent pourtant au cœur une dynamique de cybersécurité bien enclenchée.

Figure 1. Page de garde, rapport précité.

Fondée en 1948, l'Organisation des Etats Américains (OAS) est l'institution régionale la plus ancienne du monde. Cette organisation a été créée afin d'atteindre un *« ordre de paix et de justice, de maintenir [la solidarité entre les pays de l'OAS], de renforcer leur collaboration et de défendre leur souveraineté, leur intégrité territoriale et leur indépendance »*[1]. L'OAS regroupe aujourd'hui l'ensemble des 35 Etats indépendants des Amériques[2] et constitue la principale tribune gouvernementale du Continent pour les questions d'ordre politique, juridique et social. La sécurité figure parmi un des quatre objectifs de l'OAS et les Etats membres se soutiennent mutuellement sur ces questions à travers le dialogue politique, la coopération et les instruments juridiques.

Des sources et des définitions hétérogènes

La plupart des données sont issues des CERT nationaux et des unités de police spécialisées dans la lutte contre la cybercriminalité. Une des difficultés rencontrées lors de cette étude a été de recueillir des données issues d'acteurs n'utilisant pas une terminologie harmonisée.

De manière générale, l'ensemble des pays interrogés a connu une hausse des incidents en matière de cybersécurité durant l'année 2012. Cette hausse intervient alors même que beaucoup de pays se sont dotés de capacités de lutte contre la cybersécurité et ont formés leurs personnels à ce phénomène. Deux interprétations sont alors possibles. La première est que l'amélioration des capacités de détection et de traitement des incidents expliquerait cette augmentation. La seconde, que cette hausse serait bien plus importante en l'absence du déploiement de nouveaux moyens de lutte.

Les infrastructures sensibles et le système bancaire de plus en plus visés

En 2012, 51 fournisseurs de systèmes de contrôles industriels - tous pays confondus - ont rapporté près de 170 incidents. Phénomène nouveau pour certains des pays interrogés, le secteur de l'énergie et celui de la finance connaissent de plus en plus d'attaques. Nombre d'auteurs ont été arrêtés et condamnés pour ces attaques.

Les attaques visant à générer des gains financiers sont également en hausse. La principale raison de cette augmentation repose sur le faible niveau de protection des établissements, la plupart des banques utilisant

[1] Article 1er, charte OAS
[2] http://www.oas.org/fr/etats_membres/default.asp

un système d'authentification simple. Il existe un véritable **marché noir** pour la revente des informations bancaires et de nombreux post sur des forums en accès libre proposent ainsi la vente de telles informations.

Parmi les menaces les plus importantes, l'**hacktivisme** constitue également un risque majeur et a été à l'origine de nombreuses attaques, souvent menées en représailles ou en contestation de certains projets de loi portant la propriété intellectuelle ou la taxation de certains produits.

Enfin, les *spyware* sont de plus en plus utilisés par les réseaux de crime organisé traditionnels alors que les *spam* ont quant à eux diminués, grâce aux opérations de destructions de *botnet* menées par les autorités répressives.

La lutte contre la cybercriminalité : des approches variées mais cohérentes

Tandis que certains avancent des raisons de sécurité et de défense nationale, d'autres justifient leur démarche de cybersécurité par la crainte des risques pour le développement et économique et la compétitivité des Etats. Deux approches différentes mais complémentaires. Beaucoup de pays ont adopté un cadre législatif portant sur la cybercriminalité, créant ainsi des procédures spécifiques qui n'existaient pas jusque-là. De même, la plupart des pays membres ont entamé la création d'un CERT national. De récentes révélations sur les vulnérabilités d'infrastructures critiques ont en effet poussé les Etats à prendre de nouvelles initiatives, à l'image du Panama qui a développé une stratégie de protection des infrastructures critiques.

Des efforts communs

Les Etats membres de l'OAS font preuve d'une mise en commun des efforts dans la lutte contre la cybercriminalité : alors que l'Union européenne vient d'adopter une stratégie en la matière, l'OAS s'est dotée dès 2004 d'une stratégie interaméricaine unifiée en matière de cybersécurité. Cette dernière a été complétée par une déclaration en mars 2012 portant sur le renforcement de la cybersécurité en Amérique. En outre, d'un point de vue opérationnel, le Secrétariat général de l'OAS fournit aux Etats membres une assistance technique et participe à l'amélioration du niveau de cybersécurité des Etats de l'OAS. Des accords bilatéraux concernant la cyberdéfense existent, à l'exemple du Brésil[3] ou du Chili[4] qui ont renforcé leur coopération militaire avec les Etats-Unis en avril 2012. La collaboration entre les pays de l'OAS a également permis à un groupe de pays (Brésil, Argentine, Chili, Pérou et Uruguay) d'empêcher le géant du web Amazon à obtenir le nom de domaine ".amazon" auprès de l'ICANN au motif que le terme "amazon" représente un large territoire qui s'étend sur plusieurs pays[5].

[3] http://www.defense.gov//news/newsarticle.aspx?id=116075
[4] http://www.defense.gov//news/newsarticle.aspx?id=116102
[5] http://bits.blogs.nytimes.com/2013/07/18/amazon-rejected-as-domain-name-after-south-american-objections/?ref=technology

Focus par pays

Mexique
Le Mexique est le pays ayant connu la plus forte augmentation du nombre de cyberattaques, principalement menées par des hacktivistes et dirigées contre des institutions publiques. Les attaques les plus importantes ont été dirigées contre des sites gouvernementaux, notamment ceux créés spécialement pour les élections présidentielles qui se sont tenues en juillet 2012. Le Mexique s'est doté d'un centre de coordination et de prévention des crimes électroniques, remplaçant ainsi le Secrétariat général de la sécurité publique sur le sujet. Tout comme la Jamaïque, le Mexique s'est doté d'une Task Force rattachée directement au Gouvernement.

Jamaïque
La Jamaïque a connu une augmentation de 14% d'incidents en raison du manque de personnels dédiés à ces problématiques et à la mauvaise formation de ceux existant. En outre, une mauvaise coopération au niveau interne et avec des acteurs internationaux contribue à la vulnérabilité du pays. Pour y remédier, la Jamaïque a adopté en 2012 une nouvelle législation qui étend les compétences de l'unité judiciaire en matière de cybercriminalité et de communications (UFCU). Dans le même temps, une Task Force au niveau national a été mise en place.

Panama
Le Panama est un des pays qui a fourni le plus d'informations. Les attaques les plus répandues sont les opérations de défacement (27%), les attaques par déni de services (23%) et l'utilisation frauduleuses de comptes personnels (15%). La plupart des cyberattaques subies par le Panama ont été menées au quatrième trimestre 2012, ce qui correspond à l'entrée en vigueur d'une loi qui renforce la protection de la propriété intellectuelle. En mars 2013, le Panama a adopté une stratégie nationale de cybersécurité et de protection des infrastructures critiques. Le Panama s'est porté candidat à l'adhésion de la convention de Budapest.

Brésil
Le Brésil a annoncé en août 2012 le développement d'un nouveau logiciel pour la sécurité et la prévention des cyberattaques. Cette démarche s'inscrit dans la volonté du gouvernement de développer la cyberdéfense du pays, en particulier concernant les informations sensibles.

Chili et Colombie
Le Chili et la Colombie sont les seuls pays à avoir connu une baisse des incidents au cours de l'année 2012. Le Chili a attribué la baisse de la cybercriminalité au démantèlement d'un syndicat responsable de la distribution d'un malware ciblant les données bancaires et personnelles. La Colombie quant à elle a connu une diminution des incidents grâce à la mise en place d'un CERT et d'unités de police spécialisées. La Colombie a été à l'initiative de l'opération « Unmask » qui visait à mettre fin à une vague d'attaques menée contre les infrastructures critiques colombiennes et chiliennes. Cette opération, à laquelle ont participé l'Argentine, le Chili, la Colombie et l'Espagne, a été couronnée de succès en aboutissant à l'arrestation de 25 personnes et à la saisie de 250 ordinateurs. La Colombie s'est dotée en 2011 d'une stratégie de cybersécurité et de cyberdéfense connue sous le nom de CONPES 3701. Cette stratégie a mis en place 3 entités : une unité de police, un centre de commandement et un CERT.

Argentine
L'Argentine est un des pays les plus avancés en la matière : après avoir créé le Bureau national des technologies de l'information (NOIT), elle a mis en place l'ArCERT en 2005. Pour parer aux attaques contre les infrastructures critiques, elle s'est également dotée en 2012 d'un programme de protection dédié. L'Argentine vient également de mettre en place son second plan pour la cybersécurité nationale et la protection des infrastructures critiques pour les années 2013-2015.

Figure 2. Caraïbes et Amérique du Sud - http://www.populationdata.net/

Les Etats-Unis mettent à jour leurs règles d'engagement dans le cyberespace

"We now live in a world of weaponized bits and bytes, where an entire country can be disrupted by the click of mouse. There are new missions we must take on as a military, and steps we must take as a nation, to defend ourselves from this threat"[6].

Le 27 juin dernier, lors d'une conférence devant la Brookings Institution, le Général Martin E. DEMPSEY, *Chairman of the Joint Chiefs of Staff*, annonçait la publication prochaine de nouvelles règles d'engagement pour le cyberespace.

Les règles d'engagement *"sont des directives adressées aux forces militaires (individus inclus) qui définissent les circonstances, les conditions, le degré et la manière à respecter pour pouvoir ou non faire usage de la force, ou effectuer des actions qui pourraient passer pour des provocations"*[7]. Elles ont donc pour objet de permettre au commandement militaire de contrôler l'usage de la force à chaque échelon. Déterminées par des facteurs politiques, juridiques (elles doivent respecter le droit national ainsi que le droit international) et militaires, elles constituent un cadre général et sont précisées pour chaque opération. Aux Etats-Unis, elles sont contenues dans le document CJCS Instruction 3121.01B qui date du 13 juin 2005 et qui est classifié.

La multiplication du nombre de cyberattaques ainsi que l'implication croissante d'acteurs étatiques dans leur conduite ont amené les responsables américains à qualifier le cyberespace de cinquième espace de bataille. Au regard du caractère stratégique du cyberespace, des discussions au sein de l'administration américaine ont été entamées dès 2010 afin d'actualiser les règles d'engagement. Cette mise à jour s'inscrit dans le contexte général d'évolution de la politique américaine dans le cyberespace, notamment dans le domaine militaire. Ainsi, Barack OBAMA a demandé que soit dressée une liste de cibles étrangères potentielles dans le cyberespace afin que des actions offensives puissent être menées[8].

Plusieurs points ont été particulièrement discutés lors des négociations sur les nouvelles règles d'engagement. Tout d'abord, la question du niveau d'agressivité pouvant être toléré dans le cyberspace semble avoir été un des points d'achoppement des discussions[9]. De même, celle de la décentralisation du niveau d'autorisation a suscité des débats, l'objectif étant de garder un contrôle politique important dans la mise en œuvre des actions (offensives) dans le cyberespace. Enfin, ces règles d'engagement devaient s'intégrer dans la politique globale du cyberespace dessinée par la *Stratégie Internationale du Cyberespace* publiée par la Maison Blanche en mai 2011.

---

[6] General Martin E. DEMPSEY, "Defending the Nation ar Network Speed", 27 juin 2013, disponible sur http://www.brookings.edu/~/media/events/2013/6/27%20cybersecurity%20dempsey/martin%20e%20dempsey%20prepared%20remarks.pdf

[7] OTAN, *MC 362/1 "Règles d'engagement de l'OTAN"*, 30 juin 2003, disponible sur http://www.cicde.defense.gouv.fr/IMG/pdf/20030630_np_otan_mc-362-1-nato-rules-of-engagement.pdf

[8] Glenn GREENWALD, Ewen MACASKILL, "Obama orders US to draw up overseas target list for cyber-attacks", *The Guardian*, 7 juin 2013, disponible sur http://www.guardian.co.uk/world/2013/jun/07/obama-china-targets-cyber-overseas?INTCMP=SRCH

[9] Zachary FRYER-BIGGS, "Slowed by Debate and Uncertainty, New Rules Green Light Response to Cyber Attacks", *Defense News*, 27 mai 2013, disponible sur http://www.defensenews.com/article/20130527/DEFREG02/305270014/Slowed-by-Debate-Uncertainty-New-Rules-Green-Light-Response-Cyber-Attacks

Aujourd'hui, toute action dans le cyberespace requiert l'autorisation du Conseil national de sécurité de la Maison Blanche. Les nouvelles règles d'engagement devraient identifier les autorités au sein du Département de la défense pouvant autoriser le recours à des mesures de défense active dans le cyberespace, les actions préventives restant l'apanage de la Maison Blanche. L'utilisation d'armes cybernétiques restera sous la responsabilité de l'USCYBERCOM mais les commandements militaires géographiques pourront lui demander un soutien pour mener leurs actions[10].

Lors de la conférence donnée devant la Brookings Institution, le Général Martin E. DEMPSEY a présenté la façon dont une cyberattaque substantielle serait traitée par les Etats-Unis si une infrastructure d'importance vitale était attaquée par un botnet situé à l'extérieur des Etats-Unis. La première étape serait d'amasser des informations sur celui-ci afin de le connaître pour bloquer l'attaque (défense passive). Si cela n'était pas suffisant, les nouvelles règles d'engagement devraient permettre de recourir à des mesures de défense active, c'est-à-dire autoriser la désactivation du botnet (ce qui suppose d'intervenir sur une machine se trouvant hors des Etats-Unis). Enfin, en cas d'inefficacité, des consultations inter-agences et l'autorisation des plus hautes autorités seraient nécessaires pour attaquer des cibles afin de mettre fin à la cyberattaque.

Les conséquences de l'élaboration de nouvelles règles d'engagement sont doubles. Au plan interne, elles peuvent avoir pour objectif de dissuader les acteurs privés de mener leurs propres actions pour se défendre dans le cyberespace, l'administration assurant cette fonction. De plus, la décentralisation des niveaux de décision va permettre une réaction plus rapide en cas de cyberattaque.

Si les règles d'engagement sont traditionnellement à destination des forces armées, la création de nouvelles règles pour le cyberespace vient modifier cette situation. Leur élaboration est caractérisée par un changement dans la façon de travailler du Département de la défense. En effet, la communauté du renseignement s'est impliquée de façon très active dans la rédaction de ces règles[11], le Général Keith B. ALEXANDER, directeur de la NSA et chef de l'USCYBERCOM, ayant eu une place prépondérante[12]. De plus, les destinataires de ces règles d'engagement sont plus nombreux, les personnels de l'Agence nationale de sécurité étant amenés à intervenir avec les forces armées dans le cyberespace. On assiste donc à une montée en puissance spectaculaire de la communauté du renseignement qui vient concurrencer l'action des forces armées dans ses champs d'intervention. Ainsi, l'écriture de ces nouvelles règles d'engagement pour le cyberespace vient bouleverser les prérogatives des responsables de la défense de l'Etat.

Au plan international, les conséquences politiques, diplomatiques et militaires sont également très importantes. L'élaboration de nouvelles règles participe en effet à la normalisation de la cyberguerre, d'autres Etats pouvant alors invoquer le précédent américain pour aborder publiquement l'élaboration de leurs propres règles d'engagement dans le cyberespace. Dans un contexte de tensions internationales sur ces questions, cette annonce renforce donc le risque d'escalade d'un conflit en cas de cyberattaque majeure.

[10] Jorge BENITEZ, "New Rules Will Allow Military Commanders to Counterattack Foreign Cyber Threats", *NATO Source Alliance News Blog*, 28 mai 2013, disponible sur http://www.acus.org/natosource/new-rules-will-allow-military-commanders-counterattack-foreign-cyber-threats

[11] General Keith B. ALEXANDER, "Statement before the Senate Committee on Armed Services", 27 mars 2012, disponible sur http://www.airforcemag.com/SiteCollectionDocuments/Reports/2012/March2012/Day28/032812alexander.pdf

[12] Zachary FRYER-BIGGS, "Slowed by Debate and Uncertainty, New Rules Green Light Response to Cyber Attacks", *op. cit*.

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

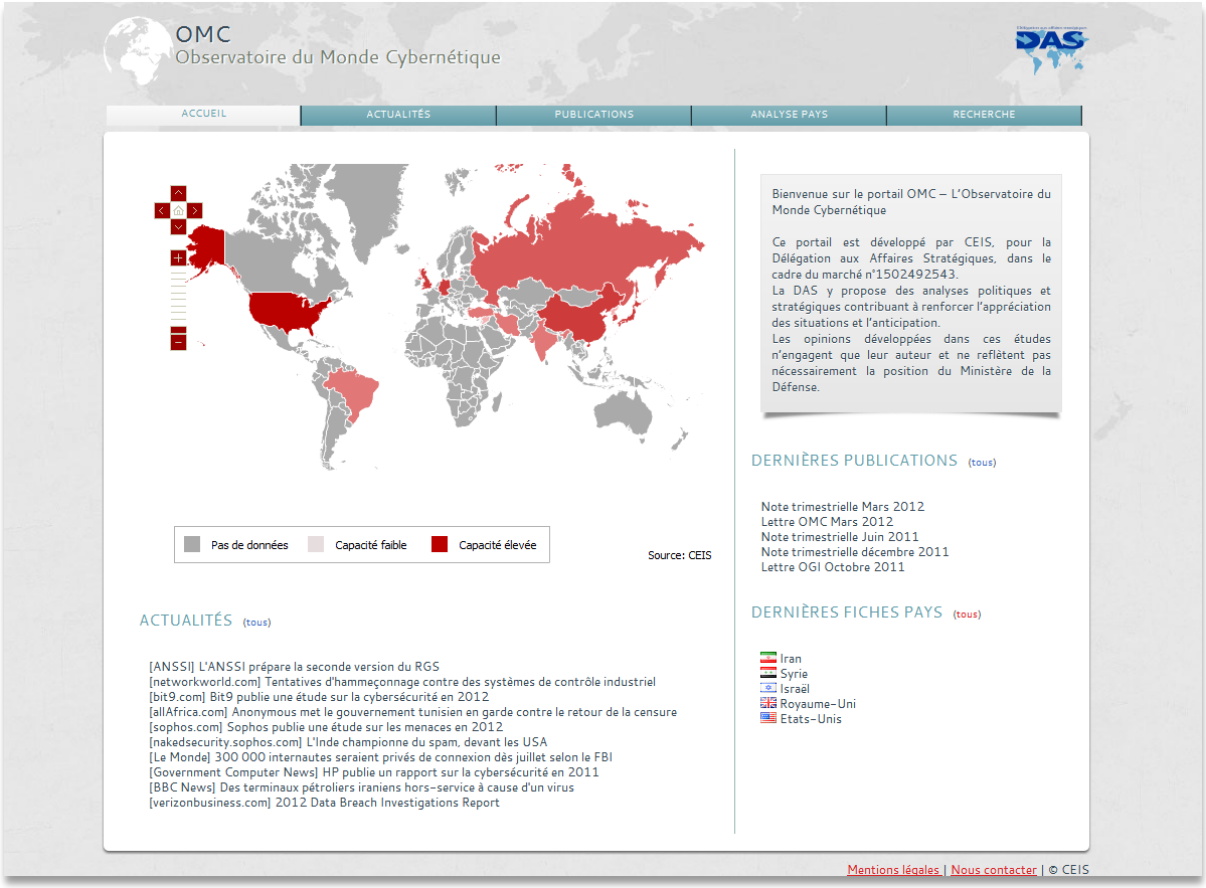

Figure 3. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Black Hat Training & Briefings USA 2013	Las Vegas (USA)	27 juillet - 1er août
DEFCON	Las Vegas (USA)	1 - 4 Août
Secutech Vietnam	Vietnam	8 - 10 août
GS Mag : Le Data Center de demain	Paris	17 septembre
Cyber Intelligence Europe	Bruxelles	17 – 19 septembre
Trophées de la Sécurité	Paris	23 septembre
Cyber Security for the Chemical/Petrochem Industry	Texas, Etats-Unis	24 - 25 septembre
Cyber Intelligence Europe	Bruxelles	17 – 19 septembre
Mois de la Cybersécurité	Europe	Octobre

CEIS

Compagnie Européenne
d'Intelligence Stratégique

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

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