Observatoire du Monde Cybernétique

Lettre n°11 – Novembre 2012

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

[L'Express] Retour sur les attaques de l'Elysée

Selon les informations recueillies par L'Express, les États-Unis seraient à l'origine de la cyberattaque dont a été victime l'Élysée en mai 2012. Les conseillers de Nicolas Sarkozy auraient été contactés via un faux profil sur Facebook (*social engineering*) les invitant à entrer leurs identifiants et mots de passe sur une fausse page intranet de l'Elysée (phishing). La question de savoir comment des personnes extérieures ont pu reproduire assez fidèlement l'intranet de l'Elysée reste entière. Les hackers auraient ensuite installé un ver *« affichant les mêmes fonctionnalités que Flame »* sur les ordinateurs, récupérant un certain nombre de fichiers confidentiels. L'Express annonce *: « La Toile n'est pas un champ de bataille comme les autres. Oubliez les codes de l'honneur, les conventions internationales ou les alliances. Tous les coups sont permis. Et mieux vaut avoir les moyens de se battre. Dans le cyberespace, personne ne vous entendra crier. »*

Dans une interview accordée au même journal, Janet Napolitano, secrétaire d'État à la Sécurité intérieure des États-Unis, n'a pas souhaité infirmer ou confirmer ces accusations. Elle a, pour seule réponse, indiqué que les Etats-Unis n'ont pas *« de partenaire plus important que la France ».* Elle a par ailleurs expliqué que le budget de son pays dans le domaine de la cybersécurité avait augmenté de 40% cette année, et que ce chiffre bondira jusqu'à 75% en 2013, *« un effort très important dans le contexte actuel ».*

[PC Inpact] Le sénateur Jean-Marie Bockel relance le gouvernement

Jean-Marie Bockel relance le gouvernement à propos des suites de son rapport du mois de juillet sur la cybersécurité. Le ministre de la Défense Jean-Yves Le Drian dit examiner le rapport et ses propositions, mais rappelle que des efforts financiers importants sont déjà consentis afin d'augmenter les effectifs de la cyberdéfense. Le livre blanc qui doit paraître début 2013 devra intégrer le travail du rapport et fixer le cap pour le pays en matière de cyberdéfense pour les quatre années à venir.

[Silicon] Cybersécurité : l'Europe soutient la recherche

Au sein du septième-programme cadre pour la recherche, l'UE consacre 350 millions d'euros à la cybersécurité. Une somme qui sera portée à 400 millions pour le budget du prochain programme (2014-2020). Ces fonds sont alloués à divers projets qui réunissent industriels et universitaires. Par exemple, le projet Ecrypt-II réunit une trentaine d'acteurs dont Orange et l'École normale supérieure autour de l'élaboration d'algorithmes de chiffrement.

[Intelligence Online] Royaume-Uni : Le directeur du GCHQ propose la création d'une cyber-réserve

Au Royaume-Uni, le directeur du Government Communications Headquarters (GCHQ), Iain Lobban, s'inquiète du départ accéléré de ses meilleurs informaticiens vers le privé à la fin de leur formation. La NSA américaine subirait le même problème. Lobban a ainsi proposé devant l'Intelligence & Security Committee la création d'une cyber-réserve, dans le cadre de laquelle les informaticiens partis vers le privé pourraient coopérer avec le GCHQ et les autres instances en charge de la cybersécurité du pays.

[Université de Bristol] Un centre de cybersécurité lancé à l'Université de Bristol au Royaume-Uni

L'Université de Bristol va accueillir un centre d'étude sur la cybersécurité qui formera la *« prochaine génération d'experts cyber »* au Royaume-Uni. Le centre est soutenu par le gouvernement via les services de renseignement du Government Communications Headquarters (GHCQ). Des entreprises comme BAE, HP ou Trend Micro seront présentes pour intervenir lors de conférences.

[Le Mag IT] L'aviation civile s'attaque à la question de la sécurité IT

L'Organisation internationale de l'aviation civile (ICAO) devrait, à l'occasion de sa onzième conférence, se pencher sur la question jusqu'alors peu étudiée de la cybersécurité, *« parce que de nombreuses organisations de l'aviation civile*

s'appuient sur des systèmes électroniques pour des éléments critiques de leurs activités ». Les avions (commande de vol électrique) et les aéroports ont en effet recours à un nombre croissant d'éléments numériques dépendants de la sécurité des réseaux informatiques.

[La Voix de la Russie] Les cyber-exercices de l'OTAN, la vision russe

Le journal Voix de la Russie, détenu par le gouvernement russe, rapporte que les pays de l'OTAN participent du 13 au 16 novembre à des exercices de coopération *« en cas de cyberguerre ».* Le journal cite les efforts de la Bundeswehr allemande et des MI5 et MI6 britanniques dans le domaine. Le directeur du Centre de recherches socio-politiques de Moscou estime que *« le but de ces exercices [serait] assez provocateur et [s'inscrirait] dans le contexte général de la dégradation des relations entre la Russie et l'OTAN ».*

[opex360] Les américains capables d'identifier les cyber-attaquants ?

Lors d'un récent discours, le secrétaire américain à la Défense Leon Panetta a indiqué que les Etats-Unis sauraient, grâce à d'importants investissements réalisés ces dernières années, identifier leurs cyber-attaquants. *« Des agresseurs potentiels doivent être conscients que les Etats-Unis ont la capacité de les localiser et de les tenir pour responsables des actions qui nuisent à l'Amérique et à ses intérêts »*, a-t-il souligné. Cette affirmation viendrait à bout d'un des principaux freins à la riposte dans le cyberespace, permettant ainsi aux Etats-Unis de contre-attaquer en cas de menace des intérêts vitaux de leur nation.

[Washington Post] Etats-Unis : Obama signe une directive secrète définissant les paramètres de l'action militaire dans le cyberespace

Le Washington Post révèle que le Président Obama a signé à la mi-octobre une directive qui encadre les opérations américaines dans le cyberespace. Les paramètres d'action en dehors des réseaux gouvernementaux sont donc désormais définis. En parallèle, le Pentagone élabore des règles d'engagement dans le cyberespace tandis que son patron, Leon Panetta, multiplie les discours peu équivoques sur la volonté américaine de combattre l'Iran dans le cyberespace. Les États-Unis s'estiment ainsi prêts à s'engager dans une cyberguerre dont ils sont aujourd'hui occupés à tracer les contours.

[Air Force Magazine] Achèvement d'un an de beta test sur le "Cyber Range" du Pentagone

La DARPA américaine a annoncé l'issue satisfaisante d'un test d'un an d'un « champ d'essai » en matière de cybersécurité. Il s'agit d'une installation sécurisée et autonome ou les cadres du Pentagone peuvent tester et approuver des technologies complexes de sécurisation des réseaux militaires et économiques.

[Search Security] Quelle articulation entre défense et offense dans les opérations cyber ?

Gary McGraw de Cigital s'inquiète de la surenchère effrénée en matière de capacités offensives cyber. Selon lui, la cherté de la mise en place de cyber-armes comme Stuxnet serait une illusion complète. L'impossibilité de l'attribution encouragerait à l'utilisation de cyber-armes. L'expert préconise la mise en place d'une cybersécurité proactive : si l'ingénierie et la construction de systèmes sécurisés sont moins attirantes que la LIO, c'est bien du côté de la défense que les États-Unis peuvent dépenser plus que leurs ennemis et éviter une cyberguerre dévastatrice et inutile.

[Krypt3ia] "Défense offensive": une idée dangereuse ?

Le blogueur Krypt3ia consacre un article à la "défense offensive" telle que proposée par des sociétés comme CrowdStrike. Ces dernières proposeraient aux entreprises de se faire justice soi-même et de contre-attaquer les pirates qui auraient volé leurs données. Sans même évoquer les difficultés légales que ces ripostes soulèvent, Krypt3ia juge cette idée « dangereuse » pour plusieurs raisons : les difficultés d'attribution pourraient amener à attaquer des adresses IP n'ayant rien à voir avec l'attaque initiale ; les entreprises vengeresses constitueraient ainsi une sorte « d'Anonymous corporate » ; se venger n'apporterait rien de bénéfique à l'entreprise ; et

ces attaques de vengeance seraient le prélude dangereux aux attaques préventives.

[Defense News] Coopération accrue entre les pays scandinaves en matière de cybersécurité

Les pays scandinaves (Danemark, Suède et Norvège) ont établi un plan de coopération prévoyant la mise en place de liens permanents entre leurs différents centres de cyberdéfense. Le partenariat pourrait rapidement s'étendre aux pays baltes.

[Intelligence Online] Les attaques contre leurs compagnies pétrolières incitent les pays du Golfe à se défendre

Les récentes attaques contre les compagnies RasGas et Saudi Aramco incitent les pays du Golfe à s'équiper en matière de cybersécurité. Abou Dhabi vient d'engager la société américaine Cyberpoint International pour l'aider à mettre en place son Electronic Security Authority. Le Qatar aurait quant à lui approché la société Booz Allen Hamilton, qui sous-traite habituellement pour les agences fédérales américaines.

[Mag Securs] L'Inde soigne son approche de la cyber-sécurité

L'Inde va prochainement nommer un Coordinateur National de la cybersécurité (NCSC) afin d'harmoniser les stratégies du pays dans le cyberespace. L'actuel chef du CERT national serait pressenti pour ce poste. De plus, l'Agence de la Défense et l'Organisation de la Recherche Technique Nationale (NTRO) devrait désormais faire office d'agence de cybersécurité du pays. Des CERT pour les infrastructures critiques (énergie et aviation) vont être créés. La collaboration public-privé devrait être accrue.

[Lockheed Martin - Cyber Alliance] Préserver la sécurité des systèmes d'information

Lockheed Martin a publié en collaboration avec le groupe Cyber Alliance (HP, Intel, Cisco, McAfee entre autres) un rapport sur *« La cybersécurité et les technologies transformatrices - maintenir la sécurité des systèmes »*. Ce rapport avance que 85% des décideurs à Washington perçoivent la cybersécurité comme une priorité. Le challenge pour les organisations gouvernementales consisterait à adopter des technologies avancées qui permettent de réduire les coûts, sans pour autant sacrifier la sécurité.

[NIST] L'institut américain des normes publie un rapport sur la sécurité des mobiles

L'Institut national des normes et de la technologie américain (NIST) a publié un rapport sur la sécurité des appareils mobiles. Citant les chiffres de l'exposition accrue de ces terminaux au piratage, le NIST préconise une sécurisation urgente de ceux-ci dans le cadre de l'entreprise où le BYOD se répand à une vitesse fulgurante. Des techniques de sécurisation plus ou moins élaborées sont mises en avant dans le document.

[ENISA] Rapport de l'ENISA sur le droit à l'oubli

L'ENISA publie un rapport sur le "droit à l'oubli" sur Internet. Le document opte pour un point de vue technique afin de compléter les débats politiques et légaux en cours à Bruxelles et à Strasbourg. Le rapport s'intéresse à la mise en œuvre technique des lois sur l'effacement des données personnelles. Selon l'Agence, la coopération des moteurs de recherche et fournisseurs d'accès est évidemment absolument cruciale. Elle encourage également les chercheurs en informatique à développer des programmes qui empêchent la collecte automatique de données.

Shamoon : une nouvelle menace visant les infrastructures critiques ?

Qu'est-ce que Shamoon ?
Shamoon est un virus informatique qui a frappé l'industrie pétrolière au courant de l'été 2012.

Cible et impact.
Le virus Shamoon aurait visé une seule organisation dans le secteur de l'énergie : le groupe Saoudien Saudi Aramco. Plus de 30 000 ordinateurs ont été infectés et rendus inutilisables.

Mode opératoire

Le virus Shamoon écrase des données dans le MBR "Master Boot Record", empêchant ainsi la routine d'amorçage de s'exécuter. Il en résulte que le PC est rendu inutilisable et ne peut être redémarré.

Après l'infection, trois modules qui s'appellent respectivement 'Dropper', 'wiper' et 'reporter', entrent en action :

1. Dropper - Premier et principal composant de l'infection, il active le deuxième module.
2. Wiper - Se charge d'effacer définitivement les fichiers systèmes vitaux en les remplaçant par une photo du drapeau américain en flamme.
3. Reporter - rapporte des informations sur l'infection à un autre PC dont les fichiers ont été également touchés, les informations sont ensuite renvoyées à l'attaquant.

Source : http://blogs.rsa.com/rsa-first-watch-team/dark-side-of-shamoon/

C'est en particulier l'appellation du module 'wiper' qui a suscité l'inquiétude, car elle aurait pu indiquer un lien avec la famille Stuxnet/Duqu/Flame. Après analyse par Symantec, puis par Kaspersky Lab, il est apparu que ce n'était pas le cas[1].

Un autre aspect confus de Shamoon est qu'il se sert du pilote RawDisk d'Eldos pour avoir un accès « administrateur » au disque de la machine. Or, cette partie du code est inutile étant donné que Windows 7 autorise l'accès au disque aux utilisateurs standards. Ce qui laisse penser que les instigateurs du virus Shamoon ne sont pas être des programmeurs de très haut niveau. Plusieurs autres erreurs de code laissent penser qu'il s'agit même d'amateurs.

Les infrastructures critiques visées ?

Après Stuxnet et Duqu, Shamoon illustre une fois de plus la progression de la dangerosité et de l'irréversibilité des dommages entrainés par des attaques visant les infrastructures critiques. Peu importe que Shamoon soit l'œuvre d'amateurs ou un acte de guerre numérique lancé par un pays ennemi - les deux extrêmes du spectre. Ce qui est préoccupant, c'est le manque permanent de protection de nombreux opérateurs d'infrastructures sensibles face à des attaques extérieures.

Une motivation incertaine

Shamoon est le dernier d'une série d'attaques (Stuxnet et Duqu) qui ont ciblé des infrastructures vitales. Cependant l'objectif du virus Stuxnet était clair : frapper les infrastructures nucléaires en Iran, quand les auteurs de Duqu ont cherché à infiltrer les réseaux afin de voler des données. Le virus Shamoon présente un mode opératoire relativement original : il écrase les données afin de rendre les postes de travail inutilisables, chose rarement vue dans les attaques ciblées.

Ce virus a cependant retenu l'attention parce qu'il était question d'une attaque *« visant une seule organisation dans le secteur de l'énergie ».* En outre, l'on a relevé dans le code une référence à l'Arabian Gulf'.

La question de qui est derrière le virus Shamoon reste officiellement sans réponse, même si plusieurs doigts sont pointés vers l'Iran. Pour les saoudiens, l'infection de ses ordinateurs par le virus Shamoon ne pouvait réussir sans un accès physique au réseau interne. Cela les a amené à se questionner quant à la loyauté du personnel et au respect des mesures et politiques de sécurité physique.

En tout cas, Shamoon semble avoir aidé à la prise de conscience des risques cyber dans la région du Golf ou, du moins, à l'accélération de la mise en place de systèmes de cybersécurité. En effet, cette attaque et celle dont a été victime deux semaines plus tard le groupe qatari Rasgas, incitent les pays du Golfe à s'équiper en matière de cybersécurité. Abou Dhabi vient d'engager la société américaine Cyberpoint International pour l'aider à mettre en place son Electronic Security Authority. Le Qatar aurait quant à lui approché la société Booz Allen Hamilton, qui sous-traite habituellement pour les agences fédérales américaines.

[1] RSA, Kaspersky et Symantec ont publié le mode opératoire détaillé du virus.

Gouvernance de l'Internet : quels enjeux pour la Conférence Mondiale des Télécommunications Internationales ?

Du 3 au 14 décembre prochains, les membres de l'UIT se réuniront à Dubaï dans le cadre de la Conférence mondiale des télécommunications internationales (CMTI) [ou *World Conference of International Telecommunications (WCIT-12)*]. Objectif : réviser le Règlement des télécommunications internationales (RTI) et mieux prendre en compte des mutations liées aux TIC.

Négocié pour la première fois en 1988, en Australie, ce traité international a été conçu pour *« faciliter, à l'échelle internationale, l'interconnexion et l'interopérabilité des services d'information et de communication ».* Il *« expose les principes généraux qui garantissent la libre circulation des informations dans le monde, encouragent l'accès équitable pour tous, à des conditions abordables et constitue la pierre angulaire de la recherche permanente de l'innovation et de l'expansion des marchés. »*[2]

En amont de la conférence, des Etats et entreprises prennent déjà position. D'un côté, certains (les Etats-Unis, Google…) alertent l'opinion publique sur un scénario catastrophe qui verrait l'UIT disposer de compétences accrues en matière de gouvernance Internet, menant droit à une censure généralisée du réseau. De l'autre, certains Etats (recoupant généralement ceux composant l'OCS – Organisation de Coopération de Shanghai), souhaitent lutter contre la mainmise des Etats-Unis sur Internet et transférer à l'UIT certaines compétences.

Enfin, d'autres Etats tardent à prendre position. Si la France a lancé une consultation ouverte sur le sujet, sa position officielle n'est en effet toujours pas connue. En témoigne le rappel de la députée Laure de la Raudière[3]. Récemment toutefois, l'Europe a pris position en diffusant une Proposition de résolution commune[4] dans laquelle elle défend elle-aussi la liberté d'expression, ainsi que « les principes d'un marché libre, la neutralité de l'internet et l'entrepreneuriat ».

Quelle est la pertinence de cette opposition schématique entre « pro-liberté d'expression » et « pro-censure » telle que présentée par les médias ? Au-delà des scénarios catastrophe, quel sera réellement l'impact de cette conférence ?

« L'UIT est le plus mauvais endroit pour décider de l'avenir d'Internet »[5]

Selon Google, il serait dangereux de transférer des compétences à l'UIT, puisque certains Gouvernements y étant représentés *« ne soutiennent pas un internet libre et ouvert »*. Cette vision manichéenne est partagée par de nombreux observateurs qui préconisent le maintien du système actuel, au cœur duquel l'ICANN joue un rôle central.

Ces observateurs fustigent notamment l'opacité de fonctionnement de l'UIT. Les débats auront lieu à huis clos, la conférence n'a été précédée d'aucun document préparatoire public, etc. Il existe même des sites

[2] CMTI-12 : A propos de la Conférence - http://www.itu.int/fr/wcit-12/Pages/overview.aspx
[3] Question écrite au premier ministre - http://questions.assemblee-nationale.fr/q14/14-10028QE.htm
[4] http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=P7-RC-2012-0498&language=FR
[5] http://www.01net.com/editorial/580665/conference-uit-de-dubai-google-s-inquiete-pour-l-avenir-du-web/

proposant des fuites (« leaks ») de documents préparatoires, à l'image de : http://www.wcitleaks.org/. Notons toutefois que nombre de critiques soulèvent l'impérieuse nécessité de réformer également les statuts de l'ICANN, en faisant évoluer l'association vers une plus grande ouverture à l'international.

Sans opter expressément pour le maintien du système actuel, Google semble plaider pour approche « multi-stakeholders » et souhaite préserver la liberté sur un Internet fortement influencé par ses utilisateurs. *« Les gouvernements ne doivent pas décider seuls de l'avenir d'Internet. Les milliards de personnes qui utilisent le Web et les experts qui le conçoivent et l'entretiennent, doivent également participer aux discussions. »* Une position qui peut surprendre, Google maîtrisant presqu'à sa guise quantité de données personnelles d'utilisateurs, parfois au mépris de législations nationales ou régionales en matière de protection des données à caractère personnel[6].

D'autres enjeux annoncés pourraient cependant justifier cette position : certaines propositions, si elles sont adoptées, obligeraient en effet certains opérateurs (comme Youtube ou Skype) à payer des droits de routage.

La « facturation » du trafic Internet – une remise en cause collatérale de la neutralité du Net ?

Au cours de cette conférence sera plus précisément abordée la question du routage et de rémunération, proposition avancée par l'ETNO (European Telecommunications Network Operators' Association)[7]. Objectif : *« permettre l'accroissement des revenus grâce à des accords de tarification de la qualité de service de bout en bout et de la valeur des contenus »* et autoriser le développement de *« nouvelles politiques d'interconnexion basées sur la différenciation des critères de qualité de service pour des services et des types de trafic spécifiques (non uniquement pour les « volumes »). »* Soit, en somme, faire payer les internautes et les entreprises pour un réseau de qualité, pour le routage et la circulation des données.

Cette mesure aurait tout d'abord pour effet collatéral de *« nuire à la liberté de communication »* et ainsi de mener à un Internet *« à plusieurs vitesses »* dans lequel il faudrait payer pour avoir un trafic prioritaire, augmentant ainsi la fracture numérique. La mesure favoriserait largement les opérateurs de poids au détriment des acteurs entrant, freinant ainsi considérablement l'innovation et la compétitivité.

Parce que des technologies d'analyse en profondeur du trafic seraient exigées pour appliquer ces mesures, la Quadrature du Net explique que cela aurait également pour conséquence la mise en péril de la vie privée des internautes. Des critiques globalement partagées par l'Union européenne[8].

Des enjeux sur la forme : quelle force juridique pour le RTI ?

Au cœur des préoccupations enfin, la force juridique des recommandations de l'UIT. Pour l'instant en effet, seules les dispositions du traité de 1988 ont force obligatoire. Toutefois, comme le souligne l'AFNIC, *« certains amendements à l'article 1 du traité proposent de rendre obligatoire l'application des normes et recommandations développées dans le cadre de travaux menés par l'UIT et de leur donner la même valeur qu'aux principes généraux énoncés dans le RTI »*[9]. Cette extension est globalement perçue comme

[6] CNIL : Google devra revoir son utilisation des données personnelles des internautes - http://www.lemonde.fr/technologies/article/2012/10/16/cnil-google-devra-revoir-son-utilisation-des-donnees-personnelles-des-internautes_1775988_651865.html

[7] http://www.laquadrature.net/fr/les-operateurs-dominants-partent-en-guerre-contre-la-neutralite-du-net-via-litu et https://www.cdt.org/files/pdfs/CDT_Analysis_ETNO_Proposal.pdf

[8] http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=P7-RC-2012-0498&language=FR

[9] Voir modification 1.6, pages 9 et 10 http://www.itu.int/en/wcit-12/Documents/draft-future-itrs-public.pdf

potentiellement dangereuse, à la fois par l'AFNIC et par l'ASIC (Association des services internet communautaires), mais aussi par l'Union européenne qui précise que *« le RTI devrait préciser que les recommandations de l'UIT sont des documents non contraignants destinés à encourager les meilleures pratiques ».*

Quels scénarios ?

Plusieurs scénarios sont envisageables à l'issue de la conférence de Dubaï :

1. Le traité reste inchangé, un scénario profitable aux Etats-Unis

Dans ce scénario, les Etats n'arrivent pas à s'entendre, le traité inchangé. Ce scénario favorable aux Etats-Unis est très probable. On se souvient en effet du Sommet mondial de la société de l'information (SMSI) de Genève les 25 et 26 mars 2004, où s'est tenu un « forum mondial consacré à la gouvernance de l'internet ». La proposition avait été faite par de nombreux pays de transférer des pouvoirs à l'IUT. Proposition restée sans effet face à la ferme opposition des Etats-Unis qui dénonçaient déjà à l'époque le risque de bureaucratie et de frein à l'innovation[10].

2. La vision étatique prédomine et la compartimentation d'internet se développe

Le traité est modifié et intègre des mesures importantes sur la cybersécurité telles que perçues par le duo Russie-Chine et exprimées dans leur proposition de Code de bonne conduite sur Internet[11]. L'impact réel et immédiat de cette adoption serait très faible. L'ICANN ne perdrait pas ses prérogatives. Et surtout, cette décision d'intégrer des mesures de cybersécurité ne changerait pas fondamentalement une situation où de nombreux pays pratiquent déjà cette censure. En somme, cela ne ferait que légitimer l'action de certains Etats la pratiquant déjà.

Sur le moyen terme toutefois, de telles dispositions justifieront l'adoption par certains autres Etats de mesures plus intrusives sur le réseau.

Enfin, sur le plus long terme, ce scénario pourrait renforcer la régionalisation et la compartimentation d'Internet. Il s'agirait d'une défaite stratégique majeure pour les américains et pour leur vision de l'internet universel. Chacun se renfermerait sur sa propre conception du réseau, créant une « balkanisation du net ». Cette dynamique est déjà enclenchée, à l'image de l'Internet chinois, ou encore iranien.

3. L'enjeu commercial prend le dessus : la question de la « facturation » du trafic Internet au cœur des débats

En fait, la question de la cybersécurité pourrait ne pas être l'enjeu majeur de cette conférence. C'est l'avis de l'Afnic qui indique que *« le fait, par exemple, que le traité révisé puisse appeler à une meilleure coopération intergouvernementale, sous les auspices de l'UIT, pour la lutte contre le spam, ou le renforcement de la cybersécurité, n'implique pas [de son point de vue] d'impact nécessaire sur le fonctionnement technique de l'Internet »*[12].

[10] http://www.zdnet.fr/actualites/gouvernance-de-l-internet-washington-ne-laissera-pas-l-onu-supplanter-l-icann-39147165.htm
[11] http://larussiedaujourdhui.fr/articles/2012/01/26/internet_un_code_de_conduite_international_est_necessaire_14141.html
[12] http://www.afnic.fr/medias/documents/Dossiers_pour_breves_et_CP/ReponseconsultationpubliqueRTIVF.pdf

Les professeurs Muller et Winsek[13] estiment quant à eux que l'enjeu principal de la conférence n'est pas le contrôle du net. *« C'est la continuation pure et simple de longues batailles sur la manière dont Internet a remis en cause des modèles traditionnels sur les marchés des télécoms. »*

Les conséquences de l'adoption des mesures préconisées par ETNO seraient, selon certains observateurs, catastrophiques pour la neutralité du Net. On assisterait à une *« hausse des prix, à la limitation de l'accès et de l'innovation »*, ce qui mettrait en cause *« l'ouverture et la compétitivité des réseaux… »*. Mais ce n'est pas l'unique enjeu : certains pays en développement pourraient en réalité trouver dans cette rémunération du routage des données une véritable source de revenus, les opérateurs de télécommunication présents sur leurs territoires n'ayant pas le statut d'opérateurs privés.

S'il est difficile d'anticiper les suites réelles de cette conférence de Dubaï en raison de l'opacité entourant les documents de travail, deux enjeux restent essentiels. Le premier étant la volonté, par des pays comme la Chine et la Russie, d'obtenir une plus large marge de manœuvre en matière de gouvernance Internet en transférant une partie des pouvoirs à l'ONU. Mais ceux-là même qui s'estiment lésés par le mode de gouvernance « multi-stakeholders » actuel privilégiant les intérêts des Etats-Unis n'ont pas besoin d'une gouvernance à l'échelle de l'ONU pour justifier un contrôle accru de leur réseau déjà largement effectif. Ils pourraient cependant, à travers une réforme du système de rémunération du routage des données, trouver un avantage non-négligeable.

[13] http://www.technologyandpolicy.org/2012/08/09/a-u-n-takeover-of-the-internet-existential-threat-or-tempest-in-a-teapot/#.ULij0Kz8ITk

Le portail OMC
La nouvelle plateforme de la DAS

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

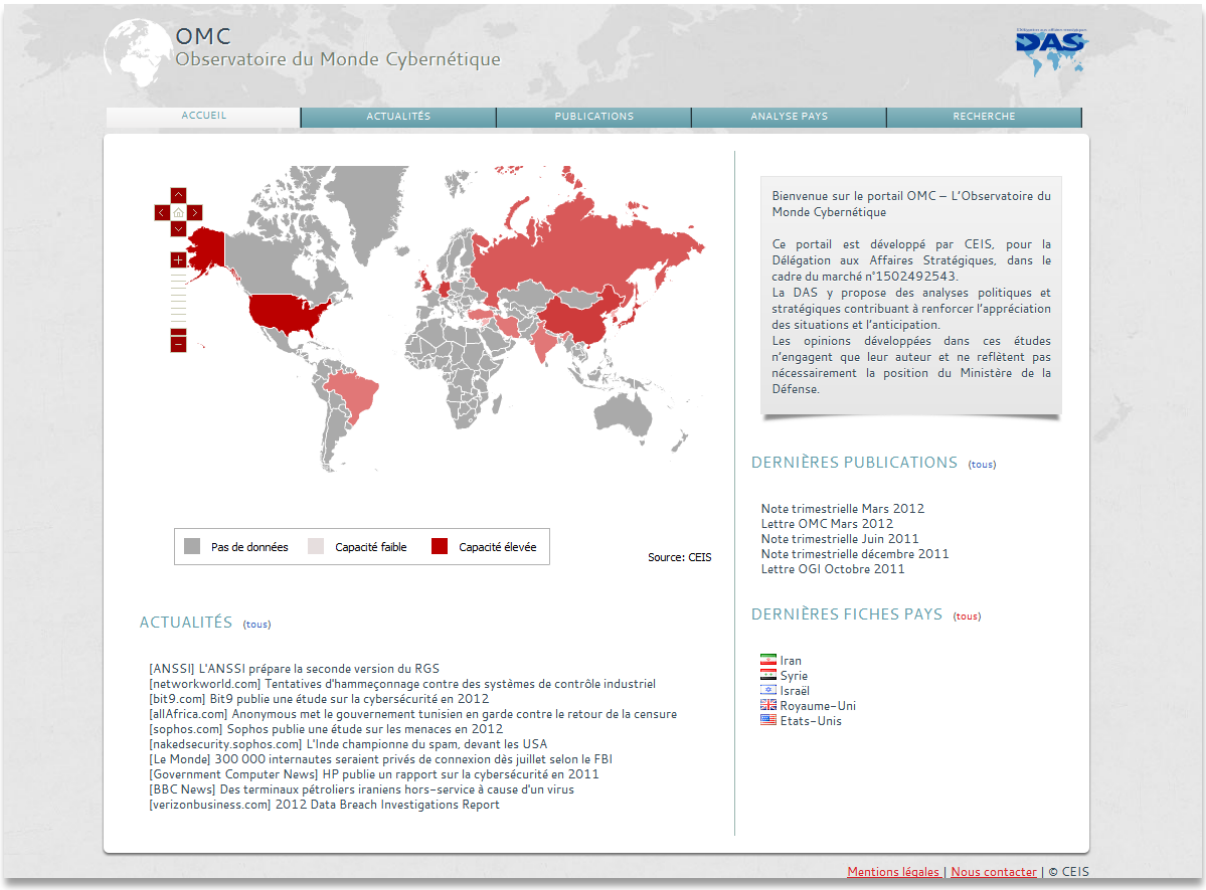

Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

IEEEE International Workshop on Information Forensics and Security	Tenerife, Espagne	2 – 5 décembre
L'Europe face à la cybercriminalité : Problèmes, réponses et perspectives	Paris	3 décembre
Cyber Security Forum Asia	Singapour	3 – 4 décembre
Gartner : Salon *Identity and Access Management*	Las Vegas	3 – 5 décembre
ACSAC (« Annual Computer Security Applications Conference ») 2012	Orlando, FL, Etats-Unis	3 – 7 décembre
Conférence mondiale des télécommunications internationales	Dubai	3 – 14 décembre
NIST : « Random Bit Generation Worksop » 2012	Washington DC	5 – 6 décembre
Colloque CDSE / Europol : "Les entreprises et l'Etat face aux cybermenaces "	Paris	6 décembre
SANS Cyber Defense Initiative (CDI) 2012	Washington DC	7 – 16 décembre
CES Gov 2012	Las Vegas	9 – 11 janvier
Cyber Defence & Network Security 2013	Londres	28 – 31 janvier
Cyber Security for Government Asia 2013	Kuala Lumpur, Malaisie	29 – 30 janvier

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