Observatoire du Monde Cybernétique

Lettre n°24 – Décembre 2013

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

[01.Net] Education : lancement d'un permis Internet pour les écoliers français

Une opération, lancée dans 38 départements et à destination 450 000 enfants, a pour but d'apprendre aux élèves de CM2 à mieux maîtriser le Net.

Un kit pédagogique a été mis en place, contenant un DVD de témoignages, des tests d'entraînement, des livrets pour les élèves, des fiches d'examen afin de valider leurs acquis, une affiche pour la classe et des permis Internet. Pornographie, rencontres dangereuses, vie privée… tous les sujets sont abordés. Ce programme devrait être étendu à toute la France dès 2014.

[Security Vibes] Le gouvernement britannique imposera des mesures de cybersécurité à ses fournisseurs

Dans le cadre de sa National Security Strategy, le gouvernement britannique va imposer dès mars 2014 un nouveau standard organisationnel en matière de cybersécurité.

Les entreprises souhaitant traiter avec le secteur public devront adopter ce standard basé principalement sur des bonnes pratiques élémentaires destinées à empêcher les attaques informatiques triviales.

[HITB] David Cameron met la Chine au défi d'être plus ouverte en cybersécurité

Le Premier ministre britannique a demandé à son homologue chinois d'ouvrir un dialogue formel avec le Royaume-Uni - et plus largement l'Europe - sur les questions de cybersécurité.

La Chine a répondu positivement sur ce sujet hautement sensible. Les principaux équipementiers télécoms chinois, Huawei et ZTE, sont en effet confrontés à la méfiance des autorités de nombreux pays européens ainsi que des Etats-Unis qui pointent du doigt les opérations d'espionnage menées par la Chine.

[Le Figaro] La Suisse se lance dans le business des « cyberbunkers »

La Confédération helvétique envisage de transformer ses bunkers antiatomiques en « cyberbunkers » permettant de stocker des données sensibles à l'abri des cyberattaques et des aléas physiques susceptibles de causer des pertes ou des vols de données. L'ancien QG de l'armée suisse, construit au cœur d'une montagne, est par exemple aujourd'hui contrôlé par une société privée, Deltalis, qui y abrite les données numériques d'entreprises ou de certains particuliers. Suite aux révélations sur la NSA, la demande en termes de protection des données a explosé, avec un business qui a « triplé en un laps de temps très court » selon Christoph Oschwald, un des dirigeants de Mount10, entreprise qui abrite sous les Alpes les données du Parlement suisse. La Confédération compterait déjà 55 « cyberbunkers ».

[Le Monde] Conservation des données : la Cour de justice européenne épingle la Commission

La Cour de Justice de l'Union Européenne (CJUE) estime que la directive européenne sur la conservation des données personnelles est incompatible avec la Charte des Droits Fondamentaux de l'Union européenne. Cette directive 2006/24/CE, votée en 2006, oblige les opérateurs télécom et les fournisseurs de services du secteur à conserver les données de leurs clients à des fins de recherche et de poursuites d'infractions graves. Cette conservation des données accroît les capacités de l'établissement détenteur à suivre très précisément et reconstruire le comportement de ces clients, tout en augmentant également le risque de détournement des données à des fins illégales, du simple fait de leur conservation.

[Infosecurity] Une campagne de cyberespionnage en amont du G20 compromet plusieurs ministères

En amont du dernier G20 qui s'est déroulé en Russie, un groupe de hackers suspecté d'opérer

depuis le territoire chinois a mené avec succès une campagne de cyberattaques contre les organismes diplomatiques (missions diplomatiques, ministères des affaires étrangères...) de plusieurs pays. Les chercheurs en sécurité de FireEye ont estimé que cette attaque, baptisée “Opération Ke3chang”, avait réussi contre au moins neuf réseaux dans cinq pays différents. En prenant le contrôle d'un serveur appartenant aux hackers, ils ont mesuré que 21 machines infectées exfiltraient des informations.

[DarkReading] Des organisations internationales s'allient contre un Botnet

La Microsoft’s Digital Crime Unit a collaboré avec l'EC3 d'Europol, le FBI et des leaders de l'industrie pour contrer un ZeroAccess Botnet qui avait infecté 2 millions d'ordinateurs et coûté 2,7 millions par mois à des entreprises publicitaires. C'est la première opération de la Microsoft’s Digital Crime Unit contre un Botnet, suite à sa création début novembre 2013.

[La Presse] Cyberdéfense : les États-Unis signent un partenariat avec l'Estonie

Le secrétaire d'État américain John Kerry a signé ce mardi 3 décembre un partenariat avec l'Estonie en matière de cyberdéfense. L'Estonie, qui accueille le centre d'excellence de l'OTAN en cyberdéfense (CCDCOE), avait été victime en 2007 d'une cyberattaque massive qui avait poussé le pays à développer largement ses capacités en matière de cyberdéfense. Ce partenariat vise à « affirmer l'engagement des États-Unis et de l'Estonie à continuer de collaborer pour améliorer des infrastructures d'information et de communication ouvertes, sûres et fiables ». Les liens entre les deux pays en la matière étaient déjà forts : l'OTAN a ainsi organisé la semaine dernière un exercice de cyberdéfense de grande ampleur en Estonie, et les Etats-Unis ont repris le modèle du réseau de volontaires spécialisés en cyberdéfense estonien dans de nombreux Etats.

[Foreign Policy] Le civil le plus important de la NSA démissionne

Chris Inglis, directeur adjoint de la NSA depuis 2006, a quitté son poste e. Sa démission officielle devrait être effective d'ici la fin de l'année 2013. Fran Fleisch, haut fonctionnaire de l'Agence, devrait lui succéder. Ces derniers mois, Fran Fleisch avait peu à peu occupé les fonctions de Chris Inglis au sein de la NSA, tandis que ce dernier se concentrait sur la défense de la NSA en pleine affaire Snowden.

[Le Monde] La NSA localise plusieurs centaines de millions de portables par jour

Le Washington Post a révélé mercredi 4 décembre l'existence du programme Co-Traveler, qui permet à la NSA de recueillir des centaines de millions de données relatives à la géolocalisation grâce à des interceptions effectuées sur les câbles internet. Deux sociétés, dont les noms ne sont pas mentionnés, aideraient la NSA dans le cadre de ce programme. Au total, c'est près de 5 milliards de données de géolocalisation qui seraient recueillies quotidiennement par le biais de ces interceptions « upstream ». Ce volume surpasserait les capacités de traitement et d'analyse de la NSA.

[Les Echos] Washington inquiet des liens entre Séoul et Huawei

Alors que le vice-président américain Joe Biden était actuellement en tournée en Asie, le comité pour les relations étrangères et celui pour les activités de surveillance et d’espionnage (« intelligence committee ») du Sénat s’inquiètent de la décision prise par la société sud-coréenne LG Uplus de confier au groupe chinois Huawei la construction d’une partie de son réseau national à haut débit. La sécurité des 28 000 soldats américains stationnés sur le territoire sud-coréen, qui avaient déjà fait l'objet d'une cyberattaque à l'été, pourrait se voir compromise par la décision de la société sud-coréenne.

[Politico] La Maison Blanche refuse de séparer les directions de la NSA et du CyberCommand

La Maison Blanche a tranché sur la question de la séparation des directions de la NSA et du Cyber Command. Celle-ci avait été soulevée suite aux révélations sur la surveillance de la NSA et les pouvoirs conférés au général Keith Alexander, premier à avoir endossé la double casquette. Ce dernier s'était vivement opposé à la séparation des directions, invoquant la complémentarité des institutions et la paralysie dans laquelle elles se trouveraient le cas échéant.

Par ailleurs, un rapport remis le 13 décembre au président américain, et mené par un groupe d'étude chargé de se pencher sur les pratiques de surveillance de l'Agence américaine du renseignement (NSA), avait conseillé au président de séparer les directions. Le Président devrait prononcer en janvier un discours sur la régulation des programmes de surveillance.

[DataSecurityBreach] Nerverquest, un trojan qui pourrait bien gâcher les fêtes de Noël

Kaspersky Lab vient d'identifier un programme malicieux capable d'attaquer « n'importe quelle banque dans le monde ». Ce cheval de Troie bancaire a été découvert en juillet 2013 et aurait déjà effectué plusieurs milliers de tentatives d'infection sur 28 sites bancaires de par le monde. Baptisé Neverquest, le trojan utilise la quasi-totalité des techniques connues pour détourner de l'argent. Les chercheurs de Kaspersky Lab estiment que le trojan reste cependant encore sous-utilisé et qu'il pourrait causer des dommages bien plus importants aux banques en ligne et à leurs clients.

[Le Monde Informatique] Des chercheurs démontrent un lien entre malware et haut-parleurs des PC

BadBios n'en finit pas de faire parler de lui. Le chercheur Dragos Ruiu avait découvert il y a quelques mois qu'un logiciel malveillant, qu'il a baptisé BadBios, pouvait se propager d'un ordinateur à un autre en utilisant les haut-parleurs et les micros des PC. Une récente recherche réalisée par le Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), un laboratoire de recherche situé près de Bonn en Allemagne, vient de confirmer cette théorie. Le malware recréé par le laboratoire s'est avéré capable de transmettre des informations entre ordinateurs en utilisant des ondes sonores à haute fréquence, inaudibles par l'oreille humaine. Les ordinateurs portables utilisés pour les tests ont pu communiquer à une distance de 20 mètres, se transmettant des données de manière très lente mais suffisamment rapide pour transmettre des séquences de lettres, des mots de passe, des clés de chiffrement PGP et d'autres micro-informations.

[Haaretz] Israël et les saoudiens préparent un nouveau ver informatique contre le programme nucléaire iranien

Selon une « source informée » du journal Iranien Fars, les services secrets saoudiens et israéliens auraient envoyé à Vienne le 24 novembre des représentants afin de discuter en secret de la « collaboration bilatérale en matière de renseignement et d'opérations de sabotage contre le programme nucléaire iranien ». Une des propositions soulevée aurait été le développement d'un logiciel malveillant plus sophistiqué que Stuxnet, qui permettrait d'espionner et de détruire les infrastructures nucléaires iraniennes. Le chef des services secrets saoudiens, le Prince Bandar bin Sultan, aurait pris part à une rencontre entre le Premier ministre israélien, Benjamin Netanyahu, et le Président de la République François Hollande.

[PressTV] Israël mène une cyberguerre contre le Liban

Le comité libanais en charge de l'évaluation du danger posé par la tour télécom israélienne dirigée vers le territoire libanais a informé le parlement des dernières activités d'espionnage d'Israël. Selon le rapport du comité, Israël mènerait une cyber guerre contre le Liban, en violant les lois nationales de protection de la vie privée et en ayant infiltré les réseaux de communication officiels ainsi que ceux de la force de l'ONU sur place, la FINUL. Le 7

novembre dernier, Beyrouth avait lancé une enquête sur le matériel d'interception des communications et d'espionnage mis en place par Israël le long de la frontière, indiquant que le Liban ne resterait pas inactif si les allégations d'espionnage s'avéraient fondées. L'enquête avait révélé la présence de 39 sites le long de la frontière destinés à l'espionnage du territoire libanais.

[Cyberwarzone] Padvish, l'antivirus iranien

Le premier antivirus national iranien a été révélé à l'Iran Elecomp 2013 comme le rapporte Mehr News. Baptisé « Padvish », c'est à dire « piège à souris » en persan, il a été construit uniquement sur la base de savoir-faire nationaux. Il est prévu que cet antivirus soit rendu disponible à l'exportation sous trois ans.

[MercoPress] L'Argentine et le Brésil coordonnent leurs efforts en cyberdéfense dans le cadre de l'UNASUR

Chefs d'Etats et ministres brésiliens et argentins ont échangé très régulièrement au cours de ces deux derniers mois au sujet de la cyberdéfense. La présidente brésilienne, Mme Dilma Rousseff, avait réagi très vivement aux révélations de l'espionnage de la NSA, déclarant vouloir mettre en place un dispositif permettant de se défendre contre les procédés américains. Ce dispositif pourrait se faire dans le cadre d'accords au sein de l'UNASUR, selon les déclarations du ministre argentin Augustin Rossi le 22 novembre dernier.

[01.Net] Tor pourrait devenir une technologie standard du web

Selon Technology Review, des ingénieurs de l'IETF - organisme qui produit la plupart des nouveaux standards de l'Internet - ont pris contact avec les responsables de Tor afin de les inciter à les aider dans leur effort. Afin de répondre aux révélations sur la NSA, les ingénieurs de l'IETF cherchent à renforcer le niveau de sécurité des protocoles de communication sur Internet, en proposant par exemple que le protocole HTTPS soit activé par défaut pour la navigation sur internet. Tor complèterait bien ce dispositif grâce à sa technologie d'anonymisation. La fondation Tor reste cependant prudente car si ce projet lui apporterait une grande légitimité, elle craint un affaiblissement du niveau technologique de son service du fait de la nécessité de collaborer avec des tiers.

[ITEspresso] Sécurité IT: vers une année prolifique pour la cybercriminalité

Dans son rapport annuel « Security Predictions », Trend Micro prédit que l'année 2014 sera une année très prolifique en matière de cybercriminalité. Si l'on peut s'attendre à « au moins » une cyberattaque massive par mois, les cybercriminels devraient chercher à profiter de la complexification de l'architecture des systèmes d'information due à la mobilité, le très haut débit, le cloud et la virtualisation. Smartphones et tablettes devraient être systématiquement ciblés afin de toucher les entreprises et dérober du contenu à forte valeur ajoutée. Trend Micro estime que le système d'exploitation Android, qui a fait l'objet de 92% des menaces répertoriées sur mobile en 2013, devrait être la cible en 2014 de 3 millions de d'applications malveillantes. Les types de cyberattaques qui auront le vent en poupe sont le phishing, les techniques de « man-on-the-middle » permettant de contourner les systèmes d'authentification sophistiqués et les rançongiciels. Trend Micro craint également que la fin du support de Windows XP augmente drastiquement la vulnérabilité de millions d'entreprises et d'utilisateurs.

[Info-Security] L'ENISA publie un guide pour la sécurisation des infrastructures critiques

L'ENISA a publié un guide de bonnes pratiques à destination des Computer Emergency Response Team (CERTs) spécialisés dans les systèmes de contrôles industriels. L'importance de ces systèmes, vitaux pour de nombreux pays, ainsi que la fréquence à laquelle ils sont attaqués, a motivé la rédaction de ce guide.

[Global Security Mag] Nouveau rapport de l'ENISA

Le rapport émis par l'Agence pour la cybersécurité de l'UE (ENISA) insiste sur la nécessité d'utiliser le chiffrement pour assurer la sécurité des données personnelles. En plus de ce chiffrement, les entreprises devraient également recruter du personnel spécialisé capable de mettre en œuvre les dernières mesures cryptographiques pour la protection des données.

[The Washington Post] Un rapport montre des faiblesses dans la cybersécurité du DHS

Selon un audit, le Department of Homeland Security américain n'a pas mis en place pour lui-même les recommandations qu'il formule au niveau national. Le sénateur Tom Coburn a vivement critiqué le DHS suite à ce rapport, affirmant que « le rapport montre des gouffres en termes de sécurité, ignorant certaines protections basiques qui seraient évidentes pour un enfant de 13 ans ». Le DHS avait pourtant initié une revue de sa sécurité et amorcé certaines réformes visant à augmenter la protection de ses systèmes d'information, notamment pour mieux protéger les documents top secrets.

Quelle place pour la cybersécurité dans la gouvernance d'Internet ?

En 20 ans, Internet est passé d'un outil partagé par quelques universitaires à un outil de masse utilisé par plus de 2.4 milliards d'individus à travers le monde[1]. La multitude des acteurs et son caractère décentralisé et ouvert sont venus remettre en cause le système westphalien fondé sur la souveraineté des Etats. Au début des années 2000, la gouvernance d'Internet est devenu un sujet de discussion important au sein de la communauté internationale, les Etats se préoccupant de plus en plus de leur souveraineté dans le cyberespace. La réponse à la question "Qui dirige Internet ?" n'a pas encore trouvé de réponse, où plutôt en reçoit une multitude regroupée sous le terme de gouvernance globale d'Internet. Gouvernance qui se définit comme *« l'élaboration et l'application par les Etats, le secteur privé et la société civile, chacun selon son rôle, de principes, normes, règles, procédures de prise de décision et programmes communs propres à modeler l'évolution et l'utilisation de l'Internet »*[2]. Compte tenu de la place grandissante de la cybersécurité dans les débats publics, il faut désormais s'interroger sur la place de la sécurité informatique au sein de la gouvernance d'Internet et sur le rôle que peuvent jouer les différents acteurs.

La cybersécurité : un sujet en marge de la gouvernance mondiale

La cybersécurité a toujours eu sa place au sein des débats sur la gouvernance d'Internet. Cependant, celle-ci a fortement évolué au cours des dernières années au point de devenir aujourd'hui un sujet à part entière. Dès le premier Sommet mondial sur la société de l'information qui s'est tenu à Genève en 2003, la cybersécurité était abordée. En revanche, l'espace dédié à la sécurité informatique a longtemps été contenu dans un espace reculé, occupé par quelques spécialistes et soulevant peu l'intérêt du grand public. Depuis 2005 à Tunis, ou lors de conférences annuelles, les questions de cybersécurité sont abordées et font l'objet d'une attention particulière dans la ligne d'action numéro 5 (C5 « Etablir la confiance et la sécurité dans l'utilisation des TIC »). En revanche son auditoire s'est peu élargi, les parties présentes lui préférant des sujets tels la place d'Internet dans la société, l'accessibilité à Internet ou la protection des enfants dans le cyberespace.

Dès 2007, l'Union internationale des télécommunications (UIT) s'est activement saisie de cette question en lançant l'Agenda global sur la cybersécurité, cadre de coopération entre les acteurs de la sécurité informatique. Il a pour objectif d'aider les Etats à lutter contre la cybercriminalité et de créer des règles de bonne conduite et des standards de sécurité afin de protéger les réseaux et systèmes d'information. L'UIT a également mis en place un centre de réponse globale pour aider les Etats à mettre en œuvre les mesures recommandées. Enfin, un Partenariat multilatéral international contre les cyberattaques (IMPACT), bras exécutif de l'UIT sur la cybersécurité, a été créé. Il rassemble les gouvernements, chercheurs et experts en sécurité informatique et a pour objectif d'améliorer les capacités de la communauté internationale à lutter contre les cyberattaques.

[1] Mary MEEKER, LIANG Wu*, 2013 Internet Trends*, KPCB, 30 mai 2013, disponible sur http://www.kpcb.com/insights/2013-internet-trends

[2] UIT, *Agenda de Tunis pour la société de l'information*, Sommet mondial sur la société de l'information, Document WSIS-05/TUNIS/DOC/6(Rév.1)-F, 18 novembre 2005, p.8 disponible sur http://www.itu.int/wsis/docs2/tunis/off/6rev1-fr.pdf

D'autres organisations internationales et enceintes de réflexion se sont également saisies de ce débat. Ainsi, l'Organisation de coopération et de développement économiques (OCDE) fut la première à reconnaître l'importance de sécurité dans le développement d'Internet. Elle a publié, en 1992, des *Lignes directrices* sur la sécurité des systèmes d'information et des réseaux[3] qui ont pour objectif final de soutenir la croissance et l'innovation. Révisées en 2002[4] puis en 2012[5], elles intègrent la *Recommandation pour la protection des infrastructures critiques*[6] de 2008 et prennent en compte les évolutions technologiques afin de mieux accompagner les Etats dans leurs politiques de cybersécurité. L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), dont le rôle a été renforcé en mai dernier[7], agit également dans le secteur de la cybersécurité en *« intervenant en tant qu'expert en matière de sécurité des réseaux et de l'information auprès des autorités nationales et des institutions européennes »*[8] et *« en favorisant l'échange de meilleures pratiques »*[9]. Enfin, on peut citer les conférences internationales pour le cyberespace qui se sont tenues en 2011 à Londres et en 2012 à Budapest et qui ont fait de la cybersécurité un des sujets centraux. Si la cybersécurité a une place restreinte au sein des forums consacrés à la gouvernance proprement dite, elle occupe un espace important au sein d'organisation spécialisées sur les télécommunications et la sécurité.

La cybersécurité : l'apanage des spécialistes et des Etats

Plusieurs acteurs participent à la maintenance et au développement d'Internet, que ce soit des infrastructures physiques ou de la couche logique. Ces acteurs peuvent être répartis entre quatre catégories. D'une part on trouve les Etats dont les revendications sur le cyberespace sont croissantes bien que parfois très différentes. D'autre part la société civile joue un rôle majeur dans la défense des droits (sociaux, civils ou politiques) des utilisateurs ou de principes tels la neutralité du net[10]. Plusieurs associations et fondations portent la voix des utilisateurs, à l'instar de l'Electronic Frontier Foundation, association américaine dont le but est la défense de la liberté sur Internet, ou de l'Internet Society (ISOC) qui a pour fonction de participer à la croissance d'Internet, au respect des protocoles ouverts et à la possibilité pour chaque personne de rejoindre le réseau. Les organisations internationales et groupes de travail internationaux à l'image de l'Internet Engineering Task Force, du World Wide Web Consortium (W3C) ou de l'UIT ont une place très importante dans le développement d'Internet, notamment au plan technique. L'ICANN, qui a pour mission la gestion des noms de domaine terminaux (TLD), des adresses IP et des serveurs de noms racines (DNS root servers), a un statut plus ambigu tant ses liens avec l'administration américaine sont forts (et sont source de contestations). Enfin, le secteur privé est particulièrement représenté, la couche physique étant principalement propriété d'entreprises privées et les géants d'Internet (Google, Facebook, Apple, Microsoft) pesant un poids considérable dans l'économie mondiale.

---

[3] OECD, *Guidelines for the Security of Information Systems*, 1992, disponible sur http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm

[4] OECD, *Guidelines for the Security of Information Systems and Networks*, 2002, disponible sur http://www.oecd.org/sti/ieconomy/15582260.pdf

[5] OECD, *Review of the 2002 Security Guidelines*, 2012, disponible sur http://www.oecd.org/sti/ieconomy/Security%20guidelines%20review.pdf

[6] OECD, *Recommendation of the Council on the Protection of Critical Information Infrastructures*, 2008, disponible sur http://www.oecd.org/sti/40825404.pdf

[7] UE, Regulation (EU) No 526/2013 of the European Parliament and of the Council concerning the European Agency for Network and Information Security (ENISA), 21 mai 2013, disponible sur http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

[8] http://www.enisa.europa.eu/media/enisa-en-francais/

[9] *Ibid.*

[10] La neutralité d'Internet se définit comme le droit pour les utilisateurs d'accéder à tout le contenu du web et d'utiliser toutes les applications qu'ils souhaitent, sans que des restrictions leur soient opposées ou charges imposées par les opérateurs ou les Etats.

Mais quel est le poids de ces acteurs sur les débats et actions ayant trait à la cybersécurité ?

L'étude des différentes enceintes au sein desquelles la cybersécurité est largement un objet d'étude laisse songeur quant à l'emploi des termes « gouvernance multi-acteurs » pour ce domaine. L'activisme de l'UIT , s'il correspond à l'esprit de ses missions, doit être relevé. En effet, alors que l'UIT revendique son rôle dans la gouvernance d'Internet et souhaite voir les missions de l'ICANN lui être attribuées, plusieurs voix se sont élevées afin de protester contre cette volonté de mainmise sur la gestion des noms de domaine terminaux par un organe dont les membres sont des Etats. Cela, selon ses détracteurs, permettrait aux Etats d'assurer un contrôle beaucoup plus grand sur le réseau mondial et remettrait en cause des principes tels la neutralité du net. La multiplication des initiatives de l'UIT en la matière laisse soupçonner une volonté de s'imposer dans un secteur stratégique pour s'affirmer comme un acteur incontournable de la gouvernance. Cette situation place donc les Etats dans une situation de quasi monopole pour l'émergence de nouveaux standards internationaux. Il faut noter la présence de nombreux experts en sécurité informatique dans le processus d'élaboration des standards et bonnes pratiques. En effet, la technicité du sujet nécessite l'apport de connaissances par des chercheurs et ingénieurs. Cette collaboration est d'ailleurs largement revendiquée par les organisations internationales. Peut-être faut-il y avoir le souhait de diminuer la seule place des Etats dans la création de ces normes. Cependant, leur adoption étant soumise aux votes de ces derniers, elles resteront très politisées.

Les forums de réflexion sur la gouvernance consacrent également du temps à la cybersécurité. Mais là aussi les intervenants se limitent à quelques spécialistes et représentants d'Etats. ***La cybersécurité ne semble pas être un domaine qui intéresse la société civile au point que celle-ci souhaite faire entendre sa voix dans l'élaboration de nouvelles règles.*** Ceci est parfaitement regrettable compte tenu du fait que l'équilibre entre sécurité et respect de principes tels les droits de l'homme et neutralité du net est difficile à atteindre. En parallèle de ces forums dominés par les Etats, ont été créées des associations qui ont pour mission de réfléchir aux évolutions de la cybersécurité afin de renforcer la protection des réseaux et systèmes d'informations des entreprises et infrastructures critiques. Elles sont particulièrement présentes aux Etats-Unis où la cybersécurité est devenu un sujet majeur. A titre d'exemple on peut citer le Centre pour la sécurité d'Internet, organisation à but non lucratif qui a pour mission d'améliorer la cybersécurité et la capacité des entreprises des secteurs privé et public à résister aux cyberattaques, ou le Conseil de la cybersécurité, organisation à but non lucratif dédiée à la sécurité d'un Internet ouvert. Dirigé par l'ancien numéro 2 du Département de la sécurité nationale, il est principalement composé d'anciens fonctionnaires de l'administration fédérale ainsi que de quelques directeurs d'entreprises de sécurité informatique. En revanche, la société civile est totalement absente. Ce qui est ici intéressant est la proclamée indépendance de ses membres, pourtant tous très liés à l'administration américaine. Nous nous retrouvons donc face à une situation où, comme pour l'ICANN, une association à but non lucratif souhaite influencer la politique américaine, voire internationale, en matière de cybersécurité tout en entretenant des liens étroits avec le gouvernement américain.

Bien que sujet soit fondamental pour le devenir d'Internet, la cybersécurité reste aujourd'hui une affaire de spécialistes. Au-delà de la question de l'efficacité des mesures prônées, il est indispensable que la société civile s'impose afin que la cybersécurité ne devienne pas une menace pour la démocratie et un Internet ouvert.

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

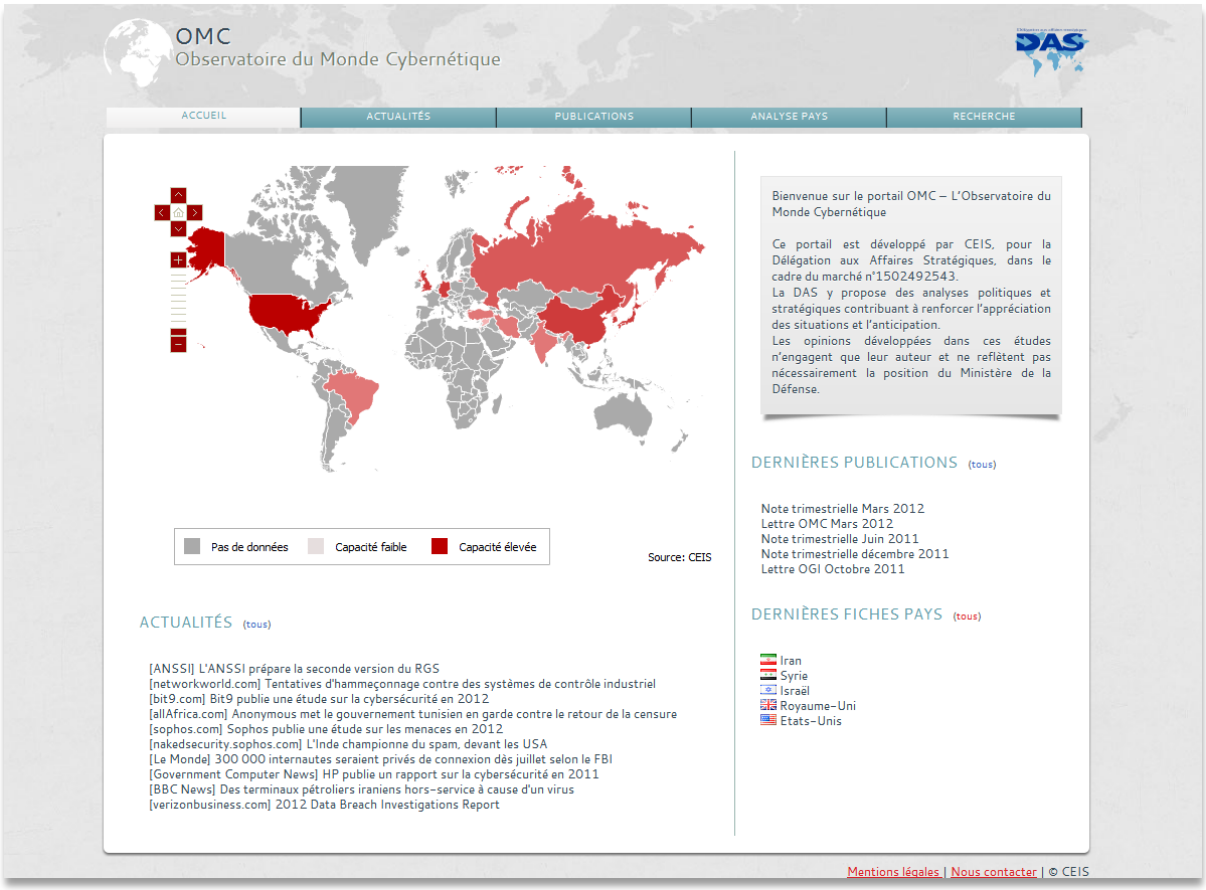

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Web2Business 2014	Paris	09 janvier
9th ETSI Security Workshop	Sophia Antipolis	15 - 16 janvier
Panorama de la cybercriminalité du CLUSIF	Paris	16 janvier
Forum International de la Cybersécurité	Lille	21- 22 janvier
Université AFCDP des Correspondants Informatique et Libertés	Issy-les-Moulineaux	27 janvier
Les débats Qualys Security Community	Paris	4 février
Dîner-débat, le cercle européen de la sécurité et des systèmes d'information	Paris	13 février
ITMeetings, palais des festivals et des Congrès de Cannes	Cannes	19 - 20 mars
3ème congrès national de la sécurité des SI de Santé	Le Mans	31 mars

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