Observatoire du Monde Cybernétique

Lettre n°27 – Mars 2014

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

[01net] Guillaume Poupard prend la tête de l'ANSSI

Guillaume Poupard, ingénieur en chef de l'armement, a été nommé en Conseil des ministres directeur général de l'ANSSI. Polytechnicien et docteur en cryptographie, Guillaume Poupard était auparavant responsable du pôle « sécurité des systèmes d'information » au sein de la direction technique de la DGA.

[Usine Digitale] Snecma victime d'une attaque informatique

La filiale du groupe Safran, Snecma, spécialisée en aéronautique, a vraisemblablement été victime d'une attaque informatique, notamment en raison des failles du navigateur Internet Explorer. S'il n'est pas encore certain que les pirates aient pu s'infiltrer dans le réseau informatique du groupe, le logiciel employé pour l'attaque a permis d'identifier des noms de domaine lui appartenant.

[Le Point] Paris accueille le volet français du Forum de la gouvernance d'Internet

Paris a accueilli, le lundi 10 mars, le premier Forum de la gouvernance d'Internet en France. Déclinaison française de l'évènement international du même nom, il a notamment pour but d'asseoir la présence française sur des domaines tels que la neutralité du net, le cloud computing ou encore la mise en place d'une véritable cyber stratégie. La question des données personnelles était aussi à l'honneur, avec plusieurs ateliers de réflexion dédiés.

[Le Monde] Internet : les Etats-Unis acceptent de ne plus gérer seuls les noms de domaine

Le gouvernement américain a annoncé qu'il était prêt *à « abandonner son rôle central dans l'attribution des noms de domaine au profit d'une gouvernance mondiale »*. Le département américain du commerce a indiqué dans un communiqué qu'il allait convoquer les *« acteurs à travers le monde pour réfléchir à des pistes »* qui permettront de revoir le rôle central du gouvernement américain dans la supervision de l'Internet Corporation for Assigned Names and Numbers (ICANN), le régulateur mondial chargé de valider les noms de domaines sur Internet. L'ICANN, créée en 1998, a son siège en Californie. En dépit d'une démarche déjà initiée de diversification de son board en faveur d'une plus grande ouverture, elle relève, en dernière instance, du département du commerce américain.

[RAND] Etude sur les marchés noirs de la cybercriminalité

Le dernier rapport de la RAND dresse un portrait démographique et économique des marchés noirs de la cybercriminalité. L'étude estime ainsi que si 70% des acteurs des marchés noirs sont des individus isolés, 5% sont des terroristes et 4% des *« acteurs sponsorisés par un Etat »*. Seul un quart d'entre eux serait réellement compétent, les autres bénéficiant d'outils *« clés en main »*. Et si leurs moyens de communication privilégiés restent les forums, les canaux IRC, le webmail et TOR, Twitter est désormais un vecteur de communication de choix. Avec des failles qui valent toujours plus cher et la banalisation de l'anonymat sur Internet, les marchés noirs de la cybercriminalité devraient encore se développer.

[Der Spiegel] Des entreprises allemandes du Net espionnées par les Etats-Unis

Selon le journal allemand Der Spiegel, citant plusieurs documents d'Edward Snowden, la NSA et le GCHQ auraient espionné plusieurs fournisseurs IP par satellite en Allemagne. Objectif : *« [développer] une large connaissance du trafic Internet transitant »* en Allemagne. Stellar, société exploitant des antennes et des capacités satellite pour fournir des services Internet de téléphonie à des sites spécifiques, fait partie des entreprises espionnées.

[NYT et CRI Online] La NSA aurait infiltré les serveurs du géant chinois Huawei – La Chine demande des explications

Selon le New York Times, la NSA aurait infiltré les serveurs du siège du géant Huawei, afin de recueillir des informations sensibles, notamment

des communications entre cadres dirigeants. Le porte-parole du ministère chinois des Affaires étrangères a demandé aux Etats-Unis de *« s'expliquer »* et de *« cesser ces pratiques »*.

[The Diplomat] Xi Jinping : la Chine doit devenir une cyberpuissance

Le président chinois Xi Jinping a mené, fin février, la première session du groupe de travail sur la sécurité d'Internet et l'informatisation, en charge de formuler la cyberstratégie chinoise. Suite à cette session, le président chinois aurait déclaré que *« des efforts* [devaient] *être faits pour que le pays devienne une cyberpuissance »*.

La Chine étant à la fois très discrète et très critiquée en matière cyber, notamment suite à la parution du rapport Mandiant en février 2013, cette prise de position du président démontre un effort de transparence et également une certaine confiance quant aux capacités en développement.

[ZDNet] La Russie accusée d'avoir développé le *malware* Uroburos

L'éditeur de solutions antivirus allemand G Data a identifié un *rootkit*, c'est-à-dire un logiciel capable de créer des *backdoors* dans les systèmes qu'il infecte, nommé Uroburos.

Le *rootkit*, plus sophistiqué que la moyenne, peut être aisément modifié pour pénétrer des systèmes ciblés et dans un second temps créer une *« porte d'entrée »* pour les attaquants. Selon G Data, le code employé serait trop complexe pour être l'œuvre de hackers indépendants. D'après l'éditeur d'anti-virus, le malware pourrait avoir été développé et distribué par le gouvernement Russe.

Avant de s'exécuter, le programme malveillant recherche la présence d'un autre *malware* appelé Agent BTZ. Si celui-ci est déjà présent, Uroburos ne s'exécute pas. Or, Agent BTZ avait déjà été utilisé lors d'une attaque contre le pentagone et dont on soupçonnait la Russie d'être à l'origine. Un détail qui permettrait à l'éditeur G Data de relier Uroburos à la Russie.

[The Independent] La Russie fait fermer des pages Internet liées aux manifestations en Ukraine

Les autorités russes ont fait fermer treize pages sur VKontakte, le premier réseau social du pays et équivalent de Facebook en Russie. L'agence russe de surveillance de l'Internet, Roskomnadzor, a fait fermer ces pages pour encouragement d'activités terroristes et participation à des actions de masse non autorisées. Le groupe le plus important, qui regroupait près de 500 000 personnes, n'est plus accessible aux utilisateurs depuis le territoire russe.

[McAfee] Un rapport de McAfee révèle des techniques de haut niveau pour voler des données

Le rapport du quatrième trimestre de 2013 de l'éditeur de logiciel antivirus McAfee met en lumière le rôle central du *Dark Web* dans l'industrie du logiciel malveillant sophistiqué. Il indique que ces logiciels malveillants sont de plus en plus facilement accessibles aux cybercriminels, qui disposent ainsi de manière croissante d'outils sophistiqués *« prêts à l'emploi »*. Cette augmentation renforce l'industrie du *« Cybercrime-as-a-service »*. Le rapport fait également plus largement état de la prolifération de la cybercriminalité et de l'augmentation significative des cyberattaques : le nombre de logiciels malveillants recensés en 2013 est de 2,47 millions, soit une augmentation de 197% par rapport à 2012. Le dernier trimestre de 2013 a, à lui seul, vu l'apparition de 744 000 nouveaux logiciels malveillants selon McAfee. Egalement de 2012 à 2013, McAfee enregistre une augmentation de 1 millions de rançongiciels tandis que les URL suspectes ont augmenté de 7%.

[Trend Micro] Siesta : une nouvelle série de cyberattaques ciblées découverte

Une campagne de cyberattaques ciblées, baptisée Siesta, a récemment été découverte par des chercheurs de Trend Micro. Celle-ci vise des secteurs variés de l'économie, allant de la défense à la finance et l'énergie. Elle se base sur du *spear*

phishing puis l'installation d'une *backdoor* une fois que le logiciel malveillant a réussi à pénétrer les systèmes d'informations ciblés. Cette campagne de cyber espionnage ciblée et sophistiquée n'a pour l'instant pas été attribuée.

[Europarl] Témoignage d'Edward Snowden devant le parlement européen

Dans un témoignage écrit envoyé au Parlement européen, Edward Snowden répond aux questions de quelques députés européens au sujet des programmes de surveillance de la NSA. Si la plupart des déclarations sont en lien avec l'inconstitutionnalité de la surveillance de masse et du contrôle de ces programmes aux Etats-Unis, Edward Snowden y soulève un point particulièrement intéressant pour les pays européens. Il indique que la stratégie principale de la Foreign Affairs Division (FAD) de la NSA serait de pousser les pays membres de l'Union européenne à adopter des programmes de surveillance de masse, pour accéder à de plus grandes quantités de données dans le cadre d'accords de partage ponctuels d'information entre services de renseignement. La révélation des programmes et leur désaveu auraient alors freiné cette dynamique.

[Le Monde] Edward Snowden : *« La NSA met le feu à Internet, vous êtes les pompiers qui peuvent le sauver »*

La question de la protection de la vie privée et de la surveillance de la NSA a été largement évoquée au festival SXSW (« *South by Southwest* ») consacré aux nouvelles technologies. La présence en vidéo-conférence d'Edward Snowden a été le *« clou du spectacle »*. S'exprimant de Russie, l'ancien consultant de la NSA a tenu à faire le point sur les 8 mois qui ont suivi la révélation de la surveillance de masse pratiquée par l'Agence. Snowden affirme ne rien regretter et se félicite même des *« réactions incroyables »* de l'opinion publique depuis ces révélations.

[Business Insider] Google prépare une plateforme pour les objets connectés

Sundar Pichai, vice-président de la division Produits présent aux cycles de conférences SXSW Interactive à Austin, a prévenu que l'étendue de ce qu'il est possible de faire dans le domaine des objets connectés avait seulement été *« effleurée »*. Le lancement d'un premier SDK pour Android a été annoncé. Si les options précises concernant ce premier SDK n'ont pas encore été dévoilées, Google veut déjà se placer sur un marché en pleine expansion.

[Janes] Budget du Pentagone en 2015 : le cyber bénéficiera d'une augmentation de 8,5%

Le budget du département de la défense américain allouera en 2015 5,1 milliards aux opérations concernant le cyberespace – ce budget avoisinait les 4,7 milliards de dollars en 2014. Les fonds alloués au cyberespace couvriront le coût des opérations liées à la cybersécurité (aspect défensif) et aux cyberattaques (aspect offensif). Lors d'un discours fin 2013, Chuck Hagel, secrétaire à la défense, présentait la recherche et le développement des aspects cyber comme une priorité pour le département de la défense.

[Boursier] Alibaba et Weibo, deux géants du net chinois souhaitent entrer en Bourse à New York

Le réseau social Weibo, surnommé le « Twitter Chinois » prépare son entrée en bourse. Un dossier a été déposé auprès de la Securities and Exchange Commission (SEC). Lancé en 2009, Weibo a réalisé près de 190 millions de dollars de chiffres d'affaires en 2013. Le réseau social, qui compte près de 130 millions d'utilisateurs actifs, a pour objectif de lever 500 millions de dollars lors de son introduction à la bourse de New-York. Le groupe Alibaba, qui détient 18% du réseau social, envisage également une entrée en Bouse pour le 3ème trimestre de l'année.

[RSF et Libération] RSF désigne les institutions ennemies d'Internet

Pour son rapport annuel sur les « ennemis d'Internet », l'association Reporters Sans Frontières s'est intéressée aux *« dérives mises en lumière par les révélations d'Edward Snowden »*. Si le rapport de l'année dernière s'était concentré sur cinq pays et cinq entreprises qui s'était distingués pour avoir fourni des outils de surveillance, force est de constater que la situation n'a pas évolué. Le rapport souligne même que *« la prise de conscience du niveau de surveillance du réseau mondial est montée d'un cran »*. Le document cible 32 institutions décrites comme ennemies d'Internet.

[Reuters] Entrainement cyber au Japon en vue des Jeux Olympiques

Le gouvernement japonais a conduit un entrainement censé renforcer la sécurité de son réseau informatique en vue d'une éventuelle cyberattaque massive lors des jeux Olympiques de 2020. Le Japon a ainsi suivit le mouvement enclenché par la Grande Bretagne avant les Jeux Olympiques de 2012. Une cinquantaine de spécialistes en cyberdéfense se sont réunis dans un centre d'urgence de Tokyo pour faire face aux attaques fictives simultanées de différents hackers. C'est la première fois qu'un exercice de ce type regroupant les agences gouvernementales et les grandes entreprises était effectué.

[News24] Quatre ans de prison pour une cyberattaque en Russie

Un opposant russe suspecté d'avoir dirigé une attaque contre les systèmes informatiques du Kremlin a été condamné à 4 ans de prison selon le FSB. Les enquêteurs ont révélé que l'attaque avait duré près d'une heure, et qu'elle avait reçu le soutien du groupe Anonymous, souhaitant voir l'annulation des dernières élections présidentielles.

.

Evolution de la gouvernance Internet : quelles perspectives avant NETMundial ?

Dans un communiqué du 14 mars 2014[1], l'ICANN a lancé un processus de transition historique qui devrait aboutir fin 2015 à sa séparation du gouvernement américain au profit d'une gestion internationale et multipartite des noms de domaines. Selon son administrateur Lawrence Strickling, l'organisation devra se doter d'un *« nouveau modèle de gouvernance mondiale*[2] *faisant participer toutes les parties prenantes d'Internet : gouvernements, société civile, secteur privé et communautés techniques »*.

Cette annonce majeure s'inscrit dans un contexte plus global de réflexion sur la gouvernance d'Internet, notamment à la lumière des révélations sur l'espionnage de masse mené par la National Security Agency, ainsi que sur les enjeux économiques, politiques, culturels croissants du cyberespace. Cette gouvernance d'Internet sera discutée lors du forum NETMundial qui se tiendra à Sao Paulo au Brésil les 23 et 24 avril prochains. A cette occasion, toutes les parties prenantes ont été invitées à soumettre une contribution sur l'avenir de la gouvernance d'Internet. Celles-ci, au nombre de 187, traduisent des représentations et des stratégies qu'il convient d'analyser pour comprendre les défis à relever à l'horizon 2015 mais aussi à long terme[3] sur la gouvernance d'Internet.

La position dominante des Etats-Unis dans un contexte de transition

Les Etats-Unis ont fait l'objet de vives critiques concernant leur position dominante sur la structure actuelle d'Internet. Au-delà du contrôle que le département du commerce américain exerce sur l'attribution des noms de domaine, l'essentiel des câbles sous-marin passe par le territoire des Etats-Unis ou un d'un de leurs alliés des "Five Eyes", et de fait sous juridiction américaine autorisant la surveillance de masse sur les non-américains. A cette « gouvernance par l'architecture » s'ajoute la prédominance des géants américains d'Internet qui renforcent encore la centralité des Etats-Unis.

Les Etats-Unis devraient ainsi essayer de conserver cette position dominante tout en acceptant un changement inéluctable face aux dénonciations croissantes de nombreux pays. En annonçant d'eux-mêmes l'évolution souhaitée de l'ICANN, les Etats-Unis retirent plusieurs bénéfices : ils évitent que la transition leur soit imposée par d'autres pays, ils gardent la maîtrise d'un processus de transition qui s'annonce complexe, et redorent leur image ternie par les révélations sur la surveillance de masse.

Au-delà de l'effet d'annonce et du crédit que leur donne l'annonce de l'évolution de l'ICANN, les Etats-Unis disposent d'au moins deux éléments qui pourront être utilisés afin de conserver une position dominante dans la future gouvernance d'Internet. Tout d'abord, ils disposent du poids économique des géants d'Internet, d'entreprises essentielles dans la gestion de la structure d'Internet, ainsi qu'une position centrale dans l'architecture actuelle de la couche physique du cyberespace. Les géants d'Internet et des télécoms américains vont donc sans aucun doute influer largement sur le système de gouvernance multipartite à venir. Dans sa contribution, le gouvernement américain recommande de conserver les institutions qu'ils ont créées

[1] http://www.icann.org/en/news/announcements/announcement-14mar14-en.htm
[2] http://www.lemondeinformatique.fr/actualites/lire-les-etats-unis-vont-emanciper-l-icann-sur-la-gouvernance-d-internet-56880.html
[3] http://netmundial.br/fr/

et qui ont fait leur preuve par le passé. Le second élément est pragmatique et peut se retrouver dans le non-dit, ou dans les ambitions affichées. Dans sa proposition soumise au forum NETMundial[4], le gouvernement américain se prononce en faveur d'une gouvernance basée sur des valeurs démocratiques, les Droits de l'Homme, le bon fonctionnement d'Internet, et ainsi que sur des standards juridiques et techniques communs *« afin d'éviter des doublons inutiles »*. Les normes communes établies devront ensuite être appliquées et contrôlées par un système mondial, multi-parties prenantes, et ce fin 2015 selon l'agenda fixé. Les parties prenantes seront sélectionnées selon un processus qu'il conviendra de définir en amont. Il est possible, au vu des ambitions annoncées et des exigences que les Etats-Unis affichent lors du processus de transition, que celui-ci ne soit pas finalisé fin 2015. Le cas échéant, cela permettrait aux Etats-Unis de conserver leur position dominante plus longtemps, tout en remettant en question l'efficacité d'une gouvernance mondiale. En conclusion, les Etats-Unis disposent de leviers majeurs pour peser dans les négociations à venir, ainsi que de la possibilité de conserver plus longtemps un rôle central en cas d'échec des discussions.

La Chine en faveur d'une gestion globale pour plus de stabilité et de sécurité, mais ne condamnant pas l'espionnage

La contribution du Ministère des Affaires Etrangères chinois[5] est le code de conduite international pour la sécurité de l'information (*international code of conduct for information security*) qui avait été soumis avec la Russie, le Tadjikistan et l'Ouzbékistan à l'Assemblée Générale des Nations Unies. Celui-ci se concentre sur le contrôle de l'information afin de protéger la stabilité intérieure des Etats, mais aussi la stabilité internationale. La résolution est en effet introduite comme suit :

Recognizing the need to prevent the potential use of information and communication technologies for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure within States, to the detriment of their security

L'ensemble du code de conduite se concentre sur le fait qu'il est nécessaire de contrôler l'information afin d'éviter de déstabiliser les Etats ou la scène internationale. Si ce code de conduite veut lutter contre la promotion de l'extrémisme, du terrorisme, du séparatisme, ainsi que contre les *« menaces, attaques, perturbations et sabotage »*, celui-ci ne mentionne nulle part les activités d'espionnage décriées par de nombreux Etats. Cela peut s'expliquer par les campagnes de cyber espionnage massives régulièrement attribuées à la Russie et la Chine, cette dernière considérant cet espionnage comme un moyen de rattraper un retard technologique et développer son économie par le biais d'opérations militaires autres que la guerre (Military Operations Other than War MOOTW).

En ce qui concerne les mécanismes de gouvernance, la Chine est en faveur d'une approche multipartite avec des mécanismes de contrôle forts, d'une transparence de la décision et de la mise en place de lois régulant la liberté de recherche et d'expression sur Internet. Une contribution faite par deux instituts chinois (China Institutes of Contemporary International Relations et Institute of Information and Development Society) insiste également sur la sécurité de l'information et le principe d'harmonie qui doit être central dans la gouvernance d'Internet. Ce principe se base sur une interaction dynamique entre tous les acteurs pour plus de sécurité et permettre à chacun de "coexister". A travers l'idée de coexistence, on retrouve l'idée de stabilité et de norme défendue par le code de conduite.

[4] http://content.netmundial.br/contribution/u-s-government-submission-for-netmundial/62
[5] http://content.netmundial.br/contribution/international-code-of-conduct-for-information-security/67

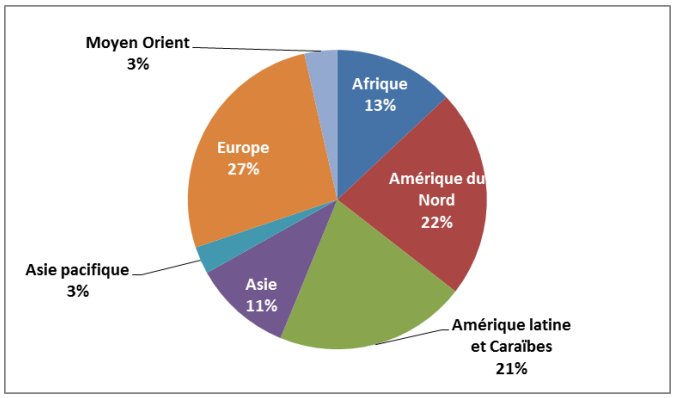
Les non-alignés de l'Internet : Brésil, Inde, Argentine et… Allemagne

Les contributions officielles du Brésil, de l'Inde, de l'Argentine et de l'Allemagne se concentrent sur la protection des Droits de l'Homme, conformément à l'esprit de la résolution qu'ils avaient proposé à l'Assemblée Générale des Nations Unies fin 2013. Cette résolution avait pour but de condamner la surveillance de masse en faisant de celle-ci une atteinte aux Droits de l'Homme. En réitérant dans leurs contributions leur soutien à ces valeurs, ils renouvellent implicitement leur condamnation de la surveillance sans pour autant apparaître comme inscrits dans un antagonisme avec les Etats-Unis.

La condamnation des Etats-Unis dans les publications est en effet indirecte. Sur les pays cités précédemment, qui se sont vivement exprimés contre la surveillance américaine depuis septembre 2013 et les révélations des écoutes des dirigeants par la Nationale Security Agency, seule l'Argentine rappelle que les Etats pratiquant une surveillance de masse doivent être sanctionnés. A l'inverse des gouvernements de ces pays, leur société civile, académique, et leur secteur privé ne manquent pas de dénoncer les pratiques américaines. Un des éléments les plus révélateurs est le nombre de publications conjointes d'organismes non gouvernementaux allemands et brésiliens, brésiliens et indiens, qui affirment clairement que la domination américaine et la centralité des Etats-Unis dans le système de gouvernance d'Internet actuel est le principal problème.

La gouvernance à venir d'Internet nécessite, selon les pays précédemment cités, des mécanismes permettant aux gouvernements démocratiquement élus d'exercer un contrôle sur les institutions de régulation, ainsi qu'un rôle dans l'adoption des normes communes qui encadreront par la suite leurs ressortissants. Cette forme de gouvernance devra être multipartite, transparente, permettre de lutter contre la cybercriminalité au niveau international et enfin favoriser l'accès et l'utilisation d'Internet dans les pays en retard technologiquement par le biais de transferts de technologies et d'expertise. A l'opposé des positions prises notamment par la Chine et la Russie, les gouvernements s'opposent à toute forme de filtrage des contenus, tout en rappelant la nécessité de respecter les Droits de l'Homme. Une part importante est accordée à la question de l'accès à Internet pour les plus démunis, mais également les femmes et les personnes âgées en ce qui concerne l'Argentine.

Quelques chiffres : répartition géographique des contributions au NETMundial



Il est possible de remarquer que les pays asiatiques, pourtant connaissant une fort taux de pénétration d'Internet, ont peu contribué au débat pour la préparation du forum NETMundial. Proportionnellement, l'Afrique a plus contribué que l'Asie à cette préparation. A l'inverse, plusieurs pays européens ont fait entendre leurs voix, de même que l'Inde et l'Amérique Latine qui est la première concernée par la domination américaine, et qui a vivement réagi aux révélations sur la surveillance de la NSA. Enfin, les Etats-Unis restent dominants par le biais de leur secteur privé : tous les géants d'Internet et des télécoms américains ont en effet contribué au Forum. Cela démontre la force de frappe dont va disposer les Etats-Unis lors des débats à venir.

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

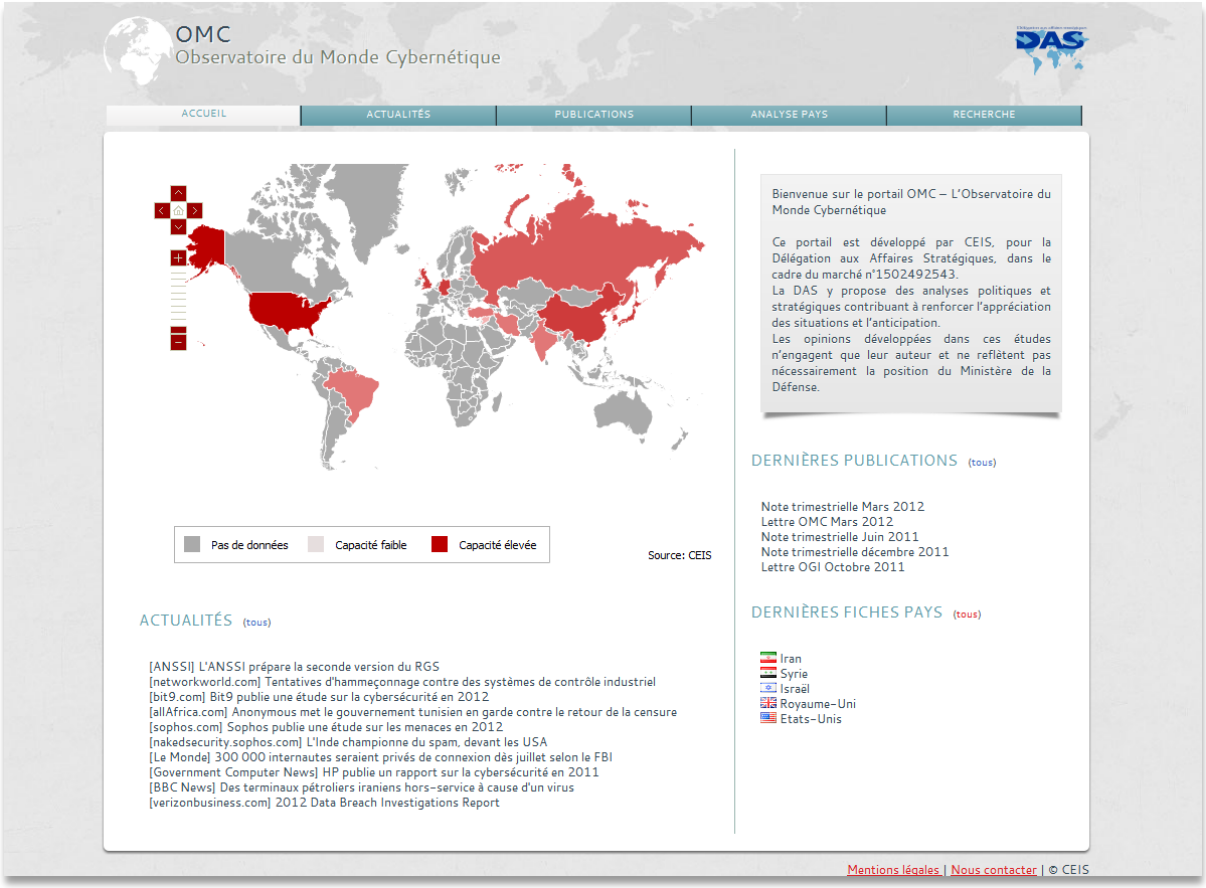


Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Cloud Computing World Expo	Paris	9 - 10 avril
2014 World Conference on Information Systems and Technologies (WorldCIST 14)	Madeira	15 avril
NETmundial	Sao Paulo, Brésil	23 - 24 avril
The Third International Conference on Cyber Security, Cyber Warfare, and Digital Forensic (CyberSec2014)	Beyrouth	29 avril
EUROCRYPT 2014	Copenhague	11 mai
Infiltrate 2014	Miami	15 mai

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