Observatoire du Monde Cybernétique

Février 2012

Actualités p. 2

- L'exercice PIRANET 2012 mené par l'ANSSI début février a permis d'évaluer la capacité de l'Etat français à résister à une éventuelle attaque informatique de grande ampleur contre ses réseaux.
- La Commission européenne saisit la CJUE afin de vérifier la conformité du traité ACTA avec les droits et libertés fondamentaux.
- Selon le reporter Spencer Ackerman, l'OTAN n'aurait toujours pas adopté de stratégie de protection de ses réseaux.
- INTERPOL ouvrira à Singapour un centre d'innovation, le *Global Complex for Innovation* (IGCI). Opérationnel en 2014, il sera dédié à la R&D dans le secteur de la cyberdéfense.
- Le président russe Dimitri Medvedev a proposé la création d'unités spéciales de lutte contre la cybercriminalité. Le Premier ministre, Vladimir Poutine, a quant à lui souligné l'importance d'une capacité de lutte dans le cyberespace.
- Selon le chef du FBI, les attaques des groupes de *hackers* comme Anonymous et Lulzsec pourraient devenir une vraie menace terroriste pour les institutions américaines.
- Dans un effort de lutte contre les groupes d'activistes opérant sur Internet, le gouvernement américain fait voter le *Cybersecurity Act of 2012*.
- Les militaires américains sont à la recherche de nouveaux talents. Pour le chef de l'*U.S. Army Cyber Command*, la création d'une force militaire composée de spécialistes en informatique est désormais indispensable.
- Lockheed Martin présente son laboratoire de *« cyber-innovation »* : le NCITE. Basé au Royaume Uni, il propose des solutions de pointe en matière de cyberdéfense.
- Selon un rapport publié par Seculert et Zscaler, les cyberattaques ciblant les institutions gouvernementales et les organisations du secteur de la Défense et de l'industrie aéronautique sont en hausse.
- Google acceptera, sur requête de certains Etats, de censurer sa plateforme de blogs *Blogger*.
- Afin de s'assurer un total contrôle sur son *« Internet national »*, l'Iran améliore son système de filtrage.
- Le gouvernement indien veut intercepter les courriels de Yahoo! et Gmail sans solliciter de collaboration légale internationale.
- L'armée brésilienne investit 6 millions de réais (2,6 millions d'euros) dans des logiciels de cyberdéfense et de simulation d'attaques informatiques au profit de son *Centro de Defensa Cibernética do Exército*.

Publications p. 4

Intelligence économique p. 5

Le marché de la cybersurveillance bousculé : quelles évolutions à venir ?

Le 6 décembre 2011, alors que les Révolutions arabes suivent leur cours, Wikileaks rend publique une liste de plus de 1000 documents (plaquettes commerciales, modes d'emplois…) dévoilant les dessous d'un marché de la cybersurveillance de masse. Peu de temps après, l'Europe annonce vouloir interdire l'exportation de ce type de produits vers les régimes autoritaires. Quelles seront les conséquences d'une telle interdiction ? Assisterons-nous au développement d'un marché Sud/Sud de la cybersurveillance ?

Agenda p. 10

L'ANSSI tire des enseignements de son exercice PIRANET 2012

L'exercice PIRANET 2012 mené par l'ANSSI début février a permis d'évaluer la capacité de l'Etat français à résister à une éventuelle attaque informatique de grande ampleur contre ses réseaux. Des acteurs des secteurs de la santé, des transports et des communications électroniques ont participé cette édition 2012 de l'exercice ; ce qui a permis de tester la qualité de circulation de l'information entre toutes les parties concernées.

La CJUE vérifiera la conformité du traité international ACTA

Suite à la signature de l'*Anti-Counterfeiting Trade Agreement* (ACTA) par vingt-deux pays membres de l'UE, la Commission européenne a décidé de saisir la Cour de Justice de l'Union Européenne afin de vérifier que le traité était bien conforme aux droits et libertés fondamentaux de l'UE. L'examen du texte débute le 29 février.

OTAN : quelle stratégie de cyberdéfense ?

Selon le reporter Spencer Ackerman, si les représentants de l'OTAN ont clairement conscience du besoin impérieux de protéger leurs systèmes d'information, ils sont loin de savoir comment les protéger. Comment délimiter les sphères civiles et militaires ? Quel type de cyberattaque déclencherait une réaction au titre de l'article 5 ? Quelle serait la réponse adéquate ? Autant de questions fondamentales qui ne trouveraient toujours pas de réponse claire. Une chose est sûre : ayant fort à faire sur les aspects défensifs, l'OTAN ne devrait pas développer de doctrine offensive pour le moment.

INTERPOL ouvrira un centre d'innovation dédié à la cybercriminalité à Singapour en 2014

INTERPOL compte ouvrir un centre d'innovation à Singapour. Opérationnel en 2014, le *Global Complex for Innovation* (IGCI) sera dédié à la R&D en matière de cyber-défense : lutte contre l'exploitation sexuelle des enfants ; création à faible coût de bases de données sur la cybercriminalité destinées aux pays en voie de développement ; recherches en matière de gouvernance de la cyber-sécurité, etc.

Le projet russe de création d'unités de lutte contre la cybercriminalité en bonne voie

Lors d'une réunion avec le ministère de l'Intérieur, le président russe Dimitri Medvedev a appelé à la création d'unités spéciales de lutte contre la cybercriminalité. Et dans son article intitulé « *Puissance comme garantie de la sécurité nationale pour la Russie* », le Premier ministre et candidat à la présidence russe, Vladimir Poutine, a souligné l'importance d'une capacité de lutte dans le cyberespace. D'après M. Poutine, *« […] Il est de la plus grande importance de posséder des capacités militaires dans le secteur aérospatial et en premier lieu - dans le cyberespace […] »*.

Le FBI et la NSA mettent l'accent sur l'importance des cyber-menaces activistes

Le chef du FBI a mis le Sénat en garde contre les cybercriminels. Les attaques des groupes de *hackers* comme *Anonymous* et *Lulzsec* contre le Nasdaq ou contre le Fonds Monétaire International illustrent la vulnérabilité d'importantes institutions économiques américaines et pourraient évoluer en véritable menace terroriste. Dans une déclaration séparée, le directeur de la NSA a annoncé que ces groupes seraient bientôt capables d'effectuer une attaque massive sur le réseau électrique des Etats-Unis.

Le Congrès américain veut faire passer le *Cybersecurity Act of 2012*

Dans un effort de lutte contre les groupes de cyber-activistes tels *qu'Anonymous* ou *Lulzsec*, le gouvernement américain a décidé d'établir le *Cybersecurity Act of 2012*. Contrairement à SOPA ou PIPA, contre lesquelles les principaux acteurs du web avaient fortement réagi, le *Cybersecurity Act of 2012* a une portée beaucoup plus restreinte. La loi essaye d'établir une analogie entre les groupes hacktivistes et les groupes terroristes tels qu'*Al-Qaeda*, ce qui suscite des craintes de la part des défenseurs des libertés en ligne.

Les militaires américains ont besoin de nouveaux talents

Selon le général Rhett Hernandez, chef de *l'U.S. Army Cyber Command* chargé de la sécurité de l'information pour l'armée de terre, la création d'une force militaire composée de spécialistes en informatique est indispensable, dans un contexte mondial où les cyber-menaces sont en croissance permanente. En décembre dernier, l'Armée de terre américaine avait déjà annoncé la création d'une cyber-brigade opérationnelle.

Lockheed Martin présente son laboratoire de cyber-innovation : le NCITE

Le *NexGen Cyber Innovation and Technology Center* (NCITE), un des centres de recherche de Lockheed Martin basé au Royaume Uni, propose des solutions de pointe en matière de cyber-défense. Le NCITE réserve également une partie de son travail au secteur de la Défense qui devient de plus en plus *« réseau-centrique ».*

Le nombre d'attaques ciblant les secteurs de défense et de l'aéronautique en hausse depuis 2009

Un rapport publié par les chercheurs de Seculert et Zscaler conclut que les cyberattaques ciblées contre les institutions gouvernementales et les organisations du secteur de la Défense et de l'industrie aéronautique sont en hausse. Les attaques prennent souvent la forme de courriels contenant des pièces jointes infectées par des virus (souvent en PDF) exploitant des failles récentes (dites *« failles 0-day »*) ou encore des fausses invitations aux conférences.

Google va censurer les blogs sur son service *Blogger*

Google a annoncé l'arrivée de la censure sur sa plateforme de blogs *Blogger*, en fonction du pays à l'origine de la demande. Une telle mesure permettrait d'agir en conformité avec les lois et les normes morales des pays en question. L'interdiction d'accès à certains blogs pour les utilisateurs desdits pays sera appliquée seulement à la demande des autorités de l'Etat. Le contenu ne sera pas bloqué pour les utilisateurs d'autres pays.

L'Iran veut contrôler son Internet national de près

Dans ses efforts de construction d'un *« Internet National »*, l'Iran aurait amélioré son système de filtrage Internet à tel point que les moyens de contournement classiques commenceraient à devenir inefficaces. Ce renforcement fait suite à l'accroissement des tensions entre l'Iran et les puissances occidentales, et aux accusations d'espionnage de la part de Google, Twitter, et Microsoft sur la population iranienne.

Le gouvernement indien veut intercepter les courriels de Yahoo! et Gmail

Les agences de sécurité indiennes auraient demandé à Google et Yahoo de faire transiter l'envoi de leurs emails par des serveurs situés en Inde, afin de pouvoir lire leur contenu sans solliciter de collaboration légale internationale. Ceci faciliterait la lutte contre le terrorisme, rendue difficile à cause des commissions rogatoires internationales nécessaires si l'adresse mail est hébergée à l'étranger.

L'armée brésilienne prépare un système de prévention contre les cyber-attaques

Suite aux attaques contre les systèmes d'information de diverses institutions financières du pays, l'armée brésilienne a décidé d'investir 6 millions de réais (2,6 millions d'euros) dans des logiciels de cyberdéfense et de simulation d'attaques informatiques. Ces services seront utilisés par le *Centro de Defensa Cibernética do Exército* dans le but de protéger les SI gouvernementaux d'attaques similaires. L'investissement prévu pour le *CDCiber* en 2012 est de 83 millions de réais (36,5 millions d'euros).

[ENISA] Study on data collection and storage in the EU

Dans cette étude, l'ENISA présente une analyse des corpus législatifs des Etats membres de l'UE relatifs aux principes de diffusion restreinte et durées minimales de stockage de données personnelles. L'étude souligne également le fait que très souvent, les politiques de respect de la vie privée annoncées par les fournisseurs de services en ligne sont très éloignées des mesures réellement mises en place.

[Kaspersky Labs] Rapports annuels 2011 sur les cyber-menaces

Les experts de *Kaspersky Labs* ont publié leur traditionnelle étude sur le développement des menaces cybercriminelles (*botnets*, escroqueries, *phishing*, *spams*, etc.) pour l'année 2011. Ce rapport rassemble des informations obtenues et traitées via le *Kaspersky Security Network* (KSN). Trois rapports ont été publiés : « Développement des menaces en 2011 », « Sommaire des statistiques pour 2011 », puis « Spam en 2011 ». L'éditeur d'antivirus y fait un classement des pays les plus dangereux en matière de cyber-sécurité. La Russie est classée comme le pays le plus dangereux avec plus de 55% des internautes ayant été victimes de cyber-attaques.

[McAfee] McAfee Threats Report : Fourth Quarter 2011

McAfee a publié son rapport du quatrième trimestre 2011 détaillant des statistiques sur les logiciels malveillants (leur nombre a dépassé les 75 millions), le nombre de sites infectés (environ 6500 par jour) et l'analyse des tendances des cyber-menaces.

[NIST] Computer Security Incident Handling Guide

Dans sa dernière révision du rapport de réponse à incidents en sécurité informatique, le *National Institute of Standards and Technology* définit sept capacités que tout plan de réponse devrait avoir, comprenant les protocoles de communication avec le Congrès américain, les citoyens, et les médias. Le guide spécifie aussi des modèles de structure d'équipe pour les agences concernées

[SDA] Public-private cooperation in cyber-security

Les approches nationales à la cyber-sécurité varient grandement en Europe et partout dans le monde. Dans certains pays, la responsabilité légale de la lutte contre le piratage incombe aux fournisseurs d'accès, l'expertise technique étant souvent plus importante dans le secteur privé. Quelle partie de la protection doit être laissée aux compagnies privées ? Le partage d'information entre institutions publiques et secteurs privés est-il efficace ? La création de standards permettrait-elle d'améliorer la cyber-sécurité ? La *Security and Defence Agenda* publie son rapport sur ce sujet.

[Diplonews] The state of Cyberwar in the U.S.

Diplonews a publié un rapport sur les méthodes employées par les Etats-Unis pour développer leur suprématie dans le cyberespace. Dans cet environnement, la suprématie n'appartiendrait plus à ceux qui ont le plus de ressources, mais à ceux qui ont le plus de connaissances techniques et qui réussissent à rendre leurs actes inaperçus.

[ens.mil.ru] Les points de vue conceptuels sur les activités des Forces armées de la Fédération de Russie dans le cyberespace

Le Ministère de la Défense russe a publié, fin 2011, un document intitulé : *« Les points de vue conceptuels sur les activités des Forces armées de la Fédération de Russie dans le cyberespace ».* Selon ce document, le pays met principalement l'accent sur une politique défensive en matière de cyber-conflits et sur l'adoption d'un traité international sous l'égide de l'ONU pour définir une stratégie commune dans le cyberespace. La Russie y souligne également qu'il est fondamental de de respecter la souveraineté des pays. Il s'agit sans doute là d'une référence aux révolutions arabes souvent perçues côté russe comme ayant été téléguidées via internet par les pays occidentaux.

Le marché de la cybersurveillance bousculé : quelles évolutions à venir ?

Le 6 décembre 2011, Wikileaks rendait publique une liste de plus de 1000 documents (plaquettes commerciales, modes d'emplois…) portant sur des technologies d'interception de télécommunication et de surveillance[1]. Tous témoignent de l'existence d'un marché de la cybersurveillance de masse, jusque-là resté à l'écart du grand public. Ce marché représenterait près de 5 milliards de dollars.

Le débat de société : le difficile équilibre entre éthique et réalités du marché

La diffusion de documents dévoilant les dessous de ce marché est intervenue au cœur d'un contexte géopolitique délicat, où Printemps arabes et lutte contre la censure et la cybersurveillance font presque quotidiennement l'actualité. Et le constat est sans appel : les principaux acteurs de ce marché que sont Bluecoat, Nokia-Siemens, Qosmos, Nice ou encore Verint (dont certains ont équipé des dictatures en outils de cybersurveillance) sont issus de pays occidentaux, démocratiques. Et c'est ce double jeu qui a pu leur être reproché[2].

Une censure omniprésente, jusque-là l'apanage de sociétés non démocratiques. D'un côté, il y a eu cet engouement autour des révolutions arabes, ce soutien massif des pays démocratiques aux révolutionnaires, face à des gouvernements qui pratiquaient déjà, au quotidien, une véritable cybersurveillance de leurs citoyens (AMMAR 404 en Tunisie, par exemple). Ces mêmes gouvernements, pour couper court aux mouvements sociaux, n'ont pas hésité à lancer des opérations de désinformation, à pirater les comptes Gmail, Yahoo! et Facebook des dissidents, à les pister, à espionner leurs conversations, ou à bloquer tout accès à Internet dans leurs pays.

Un marché d'armes de surveillance détaché de toute considération éthique. De l'autre côté, il y a la réalité du marché. Les outils de cybersurveillance se vendent comme n'importe quels autres produits, avec un service après-vente et un accompagnement, à des clients ayant pour certains des motivations que l'on peut considérer comme non légitimes. Mais cela importe peu sur ce marché. Comme a pu le souligner Jerry Lucas, organisateur de l'ISS[3], salon rassemblant plusieurs fois par an les professionnels des technologies d'interception de communications : *« Ce n'est pas [son] job de faire le tri entre les bons et les mauvais pays. […] C'est un marché ouvert. »* Mais surtout, c'est un marché légal.

[1] OWNI a mis à disposition sur spyfiles.orgl une cartographie de ces produits.

[2] Voir cette pétition, « Stop the sale », visant à interdire l'exportation de matériel de cybersurveillance, https://www.accessnow.org/page/s/stop-the-sale

[3] http://www.issworldtraining.com/ISS_WASH/

L'encadrement juridique de la vente de matériel de cybersurveillance : vers une évolution substantielle ?

En France, par exemple, **l'exportation de matériel de cybersurveillance n'est actuellement pas soumise à l'autorisation prévue par le code pénal.** L'article 226-3 du code pénal punit bien[4] *« la fabrication, l'importation, la détention, l'exposition, l'offre, la location ou la vente, en l'absence d'autorisation ministérielle […] d'appareils »* permettant l'interception, le détournement, l'utilisation ou la divulgation de correspondances émises, transmises ou reçues par la voie des télécommunications, sans accord préalable de la commission consultative *« relative à la commercialisation et à l'acquisition ou détention des matériels permettant de porter atteinte à l'intimité de la vie privée ou au secret des correspondances »*. Mais l'article ne vise en aucun cas l'exportation. Ainsi, si la nature même du matériel de cybersurveillance vendu par de nombreuses entreprises à des Etats non démocratiques entre bien dans le cadre des articles 226-3 et 226-15 précités, les opérations d'exportation de ce matériel de cybersurveillance restent en dehors de la compétence de la commission consultative.

L'exportation de matériel de cybersurveillance échappe également au contrôle de l'exportation des matériels de guerre. C'est l'arrêté du 17 juin 2009 qui fixe la liste des matériels de guerre et matériels assimilés soumis à une procédure spéciale d'exportation. On y retrouve du matériel de chiffrement, par exemple. Mais il n'est nullement fait mention, de près ou de loin, du matériel de cybersurveillance. Le Secrétariat général de la défense et de la sécurité nationale (SGDSN), chargé du contrôle des exportations des matériels de guerre, a ainsi eu l'occasion de préciser au webzine OWNI, que le système Eagle n'avait pas eu besoin d'obtenir l'agrément préalable de la Commission interministérielle pour l'étude des exportations de matériels de guerre (CIEEMG) chargée, pour le compte du Premier ministre, d'émettre un avis sur l'autorisation, ou non, de ce genre de d'exportations[5].

L'exportation de matériel de cybersurveillance échappe également au contrôle de l'exportation des biens et technologies à double usage. Le règlement européen n° 1334/2000 du Conseil en date du 22 juin 2000 soumet les biens et technologies à usage dual à un contrôle spécifique de leurs exportations. Initialement, sont considérés comme biens à double usage tous les produits, logiciels et technologies susceptibles d'avoir une utilisation tant civile que militaire. Mais le matériel de cybersurveillance ne figure pas dans l'annexe I du règlement (CE) n° 428/200 établissant une liste des biens et technologies à usage dual en question.

Vers une évolution des textes applicables à l'échelle nationale. Récemment, le SGDSN a élaboré un projet de texte précisant les outils informatiques soumis à l'autorisation du premier ministre dans le cadre de l'article 226-3 du code pénal[6].

Le renforcement, à l'échelle européenne, du contrôle de l'exportation des technologies de cybersurveillance, technologies à double usage. En septembre 2011, le Parlement européen avait déjà indiqué qu'il entendait renforcer le contrôle des exportations de matériel permettant la surveillance d'appels téléphoniques, de SMS et de trafic Internet de grande échelle.

- Ces produits devraient désormais être explicitement inclus dans la liste de technologies à double usage.

[4] « d'un an d'emprisonnement et de 45000 euros d'amende »

[5] http://owni.fr/2011/09/28/amesys-libye-kadhafi-droit/

[6] http://www.pcinpact.com/news/68829-sgdn-autorisation-vie-privee-informatique.htm

- A été prononcée l'interdiction des exportations à double usage vers les pays soumis à un embargo sur les armes imposé par le Conseil de l'Union européenne, l'Organisation pour la sécurité et la coopération en Europe (OSCE) ou par les Nations unies.

- De plus, pour la plupart des biens à double usage, les exportations vers les États-Unis, le Canada, l'Australie, la Nouvelle Zélande, le Japon, la Norvège, la Suisse et le Liechtenstein, il faudra une autorisation générale d'exportation émise par l'Union européenne[7].

L'effectivité de cette disposition ne pourra se mesurer qu'en fonction du type de norme adoptée par l'Europe. Si cette interdiction reste à l'état de simple encouragement, il y a fort à parier que le statut juridique des outils de surveillance reste en l'état, sa mise en œuvre étant laissée à la discrétion des États membres.

Les choses se compliquent selon que l'on est en présence d'une directive ou d'un règlement. Le règlement européen est directement applicable au sein du droit national, sans besoin d'une transposition dans l'ordre juridique interne des Etats. Il s'applique de manière simultanée à l'ensemble des Etats membres de l'Union. A l'inverse, la directive laisse une marge de manœuvre confortable aux Etats, qui en transposent l'essentiel dans le but d'atteindre les objectifs qu'elle pose dans un certain délai. Ainsi, si l'interdiction d'exporter du matériel de cybersurveillance vers certains pays est actée dans une directive, l'émergence de distorsions de concurrence entre les différents pays est à prévoir. Si la mesure est actée dans un règlement, tous les Etats membres de l'Union seront logés à la même enseigne. S'il n'est pas possible de parler de distorsion de concurrence entre Etats européens, qu'en est-il avec les Etats hors de l'Union ?

Une telle décision constituerait un réel frein au marché de la cybersurveillance tel que dévoilé par Wikileaks. Ces produits qui, jusque-là, n'étaient soumis à aucun contrôle, pourraient voir leur commercialisation soumise à des délais importants, et limitée à des pays démocratiques désirant les exploiter à des fins légitimes, respectant les *« droits en ligne »*.

Le développement d'offres émanant du Sud : vers un marché Sud/Sud de la cybersurveillance ?

Si la majeure partie des vendeurs d'outils de cybersurveillance sont issues de pays d'Europe de l'Ouest et des Etats-Unis, les offres issues de pays du Sud et pays émergents sont en plein essor :

- Suntech Intelligence : cette société brésilienne, récompensée en 2011 par l'AT Kearney Best Innovator Award[8], se positionne sur le marché des interceptions légales, du DPI et de la gestion de trafic de masse pour les FAI et les gouvernements[9].
- Asoto, société colombienne.
- ZTE Corp, société chinoise. L'entreprise est présente en Europe de l'Ouest, de l'Est et en Amérique du Nord.
- Huawei Technologies, société chinoise.
- Vixtel[10], société chinoise positionnéesur le marché de l'interception légale (LI ou *lawful Inteception*). La société est partenaire de China Mobile, China Telecom, China Unicom ou encore PCCW.

[7] http://www.europarl.europa.eu/news/fr/pressroom/content/20110927IPR27586/html/Contr%C3%B4ler-les-exportations-%C3%A0-double-usage

[8] http://www.bestinnovator.de/

[9] http://www.suntechintelligence.com/en/about-us/

- Shogi Communications[11], société indienne spécialisée dans l'écoute du protocole GSM.
- ClearTrail[12], société indienne ayant comme produit phare un outil d'interception de masse de voix sur IP.
- Shield Security[13], société indienne.
- Etc.

Parmi ces offres, l'Inde et la Chine se distinguent[14]. Shogi Communications, société indienne est présente en Europe, mais aussi en Asie, Afrique du Sud, et Amérique du Sud. D'autres sociétés, non mentionnées par Wikileaks, s'illustrent aussi sur ce marché. Paladion Networks, autre société indienne dont la spécialité est la surveillance du web social, est par exemple déjà implantée dans une trentaine de pays en Asie, aux Etats-Unis et en Europe.

La Chine n'est pas en reste avec, par exemple, Semptian, société fondée par des ex-responsables du géant Huawei, qui a commencé par développer des solutions d'administration réseaux et pare-feu pour l'Etat chinois, et s'est finalement tournée vers des technologies de censure et d'identification d'internautes[15].

Ces acteurs ont l'immense avantage de ne pas devoir se plier aux encadrements stricts que connaissent (ou connaitront) leurs concurrents européens par exemple, et peuvent exporter leurs technologies sans entrave – et à un moindre coût pour l'acheteur. Ceci, couplé aux ambitions de la Commission européenne, laisse un véritable boulevard à ces sociétés sur le marché de la cybersurveillance.

DE L'EXPORTATION A L'IMPORTATION

L'importation de matériels de cybersurveillance en Europe ne sera cependant pas si simple. Si la Commission européenne souhaite restreindre l'exportation, elle voudra peut-être restreindre l'importation de ces produits. C'est ce que prévoit déjà le système français. En effet, l'article 226-3 du code pénal mentionné précédemment, s'il ne vise pas l'« exportation », soumet bien l'importation de ce type de technologies à autorisation de la commission consultative *ad hoc*. Ainsi, les géants asiatiques de la cybersurveillance seront probablement limités dans la vente de leurs produits à des Etats européens, si ces derniers adoptent un système similaire à la France. Les processus d'autorisation, relativement longs, seront peut-être dissuasifs. Ce qui renforce l'hypothèse du développement d'un marché « Sud/Sud ».

[10] http://www.vixtel.com/Web-en_US/NGNVoIP%20Lawful.html

[11] http://wikileaks.org/spyfiles/files/0/160_SHOGI-2006-semiactive_gsm_monitoring.pdf

[12] http://wikileaks.org/spyfiles/files/0/111_CLEARTRAIL.pdf

[13] http://www.shieldsecurity.org/

[14] http://www.intelligenceonline.fr/intelligence-economique/terabytes/2011/12/08/les-(futurs)-geants-asiatiques-de-l-interception-de-masse,95168669-ART

[15] http://www.securityvibes.fr/cyber-pouvoirs/milipol-2009-lannee-des-grandes-oreilles/

La formation et la fourniture d'outils de contournement de la censure, un nouveau marché pour les entreprises françaises, européennes ?

« No Disconnect » [16] **:** Dans sa stratégie « No Disconnect », Neelie Kroes appelle au développement d'*« outils technologiques destinés à améliorer la protection de la vie privée et la sécurité des populations qui utilisent des TIC dans des régimes non démocratiques »*[17]. Plus précisément, la Commission européenne souhaite fournir aux dissidents des « *logiciels qui peuvent être installés sur un ordinateur de bureau, un ordinateur portable, un* smartphone *ou tout autre appareil ».* Sont ici visés : VPN, proxys ou autres technologies permettant de garder l'anonymat sur Internet.

Un alignement sur la stratégie américaine. Avec ce document, l'Europe s'aligne sur la stratégie américaine visant à promouvoir les outils de lutte contre la censure dans les pays dictatoriaux. L'administration Obama soutient déjà activement ces technologies via des projets de téléphonie mobile et d'Internet fantôme. A l'aide de leur concept de *« diplomatie numérique »*, les Etats-Unis ont pu appuyer les révolutions, notamment en envoyant des équipes former et soutenir les cyberactivistes égyptiens, grâce à des programmes financés par le Département d'Etat ou des fondations privées (*Freedom House ou la FED*). Ces programmes, qualifiés par Alec Ross (conseiller spécial à l'innovation d'Hillary Clinton) de « *confidentiels* », auraient coûté près de 150 millions de dollars. Comme l'a exprimé Hillary Clinton dans son discours du 15 février 2011, *« la défense de la liberté d'Internet est* [déjà] *un dossier prioritaire de [la politique étrangère américaine] »,* et près de 25 millions de dollars ont été promis pour la création d'outils au profit de la liberté d'expression des cyberactivistes dans le monde[18].

Les *« kits de survie sur Internet »* évoqués par Neelie Kroes ne sont donc pas sans rappeler les fameuses valises *« Internet fantôme »* imaginées par les Etats-Unis. Un budget de 2 millions de dollars US avait été affecté au développement de ce produit essentiellement destiné aux dissidents de pays où les réseaux mobiles et Internet seraient coupés. Il s'agit là peut-être de l'émergence de nouvelles cibles pour les entreprises fabriquant VPN et autres technologies d'anonymisation et de contournement de la censure.

Vers un marché de « la défense des droits de l'homme sur Internet » ? Le développement de prestations de collecte de renseignement afin de contrôler les *« niveaux de censure »*, le déploiement de produits de contournement de cette censure, de prestations d'hébergement et d'acheminement des données censurées ou encore la formation de dissidents pourraient constituer un point de départ pour un nouveau marché de *« la défense des droits de l'homme sur Internet »*.

---

[16] « Stratégie numérique: Mme Kroes invite M. Karl-Theodor zu Guttenberg à promouvoir la liberté d'expression sur l'internet au niveau mondial », http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1525&format=HTML&aged=0&language=FR&guiLanguage=en

[17] « Stratégie numérique: Mme Kroes invite M. Karl-Theodor zu Guttenberg à promouvoir la liberté d'expression sur l'internet au niveau mondial », http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1525&format=HTML&aged=0&language=FR&guiLanguage=en

[18] Voir Source : Valeurs Actuelles, n°3883, Avril/Mai, « L'Amérique manipule Twitter », p. 3

RSA Conference	Etats-Unis	Du 27 février au 2 mars 2012
Black Hat 2012	Amsterdam (Pays-Bas)	Du 14 au 16 mars 2012
Congrès Big Data Paris 2012	Paris (France)	20 et 21 mars 2012
2nd annual Cyber Security	Pékin (Chine)	Du 22 au 23 mars 2012
IST International Forensic Technologies Fair	Varsovie (Pologne)	Le 28 mars 2012
HackCon	Oslo (Norvège)	Du 26 au 29 mars 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 notre extranet
https://owldesk.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