Observatoire du Monde Cybernétique

Lettre n°5 - Mai 2012

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

Vers la création d'une NSA à la française ?

Le chef du service technique de la DGSE envisagerait de créer un nouveau service de renseignement aux compétences exclusivement techniques, sur le modèle du GCHQ britannique ou de la NSA américaine.

Cette structure interministérielle verrait rassemblées, en une seule entité, toutes les capacités techniques dont disposent la DGSE et la DRM.

Infosecurity Europe 2012 : Neelie Kroes détaille la stratégie européenne de cybersécurité

La stratégie de sécurité paneuropéenne sur Internet décrite par Neelie Kroes, commissaire européenne chargée de la société numérique, implique de profondes transformations. Selon elle, la cybersécurité ne peut être laissée aux seules agences de sécurité nationale tandis que le cyberespace ne peut se résumer à un nouveau théâtre de guerre. Un nouveau Forum Européen contribuerait à la création d'une nouvelle structure de gouvernance, qui s'assurerait de la centralisation et du partage d'informations entre Etats membres.

Neelie Kroes propose l'obligation de notification des failles de sécurité en entreprise, une augmentation du budget de l'UE consacré à la cybersécurité ainsi qu'une coopération globale afin de s'assurer de la sécurité des produits informatiques entrant dans l'UE.

L'Europe protège ses SCADAs et ses smart grids avec Crisalis

La Commission européenne a financé à hauteur de 3,4 millions d'euros, sur 5,3 millions d'euros de budget total, le programme Crisalis (Critical Infrastructure Security Analysis) qui vise à améliorer la détection des intrusions et la protection des réseaux SCADA et des smarts grids. Piloté par Symantec et l'Université de Twente (Pays-Bas), ce projet réunit deux opérateurs électriques (Enel et Alliander), ainsi que Siemens, dont les produits avaient été la cible du virus Stuxnet.

Le ministre de l'Intérieur allemand souhaite pour une coopération internationale renforcée

Le ministre de l'Intérieur allemand Hans-Peter Friedrich a plaidé, en introduction d'un discours à Washington le 2 mai 2012, en faveur d'une coopération internationale renforcée en matière de lutte contre la cybercriminalité, contre le cyberterrorisme et pour la protection des infrastructures d'importance vitale.

Le ministre a rappelé qu'un groupe d'experts des Nations Unies commencera à développer, dès cet été, des solutions communes.

Flame, un ver bien plus complexe que Stuxnet ou Duqu

Kaspersky et l'Union internationale des télécommunications (UIT) ont récemment annoncé la découverte de « Flame ». Véritable cyberarme, ce ver posséderait un code vingt fois plus complexe que ses prédécesseurs Stuxnet ou Duqu.

Visant principalement les terminaux du Moyen-Orient (Cisjordanie, Iran, Liban), le malware est capable de voler des données sensibles, notamment en capturant l'écran, les frappes du clavier ou le son du microphone de sa cible.

Le secteur maritime victime tant des pirates informatiques que des pirates physiques

Les pirates qui sévissent dans le Golfe d'Aden ont de plus en plus recours au renseignement, voire au piratage informatique, pour préparer leurs attaques.

Profitant du fait que les armateurs et les spécialistes de la sécurité maritime sont peu conscients de ces risques, les pirates réussissent généralement à se procurer des informations capitales en ligne : cargaison du bateau, présence d'une escorte, d'hommes armés, itinéraire, etc.

Élévation du statut de l'unité de cyberguerre américaine

Le général américain Martin Dempsey, président des chefs d'état-major des armées, prône l'élévation du statut de l'unité de cyberguerre à celui de commandement de combat à part entière. Cette initiative confirme la stratégie des États-Unis, visant à projeter des forces militaires dans le cyberespace à des fins de dissuasion. Même si des efforts diplomatiques sont menés en parallèle afin d'apaiser les tensions avec leurs adversaires. La question de la légitimité d'une cyberattaque, dans le cadre de la défense « active », reste cependant non résolue.

Les Etats-Unis développent des règles d'engagement dans le cyberespace

Le chef du Cyber Command américain a déclaré que le lancement d'une cyberattaque par les Etats-Unis ne pourrait avoir lieu sans l'approbation des plus hauts responsables américains. Il a par ailleurs écarté l'hypothèse d'un scénario catastrophe dans lequel des pirates réussiraient à attaquer le réseau électrique américain. Le Département à la Défense réfléchirait à la définition de règles d'engagement à destination des officiers.

Le FBI crée le Domestic Communications Assistance Center

Le FBI a annoncé la création du DCAC, Domestic Communications Assistance Center. Ce centre serait chargé de l'interception et du décodage de communications privées, notamment sur Skype et d'autres réseaux sociaux. Très peu d'informations ont pour l'instant été rendues publiques. Le FBI sera toutefois dans l'obligation de dévoiler, trois mois après l'instauration du centre, des informations sur sa structure et ses partenaires privés.

Un nouveau « deputy commander » nommé au sein du « Fleet Cyber Command » américain

La Contre-amirale Diane E. H. Webber est nommée « deputy commander » du « Fleet Cyber Command » situé à Forte Meade, Maryland aux Etats-Unis. Elle occupait précédemment le poste de directrice des communications au sein de l'« Office of the Chief of Naval Operations » situé à Washington, D.C.

Résultats du concours national de cyberdéfense américain

La dernière édition du concours national de cyberdéfense, qui s'est tenue du 20 au 22 avril à l'Université de San Antonio, a vu la victoire pour la deuxième année consécutive de l'équipe de l'Université de Washington, suivie par l'académie de l'US Air Force et l'Université du Texas. Le Cloud computing était un des sujets phares de cette édition.

Des portes dérobées dans l'architecture de produits équipant des systèmes critiques

Un chercheur a révélé l'existence de portes dérobées dans les produits de la société RuggedCom, utilisés dans les réseaux de systèmes critiques. Cet accès, laissé volontairement par le fabricant, permettrait à des hackers de s'introduire dans les systèmes. 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 DHS américain). Suite à ces révélations, la société RuggedCom a annoncé procéder rapidement à la correction des failles existantes.

Des iraniens auraient pénétré le système d'un drone américain

Selon le général Amir Ali Hajizadeh, des scientifiques iraniens auraient réussi à pénétrer le système interne du drone que Téhéran a annoncé avoir capturé en décembre 2011. Pour étayer son affirmation, le général a révélé certaines informations secrètes sur le parcours du drone, des missions auxquelles il aurait participé, ainsi que des périodes pendant lesquelles il aurait été placé en maintenance. Le débat est toujours vif autour de la capture de ce drone, à la fois sur le type d'équipement qu'il embarquait et sur la possibilité d'en tirer des informations stratégiques.

Les Etats-Unis renforcent leur coopération avec le Chili et le Brésil

La cybersécurité était au cœur de la dernière rencontre entre les ministres de la Défense brésilien et américain. Le ministre de la Défense américain, Leon Panetta, a estimé que la collaboration dans ce domaine serait profitable pour les deux nations. Le sujet était également au cœur des discussions lors d'une rencontre avec son homologue chilien, Andrés Allamand.

Rapprochement entre les Etats-Unis et les Philippines

Le ministre de la Défense américain, Leon Panetta a déclaré que la coopération avec les Philippines allait être renforcée afin, notamment, d'aider Manille à se défendre contre les attaques de hackers se revendiquant Chinois.

Projet de « téléphone rouge » entre le Kremlin et la Maison-Blanche

Les Etats-Unis et la Russie discutent la mise en place d'un moyen de communication sécurisé permettant de désamorcer les éventuelles tensions dues à des incidents informatiques, sur le modèle éprouvé du « téléphone rouge » utilisé pour éviter les conflits nucléaires. Cet accord serait le premier du genre entre les USA et un autre pays. Les discussions entre Washington et Pékin avancent quant à elles bien plus lentement. Les Chinois auraient refusé d'appliquer les principes d'usage proportionné de la force et de minimisation des dégâts civils au cyberespace.

Les Etats-Unis encouragent l'Inde à renforcer sa cybersécurité

Les Etats-Unis ont encouragé l'Inde à renforcer ses capacités en cybersécurité. L'Inde accueille en effet les « back-offices » d'un grand nombre d'entreprises américaines. Autant de succursales qui représentent des points d'entrée dans les réseaux des entreprises dont le siège social serait situé aux Etats-Unis. L'Inde devrait en ce sens améliorer ses capacités de détection et d'investigation des cybercrimes.

La Russie et l'Abkhazie signent un accord de coopération dans le domaine des TIC

La Russie et l'Abkhazie ont signé un accord de partenariat stratégique dans le domaine des TIC, a annoncé le service de presse du ministère des Communications de la Fédération de Russie. Le document a été signé par Igor Shchegolev, adjoint du ministre des Communications de la Russie et un représentant du chef de l'Abkhazie, Christian Bzhania.

L'Inde et le Japon renforcent leur collaboration en matière de cybersécurité

L'Inde et le Japon ont entamé le 6ème round d'un dialogue visant à renforcer leur coopération stratégique, notamment en matière de cybersécurité.

Cette initiative pourrait déboucher sur une coopération régionale associant la Corée du Sud, les Philippines, la Thaïlande, voire l'Australie.

La Chine maintient ses efforts en matière de cyberguerre

D'après un rapport du département américain de la Défense, la Chine poursuivrait ses investissements dans le développement de capacités de lutte informatique défensive et offensive. L'étude rappelle que la Chine développe également ses forces nucléaires, ses missiles balistiques conventionnels et de croisière, ses forces aériennes, marines, sous-marines, en plus de ses capacités de cyberguerre.

Cette modernisation militaire devrait lui permettre de mener un large éventail de missions dans le futur. Selon Gary Li, analyste défense à Londres, ce rapport est cependant *« étrangement court »*, car comportant peu de données quantifiées.

[ENISA] L'ENISA publie un document sur les stratégies de cybersécurité

Dans un document publié le 8 mai, l'ENISA fait le point sur les stratégies de cybersécurité de différents pays européen et non-européens (tels que les Etats-Unis, le Canada et le Japon). L'agence identifie leurs points communs, leurs différences et formule plusieurs recommandations. Ce document est la première étape de la rédaction d'un guide de bonnes pratiques prévu pour fin 2012.

[Group-IB] Lancement de Global Security Map

Group-IB et HostExploit ont annoncé le lancement du projet « Global Security Map ». Ce classement de pays liste 219 pays en termes de cybercriminalité. La Lituanie est classée première. D'après les chercheurs, le principal problème des pays baltes est la forte concentration de centres de contrôle des botnets tels que Zeus et Citadel.

[GAO] Les cybermenaces visant les Etats Unis

Selon un rapport du GAO (Government Accountability Office) américain, les Etats-Unis font face à un éventail de cybermenaces en perpétuelle évolution. Ces menaces sont d'autant plus importantes que les systèmes gouvernementaux sont vulnérables. Les attaques sur ces systèmes auraient augmenté de 680 % au cours des 6 dernières années.

[Gartner] Le marché des passerelles Web sécurisées

Dans son étude sur le marché des passerelles Web sécurisées réalisée au premier trimestre 2012, le cabinet Gartner estime que la détection de malwares représente un différentiateur clé sur ce marché, tandis que les capacités de détection de trafic sortant malveillant sont rares. La catégorisation d'URLs représente également une forte valeur ajoutée et ne devrait pas être considérée comme un service trivial. Le contrôle d'application et les politiques de gestion des réseaux sociaux représentent des axes prioritaires pour les entreprises. Ces dernières attendent, par ailleurs, des passerelles sécurisées qu'elles possèdent des fonctionnalités de reporting et soient aisées à administrer. Les spécifications à venir se focaliseront sur la mobilité et les plateformes distinctes des PCs. L'intérêt pour les technologies DLP et les applications dans le Cloud computing progresse, mais reste faible.

En revanche, Gartner observe un intérêt croissant pour les applications virtuelles. Enfin, les passerelles Web sécurisées et les firewalls restent à ce jour peu intégrés.

[PandaLabs] Rapport du premier trimestre 2012

Pour le premier trimestre 2012, le laboratoire PandaLabs conclut que les chevaux de Troie représentent 80 % des six millions de nouvelles menaces créées, précédant les vers, à 9,3 %, et les virus à 6,43 %. Le pourcentage moyen d'ordinateurs infectés dans le monde est de 35,51 %, soit trois points de moins qu'en 2011, selon les données collectées par le système d'Intelligence Collective Antimalware de Panda Security. La Chine est de nouveau le pays le plus infecté (avec 54,25 % d'ordinateurs compromis), suivie par Taïwan et la Turquie. Parmi les 10 pays les moins infectés, on compte le Japon et 9 pays européens, dont les moins touchés sont la Suède, la Suisse et la Norvège.

Le rapport traite également des récentes attaques sur les systèmes Android, de la propagation de codes malveillants sur Facebook, de l'affaire MegaUpload, de la cyberguerre et des dernières actions des groupes Anonymous et LulzSec. Il conclut que la tendance des années passées se poursuit en 2012, les cybercriminels continuant *« à recourir à tous les moyens possibles et imaginables pour mettre la main sur les données et l'argent des internautes »*.

CISPA et la difficile conciliation entre cybersécurité et respect de la vie privée

Alors que les remous suscités par les projets de loi SOPA[1] et PIPA[2] commencent à s'estomper, un nouveau texte, CISPA, fait polémique. Le Cyber Intelligence Sharing and Protection Act ou « H.R. 3523 », s'il est adopté, encouragera et favorisera les échanges entre les agences de sécurité gouvernementales américaines et les entreprises privées, afin d'améliorer la lutte contre la cybercriminalité.

112TH CONGRESS
1ST SESSION

H. R. 3523

To provide for the sharing of certain cyber threat intelligence and cyber threat information between the intelligence community and cybersecurity entities, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

NOVEMBER 30, 2011

Mr. ROGERS of Michigan (for himself, Mr. RUPPERSBERGER, Mr. KING of New York, Mr. UPTON, Mrs. MYRICK, Mr. LANGEVIN, Mr. CONAWAY, Mr. MILLER of Florida, Mr. BOREN, Mr. LOBIONDO, Mr. CHANDLER, Mr. NUNES, Mr. GUTIERREZ, Mr. WESTMORELAND, Mrs. BACHMANN, Mr. ROONEY, Mr. HECK, Mr. DICKS, Mr. MCCAUL, Mr. WALDEN, Mr. CALVERT, Mr. SHIMKUS, Mr. TERRY, Mr. BURGESS, Mr. GINGREY of Georgia, Mr. THOMPSON of California, Mr. KINZINGER of Illinois, Mr. AMODEI, and Mr. POMPEO) introduced the following bill; which was re-

Figure 1. Projet de loi CISPA

Mais ce partage d'informations au profit de la cybersécurité, qui pouvait être considéré comme bénéfique, fait l'objet de vives contestations, tant de la part des défenseurs récurrents de la vie privée que des plus hautes instances politiques américaines. L'administration Obama s'oppose en effet fermement à ce projet de loi.

Un objectif louable : le partage d'informations comme outil de lutte contre les cybermenaces

Le principe de CISPA est simple : protéger les Etats-Unis des cybermenaces en améliorant le partage d'information. Le texte permettra à des entreprises privées telles que Facebook ou Google de partager avec le gouvernement et les agences de sécurité américaines tous types d'informations (historiques de recherche, contenus d'emails, etc.). En échange de quoi, le gouvernement les avertira de l'apparition et de la détection de nouvelles menaces informatiques.

Dans sa première version, le projet permettait de libérer les entreprises de certaines contraintes réglementaires quant au partage des informations[3]. Concrètement, si elle avait été adoptée sous sa forme initiale, la loi aurait ôté toute responsabilité juridique aux entreprises s'agissant de la surveillance des utilisateurs « à risque ».[4]

Ce système a initialement recueilli le soutien de près de 800 entreprises privées telles que Facebook, AT & T, Intel, Verizon et Microsoft. La remise des données au gouvernement leur permettrait en effet de renforcer leurs mesures de sécurité par la mise en œuvre de nouvelles ressources et outils gouvernementaux. Comme l'indique Facebook dans un billet publié le 13 avril dernier : *« une défense réussie […] exige […] [que la société ait] des renseignements pertinents sur les cybermenaces. [...] Quand une entreprise détecte une attaque, un partage rapide d'informations avec d'autres entreprises peut aider à protéger ces autres sociétés et leurs utilisateurs et leur éviter d'en être victimes [à leur tour]. De*

[1] Stop Online Piracy Act, http://thomas.loc.gov/cgi-bin/bdquery/z?d112:h.r.3261:

[2] PROTECT IP Act

3 http://news.cnet.com/8301-31921_3-57414992-281/cispa-gets-a-rewrite-but-still-threatens-americans-privacy/

4 http://www.technolog.msnbc.msn.com/technology/technolog/facebook-cool-cispa-how-about-you-719091

même, si le gouvernement est informé d'une intrusion ou d'une autre attaque, [s'il partage cette information] avec des entreprises privées […], meilleure est la protection des utilisateurs et de nos systèmes »[5].

« La cybersécurité passe avant tout par le partage d'information »

C'est ce qu'a pu rappeler l'ENISA dans son rapport « Incentives and Challenges for Information Sharing in the Context of Network and Information Security ». La méthode est éprouvée et reconnue par tous comme étant une étape majeure de la mise en œuvre d'une politique de cybersécurité.

Mais, surtout, l'étude rappelle que ce partage d'informations doit s'inscrire dans un cadre précis. Selon l'ENISA, en effet, la création d'infrastructures spécifiques telles que des centres d'analyse et de partage d'informations s'impose. L'Agence insiste également sur la nécessité d'une classification des informations par criticité et/ou sensibilité. Elle souligne, enfin, que l'encouragement de nature financière et l'accès à des données de qualité en retour restent, pour les acteurs privés, les deux éléments incitatifs majeurs.

Notons que 6% des acteurs craignent la mise en cause de leur responsabilité en cas de divulgation de données nominatives ou confidentielles.

Un projet pourtant largement critiqué

1. Un champ d'application dépassant le simple cadre de la cybersécurité : une entorse au « IV^{ème} amendement » ?

Un amendement apporté au texte prévoit que ces échanges d'informations serviraient en cas de cybermenace, mais aussi pour la protection des individus « de la mort ou de sérieuses blessures », des mineurs et pour la « sécurité nationale des Etats-Unis ». Ce qui n'est pas sans rappeler les dispositions controversées du Patriot Act[6].

"(1) LIMITATION.-The Federal Government may use cyber threat information shared with the Federal Government in accordance with subsection

(b) - (A) for cybersecurity purposes;

(B) for the investigation and prosecution of cybersecurity crimes;

(C) for the protection of individuals from the danger of death or serious bodily harm and the investigation and prosecution of crimes involving such danger of death or serious bodily harm;

(D) for the protection of minors from child pornography, any risk of sexual exploitation, and serious threats to the physical safety of such minor, including kidnapping and trafficking and the investigation and prosecution of crimes involving child pornography, any risk of sexual exploitation, and serious threats to the physical safety of minors, including kidnapping and trafficking, and any crime referred to […]; or

(E) to protect the national security of the United States".

Voir : Amendment to the rules committee print of H.R. 3523

Le projet de loi ne précise cependant pas les modalités de vérification des informations : il n'indique pas comment les entreprises déterminent, a priori, si les données sont effectivement liées à la cybersécurité ou à la défense nationale. Il ne prévoit pas non plus de hiérarchisation entre les différents types de données soumises à surveillance, ce qui pose évidemment la question de la pertinence de certaines d'entre-elles au regard des objectifs poursuivis. Ce flou juridique

[5] https://www.facebook.com/notes/facebook-washington-dc/a-message-about-cispa/10150723305109455
6 https://www.eff.org/deeplinks/2012/04/voices-against-cispa

est d'autant plus problématique que des canaux de communication privés pourraient être surveillés (médias et réseaux sociaux, relevés de chat en ligne ou historiques d'appels).

L'imprécision de ces dispositions a pour conséquence directe d'élargir les pouvoirs du gouvernement au-delà de la détection et de la défense contre les seules cybermenaces. Cela permettrait, au moyen d'une justification incertaine voire absente, un usage abusif du partage d'informations, notamment à caractère personnel ou portant potentiellement atteinte à la vie privée des internautes.

Cette hypothèse, si elle est confirmée par les prochaines lectures du texte, constituerait une entorse au IV^{ème} amendement de la Constitution américaine qui protège les citoyens contre les perquisitions et saisies non motivées, comme le soutiennent des organisations telles que l'Electronic Frontiers Foundation (EFF) et Reporters Without Borders. C'est également la principale préoccupation de la Maison Blanche, particulièrement opposée au projet de loi tel que rédigé aujourd'hui.

2. La protection de la vie privée laissée au bon vouloir des entreprises privées

Si le champ d'application de CISPA est extrêmement large, le texte prévoit tout de même de respecter les restrictions apportées par les entreprises privées elles-mêmes. Si elle le souhaite, une société telle que Facebook peut choisir de ne partager avec le gouvernement américain que des données complètement anonymisées, afin de protéger la vie privée de ses utilisateurs. La protection en amont des données, et donc de la vie privée des utilisateurs, qui devrait être prévue par les textes eux-mêmes, est entièrement laissée à la discrétion des opérateurs privés.

> "Cyber threat information shared in accordance with paragraph (1)—
>
> (A) shall only be shared in accordance with any restrictions placed on the sharing of such information by the protected entity or self-protected entity authorizing such sharing, including, if requested, appropriate anonymization or minimization of such information ;"
>
> Voir : "Cyber Intelligence Sharing and Protection Act of 2011"

Dans son billet sur CISPA précité, Facebook s'est par exemple engagé à ne pas « *partager des informations personnelles sensibles avec le gouvernement au nom de la protection de la cybersécurité* ».

3. L'immunité accordée aux entreprises privées dans le partage d'informations

Dans sa première mouture, le projet de loi affranchissait les acteurs privés de toute responsabilité juridique en cas de partage d'informations avec le gouvernement, sauf « faute intentionnelle » de leur part. Cette disposition, accueillie favorablement par les entreprises privées, a cependant été modifiée. Désormais, seules les entreprises ayant agi de bonne foi, à des fins de lutte contre l'activité criminelle, pourront prétendre à cette exonération de responsabilité.

Un avenir incertain pour CISPA

1. Un prochain désaveu du secteur privé ?

Si des projets de loi tels que SOPA et PIPA ont été largement contestés par ces mêmes acteurs privés, c'est en partie en raison de la faible protection juridique dont ils faisaient bénéficier ces derniers. Il est donc fort probable que CISPA connaisse le même sort que ses prédécesseurs, en raison de l'allègement significatif de la protection accordée aux acteurs privés censés partager leurs données avec les entités nationales américaines.

2. L'opposition de l'administration Obama

Le gouvernement américain a ouvertement exprimé son opposition au texte, affirmant que ce projet mettait en péril la vie privée. Il a exigé que le texte soit « accompagné des protections nécessaires pour les particuliers ». Plus précisément, l'administration Obama reproche au texte d'exonérer les entreprises privées de leur responsabilité de protéger les données touchant à la vie privée de leurs clients et de réduire ainsi à néant toute forme d'incitation à la cybersécurité[7]. En l'absence de modification de ses dispositions (certains parlementaires ont d'ores et déjà promis quelques amendements[8]), et s'il est adopté par le Sénat (majoritairement démocrate), CISPA risque de se voir opposer le veto du président américain.

Lutte contre la cybercriminalité et respect de la vie privée : deux impératifs finalement difficilement conciliables

Plus qu'une simple loi permettant le partage d'informations ou menaçant la vie privée, CISPA relance le débat de la difficile conciliation entre une cybersécurité accrue et la protection de la vie privée des internautes.

La lutte contre la cybercriminalité se heurte généralement à des contraintes d'ordre éthique et juridique. D'un côté, les notions de vie privée, libertés fondamentales, droit à l'anonymat, secret des correspondances ou encore droit à l'oubli sont essentielles. De l'autre, la lutte contre la cybercriminalité serait évidemment facilitée en cas de transparence des réseaux, d'absence d'anonymat, de partage accru d'informations entre secteur privé et institutions publiques. Comment concilier les impératifs du respect de la vie privée des citoyens et le besoin d'information inhérent à une démarche efficace de lutte contre les cybermenaces ?

Classification et hiérarchisation des informations, intégration du juge au processus de partage de données ou encore création d'un régime d'exception sont autant de pistes à explorer. Dans le cas contraire, les projets de loi entraînant une transparence accrue et un accès facilité à l'information, même personnelle, risquent de se heurter au refus catégorique de la société civile et des défenseurs des droits et libertés fondamentaux.

[7] http://www.washingtonpost.com/politics/obama-threatens-to-veto-cispa-cybersecurity-bill-citing-privacy-concerns/2012/04/25/gIQAkS3khT_story.html

[8] http://thenextweb.com/us/2012/04/26/cispas-fate-may-be-determined-today-as-its-amendments-are-weighed/

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

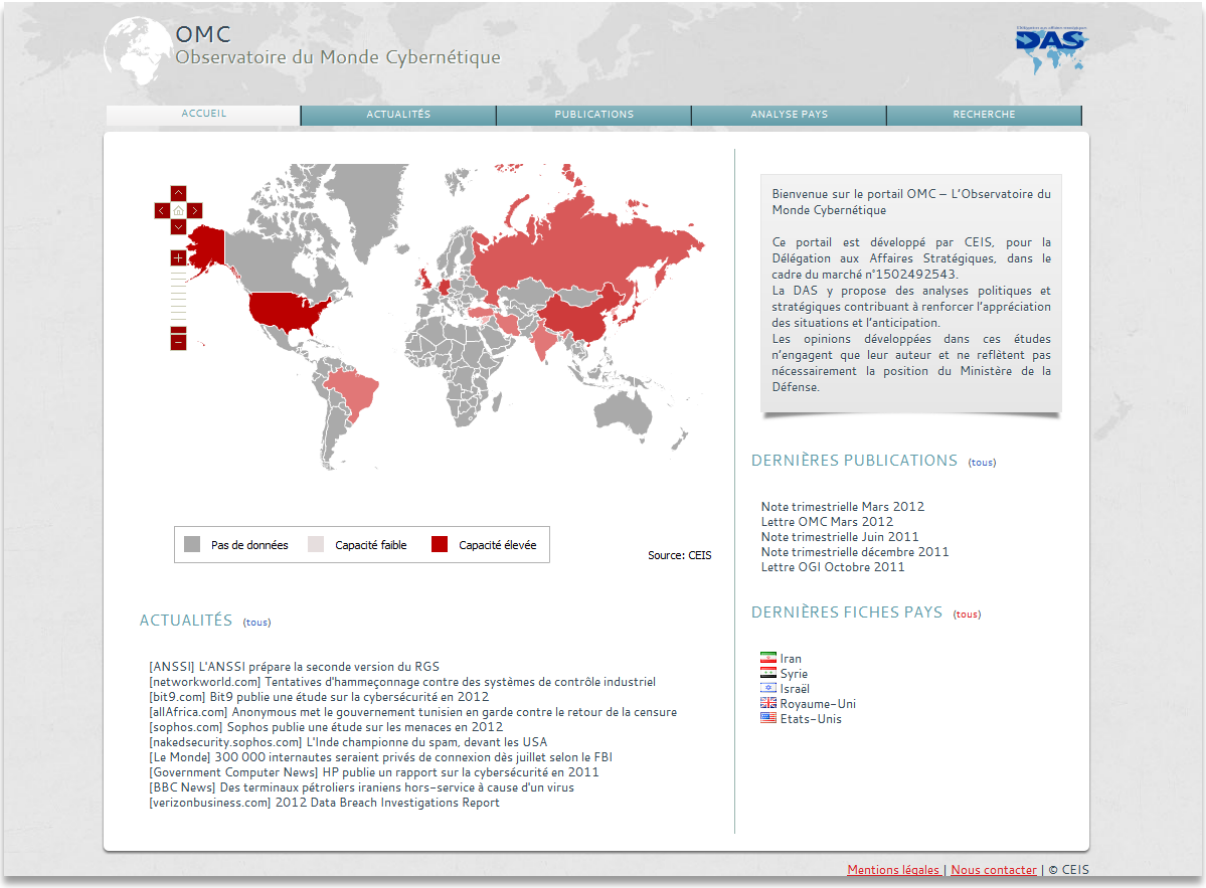

Figure 1 - Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Challenge Hacknowledge RSSIL	Maubeuge (59)	2 – 3 juin 2012
Techno Security Conference 2012	Myrtle Beach, USA	3 juin 2012
Conférence Octopus : coopération contre le cybercrime	Strasbourg	6 – 8 juin 2012
Integralis Security World	Boulogne	7 juin 2012
Cyberdef-CyberSec (Salon international Eurosatory)	Paris	13 juin 2012
Recon 2012	Montréal	14 juin 2012
CyberDefence 2012 SMI Group	Londres	18 – 19 juin 2012
Hack In Paris	Paris	18 – 22 juin 2012
The 1st International Conference on Cyber Crisis Cooperation - Cyber Exercises	Paris	27 juin 2012
Hackademic	Newark, USA	29 juin 2012

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