# Observatoire du Monde Cybernétique

Lettre n°9 – Septembre 2012

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

**[Défense.gouv.fr] Des réservistes spécialisés en cyberdéfense**

L'officier général Cyber français a annoncé lors des Universités d'été de la Défense qu'un groupe de réservistes spécialisés en cyberdéfense dans le cadre de la réserve citoyenne allait être mis en place. Coordonnée par l'OG Cyber et Luc-François Salvador, qui recevra pour cela une lettre de mission personnelle, cette réserve cyber aura pour objectifs de relier monde civil et monde militaire, *« d'expliquer la dimension stratégique de ce domaine en pleine expansion, d'y préciser la place des armées et de donner des clés de compréhension des différents enjeux ».*

**[Zataz] Bull.fr infiltré par un hacker algérien**

Un hacker algérien « white hat » aurait détecté plusieurs failles de sécurité sur le site de la société Bull, permettant notamment l'affichage de certaines informations appartenant à des employés de de la société, à des entreprises partenaires, des sites gouvernementaux, etc. L'ANSSI a été contactée afin de permettre la correction des failles.

**[La lettre A] Huawei s'établira en Grande-Bretagne**

L'opérateur de télécoms chinois Huawei Technologies a annoncé l'investissement de 2 milliards de dollars et l'extension de ses activités en Grande-Bretagne. La France ne sera pas en reste puisque le groupe envisage de recruter des experts en sécurité. Objectif : s'assurer de l'obtention des autorisations françaises nécessaires à la commercialisation de certains produits. Cette annonce intervient quelques mois après la publication du rapport sur la cyberdéfense française du sénateur Jean-Marie Bockel. Le document remettait en cause la fiabilité de certains équipements de cœur de réseau, notamment ceux « d'origine chinoise »

**[Zataz] Journée internationale contre Indect**

Suite aux protestations contre le projet européen de surveillance intelligente INDECT, les Anonymous ont appelé *« les citoyens »* à une nouvelle journée de mobilisation le 20 octobre prochain. Les militants demandent à l'Union Européenne un arrêt total du projet accusé de permettre un contrôle systématique des populations - et la prohibition de la vente de ces technologies à d'autres pays.

**[ZDNet] Gouvernance Internet : Neelie Kroes s'oppose à la montée en puissance de l'UIT**

Dans une récente interview, Neelie Kroes, commissaire européenne chargée de la société numérique, s'est montrée réticente quant au transfert de certaines compétences en matière de gouvernance d'Internet à l'UIT. Selon elle, cette proposition soutenue par des pays comme la Chine et la Russie, n'est pas opportune. La commissaire a également indiqué qu'elle était défavorable à la création d'une nouvelle structure *ad hoc*.

**[EUROPA] Vers le renforcement de la cybersécurité des institutions de l'UE avec le CERT-UE**

Conformément aux engagements tenus dans la stratégie numérique pour l'Europe adoptée en mai 2010, la Commission européenne a mis en place le CERT-UE. *« Les institutions de l'UE peuvent désormais compter sur un CERT permanent pour contrer des menaces informatiques de plus en plus sophistiquées »,* a pu souligner Neelie Kroes.

**[Nextgov] La légitime défense envisageable face à certaines cyberattaques**

Selon le juriste du Département d'Etat américain Harold Koh, certaines cyberattaques pourraient justifier l'emploi de la légitime défense par le déclenchement des articles 2(4) et 15 de la Charte de l'ONU. Il a cependant précisé que, pour ce faire, ces cyberattaques devraient blesser ou infliger des dommages matériels similaires à ceux engendrés par une arme cinétique traditionnelle (comme une bombe ou un missile).

**[The Washington Post] Enquête sur le business controversé des 0-day**

Alors que la demande pour les failles 0-day est de plus en plus importante, certaines voix s'élèvent

pour réclamer un meilleur encadrement de ce marché très secret, en s'inspirant par exemple de la législation allemande, même si l'effectivité de telles mesures resterait limitée. Les éditeurs de logiciels s'organisent en effet en offrant des récompenses aux chercheurs qui découvrent des failles importantes. Certaines sociétés, comme Vupen, cherchent cependant à rassurer les plus sceptiques et affirment sélectionner leurs clients et n'offrir leurs services qu'à des agences gouvernementales de pays membres de l'OTAN, ou leurs alliés.

**[gov.aol.com] Le sénateur Joseph Lieberman attribue les cyberattaques contre Bank of America à Téhéran**

Selon le sénateur américain Joseph Lieberman, directeur du comité sénatorial sur la sécurité nationale, les attaques ayant visé Bank of America auraient été commanditées par l'Iran. Certains experts estiment qu'il s'agirait là de représailles au virus Stuxnet, lancé contre l'Iran par les Etats-Unis.

**[Foreign Policy] Les Etats-Unis améliorent leur capacité d'identification des auteurs de cyberattaques**

Eric Rosenbach, assistant du secrétaire à la Défense en matière de politique de cybersécurité, a déclaré que les experts du ministère de la Défense avait fait des progrès significatifs en matière d'attribution des cyberattaques. Alors que l'origine des attaques n'était identifiée que dans un tiers des cas il y a 5 ans, ce chiffre a augmenté de façon satisfaisante selon Jim Lewis, directeur de programme au Centre d'études stratégiques internationales.

**[Data Security Breach] Anonymous diffuse les plans d'une base militaire américaine**

Un pirate se revendiquant des Anonymous a diffusé 18Mo de données sensibles concernant la base navale d'Elinkine, au Sénégal : plans, détails des constructions, rapports géotechniques, etc.

Ces documents proviennent de groupes comme le CNTPO (département de la défense contre les narcotrafiquants et le terrorisme), Northrop Grumman ou l'AFRICOM, et pourraient avoir été volés sur un serveur de la société de conseil Simpkins & Costelli.

**[Intelligence Online] La cyberguerre entre dans l'ère industrielle**

Les représentants des plus grandes entreprises américaines d'informatique militaire ont assisté le 20 septembre dernier à une présentation classifiée « secret » de Daniel Roelker, le nouveau responsable « cyberguerre industrielle » de la DARPA. A notamment été présenté le projet « Plan X », qui vise à doter la cyberdéfense américaine de chaînes de programmes automatisées, capables de générer une contre-attaque en cas d'intrusion, voire de mener des offensives coordonnées et prolongées sans pilotage humain. Un premier appel d'offres pour ce projet sur 5 ans et doté de 100 millions de dollars devrait être lancé à l'automne.

**[ZDNet] Le Japon va créer une unité de cyberdéfense**

Le Japon recrutera d'ici à 2013 une centaine de personnes spécialisées dans la sécurité informatique afin de monter une unité de cyberdéfense. Objectifs : permettre aux Forces d'Auto-Défense de mieux réagir en cas d'attaque informatique ; collecter et analyser des informations sur les cybermenaces existantes.

**[Korea JoongAng Daily] La Corée du Sud améliore sa cyberdéfense**

Séoul a annoncé le renforcement de ses capacités en termes de cyberdéfense, notamment afin de se défendre face à la menace croissante que la Corée du Nord fait peser sur ses systèmes d'informations. La Corée du Sud envisage ainsi de doubler les effectifs de son Cyber Command pour atteindre un total de 1000 professionnels. Cet effort s'inscrit dans une stratégie de défense globale contre Pyongyang.

**[Freedom Online Kenya] Le Kenya accueille la première conférence africaine sur la liberté sur Internet**

Plus de 300 représentants venus du monde entier étaient présents à Nairobi les 6 et 7 septembre pour le second sommet mondial sur la liberté sur

Internet. Celui-ci s'est tenu pour la première fois sur le continent africain, symbolisant ainsi le rôle croissant des TIC en Afrique.

**[New Europe] Une société de télécom sud-africaine aurait fourni du matériel de cybersurveillance américain à l'Iran**

Le groupe sud-africain MTN est accusé d'avoir fourni du matériel américain à l'Iran via la joint-venture Irancell dont il possède 49%, contournant ainsi l'embargo imposé au pays par les États-Unis. Selon les informations disponibles, il s'agissait de matériel fabriqué par Sun Microsystems, Oracle, Cisco, Hewlett Packard, IBM et EMC et destiné entre autre à effectuer des écoutes.

**[The Next Web] Rapprochement entre l'Iran et la Corée du Nord**

L'Iran et la Corée du Nord ont signé le 1er septembre dernier un accord de coopération scientifique et technologique.

Mikko Hypponen, expert en sécurité informatique chez F-Secure, a commenté cette annonce en expliquant que les deux pays allaient sans doute chercher à renforcer leurs capacités en matière de cybersécurité, notamment en matière de lutte contre les attaques ciblées de type Stuxnet ou Flame.

**[Maxisciences] L'Iran franchit la première étape vers son intranet national**

Annoncé depuis quelques temps, le projet iranien d'internet « hallal » semble prendre forme. Un officiel a en effet annoncé le 24 septembre le filtrage de Google et de sa messagerie Gmail. Le vice-ministre des communications et des technologies, Ali Hakim-Javadi, a déclaré que tous les organismes gouvernementaux avaient d'ores et déjà été raccordés à un réseau national d'information. La finalisation du projet est annoncée pour mars 2013.

**[hurriyetdailynews.com] La Turquie envisage de former des « cyber combattants »**

Le gouvernement turc a annoncé son intention de mettre en place une unité dédiée à la guerre cybernétique. L'objectif est de lutter en particulier contre les groupes de hackers tels qu'Anonymous ou Redhack qui ciblent depuis plusieurs semaines les sites institutionnels turcs. Cette décision fait suite à la publication d'un document officiel détaillant les orientations stratégiques turques en matière de défense. Ce dernier inclut également des préconisations sur la protection des infrastructures vitales de l'Etat et invite les autorités turques à organiser des exercices de simulation afin de développer de réelles capacités cybernétiques.

**[Secure List] Retour sur le virus Wiper**

Les chercheurs de Kaspersky ont livré les résultats de leur enquête sur le virus Wiper. Selon eux, le maliciel serait lié à Duqu et Stuxnet. Si le lien avec le malware Shamoon semble évident, le doute subsiste quant au lien entre Wiper et Flame.

**[Symantec] Publication du « Norton Cybercrime Report 2012 »**

Dans l'édition 2012 de son rapport, Symantec évalue à 110 milliards de dollars le coût de la cybercriminalité dans le monde, estimant que 556 millions de personnes en ont été victimes tout au long de l'année. Les auteurs mettent également l'accent sur les mutations des modes opératoires cybercriminels auxquels les consommateurs sont particulièrement vulnérables, ces derniers étant souvent réticents à faire évoluer leurs usages.

**[CCD COE] Publication du « Manuel de Tallinn » sur le droit international applicable à la cyberguerre**

Le centre de l'OTAN consacré à la cyberdéfense a publié un recueil concernant le droit international applicable à la cyberguerre, qu'il s'agisse du *jus ad bellum* ou du *jus in bell*o. Ce document de 215 pages, qui réunit les contributions d'experts australiens, britanniques, américains, canadiens et néerlandais, n'exprime pas la position officielle de l'OTAN mais uniquement l'opinion de ses rédacteurs.

**[IRIS] Observatoire géostratégique de l'information : stratégies dans le cyberespace (2)**

L'IRIS publie, sous la direction de François-Bernard Huyghe, le deuxième volet de son étude sur la stratégie dans le cyberespace. Outre la contribution du sénateur Bockel, auteur du rapport sur la cyberdéfense paru en juillet 2012, cette publication compte les contributions de Chris Demchak, professeur à l'US Naval War College, sur la capacité d'adaptation des États-Unis dans le cyberespace, de Rebecca Lopez, chercheuse à l'IRIS, sur la stratégie russe, et de Bertrand Boyer, officier spécialisé dans la SSI, à propos de la géopolitique du cyberespace.

**[Huawei] Huawei publie son Cyber Security White Paper**

Faisant le constat de l'internationalisation de la production, conception et développement des technologies supportant Internet, Huawei rappelle que la cybersécurité est l'affaire des gouvernements et des industriels du monde entier. Dans ce rapport signé par John Suffolk, ancien Chief Information Officer du gouvernement britannique, le fournisseur en réseaux et télécommunications chinois plaide pour une collaboration internationale transparente, *« vérifiable »* et basée sur la confiance. Surtout, Huawei s'engage à : adopter tout standard international ou toute bonne pratique, dès lors que ceux-ci font l'objet d'un consensus international ; encourager la recherche en matière de cyberdéfense ; opérer de manière transparente avec les gouvernements.

**[IBM] IBM publie son rapport sur les tendances et les risques en matière de cybersécurité**

Les médias sociaux seraient les cibles les plus vulnérables aux cyberattaques, selon le dernier rapport d'IBM intitulé « X-Force 2012 Mid-Year Trend and Risk Report ». Le document souligne également une forte hausse des attaques menées contre les navigateurs Web et les terminaux mobiles, notamment en raison de l'importance croissante du BYOD (Bring Your Own Device). IBM a accompagné la publication de ce rapport de la création d'un SOC (security operation center) à Wroclaw, en Pologne. Objectif annoncé : proposer une approche proactive intégrant l'analyse en temps réel des menaces.

# e-Diplomacy

## *Des programmes illustrant le smart power à l'américaine*

Les pays du monde entier se familiarisent avec les différents moyens de penser la diplomatie en ligne. Récemment, on apprenait qu'un nouveau programme était lancé par l'Université d'Haïfa pour former les étudiants à être *« des ambassadeurs officieux d'Israël sur Internet ».* L'objectif étant d'apprendre aux étudiants à *« faire face à la délégitimation d'Israël sur le web et au sein des réseaux sociaux en particulier ».*[1]

Mais ce sont les Etats-Unis qui sont les précurseurs de la diplomatie numérique : l'art d'utiliser les nouvelles technologies comme des outils diplomatiques permettant de soutenir et de défendre les intérêts nationaux. L'ensemble de leurs technologies et programmes de formations, que certains comparent à une version moderne de la radio « Voice of America », s'inscrivent dans le cadre d'un large projet, lancé par les États-Unis il y a quatre ans, pour soutenir les dissidents chinois et les aider à contourner la censure de leur gouvernement. Suite aux manifestations iraniennes de 2009 et aux évènements du Printemps arabe de 2011, le Congrès américain a ensuite décidé d'allouer au projet 57 millions de dollars supplémentaires pour les trois années à venir et de soutenir ainsi les opposants aux régimes autoritaires du monde arabe.

Mélange de soft power et de smart power, la diplomatie numérique américaine se situe dans le droit fil de la doctrine de smart power que la secrétaire d'Etat Hillary Clinton a appelée de ses vœux depuis son entrée en fonction. Cette stratégie se matérialise par ***deux grandes catégories de programmes au sein d'e-Diplomacy : les programmes opérationnels d'une part, et les programmes centrés sur « l'humain » d'autre part.*** Les premiers, qui consistent à apporter une réponse dans le cadre de situations de crise, se rapprochent d'une logique de hard power, d'une logique d'affrontement. Il ne s'agit cependant pas de fournir des armes, mais de mettre à la disposition des dissidents des outils leur permettant de mener leur lutte à bien et de déstabiliser les régimes hostiles aux Etats-Unis. Les seconds se rapprochent plus du soft power, de la séduction et de l'influence sur le long terme et cherchent à faire de l'étranger un futur partenaire, indépendamment de toute situation de crise.

## I – Les programmes opérationnels

La finalité des programmes opérationnels d'e-diplomacy est de donner aux insurgés la possibilité de communiquer sur leur lutte. Cela passe par plusieurs étapes :

1. ***Assurer une capacité de connexion en toutes circonstances, ce qui implique la possibilité de se connecter même lorsque les infrastructures télécoms sont désactivées ou endommagées.***

Le contrôle des infrastructures est en effet un avantage déterminant dans les mains des régimes autoritaires pour museler les dissidents. L'Etat peut ainsi diminuer fortement le débit ou couper la connexion dans une zone, voir isoler complètement le pays. Cela est possible par l'organisation fortement centralisée que l'on retrouve dans certains pays : nombre restreint d'opérateurs ou de fournisseurs d'accès, fort contrôle

[1] http://jssnews.com/2012/02/29/luniversite-de-haifa-cree-un-diplome-de-diplomatie-numerique/

gouvernemental sur ceux-ci, taux de pénétration souvent modestes[2] et faible quantité de connexions au réseau international.

Pour contourner le contrôle des infrastructures par les Etats, il existe déjà plusieurs solutions. L'armée américaine dispose ainsi d'équipements de guerre électronique qui permettraient non seulement de diffuser des émissions radio et TV dans certains zones mais aussi d'offrir une connectivité internet[3]. Ces techniques demandent cependant de grosses infrastructures, ainsi que l'engagement physique de ressources militaires. L'objectif est alors être de réduire la taille du matériel engagé : la *New America Foundation* a obtenu une subvention du département d'Etat américain pour développer le projet « Internet in a suitcase »[4], qui permettrait de se connecter à Internet à partir d'une sorte de mallette, malgré une coupure générale de réseau[5]. Dans ce cas, il serait plus difficile de prouver une implication étatique directe, comme dans le cas de l'usage d'un navire ou d'un avion. De nombreux projets à l'étude misent sur un réseau décentralisé permettant d'échapper à un contrôle étatique, ou même à un quelconque contrôle. A l'image du système Serval[6], ou de Commotion[7] - deux projets qui ont reçu des fonds du gouvernement américain -, l'idée est que chaque terminal puisse communiquer avec les autres, formant un réseau maillé impossible à contrôler.

2. ***Fournir un équipement, même rudimentaire, permettant de témoigner et de documenter la lutte (ordinateur portable, caméra, …) et permettre le fonctionnement de ce matériel (alimentation électrique, consommables, etc.).***

Cet aspect est peu abordé tant il est considéré comme évident. Pourtant, apprendre aux insurgés à se servir en toute sécurité des outils numériques sans s'assurer que ces derniers possèdent suffisamment de matériel est inutile. Il faut également se soucier des problèmes d'alimentation en électricité, essentielle pour recharger les appareils.

3. ***Permettre le contournement des moyens de censure étatiques, afin que les informations d'un cyberdissident puissent être librement accessibles sur Internet par un autre dissident, ou par la scène internationale.***

   - **Permettre aux dissidents de communiquer entre eux et avec l'extérieur**

Il faut permettre le contournement des moyens de censure étatiques et former les utilisateurs à l'utilisation des outils numériques en toute sécurité. La base de l'apprentissage consiste à *« déjouer la surveillance policière sur Internet »*[8]. Pour cela, le département d'Etat initie certains blogueurs dissidents aux techniques d'anonymisation des connexions Internet et de chiffrement des données[9]. On apprend aux rebelles à éviter les écoutes téléphoniques ou à utiliser des protocoles de chiffrement sur Internet[10], ce qui est assez classique désormais. On met également à leur disposition des applications innovantes permettant par exemple d'effacer le contenu de leur téléphone en cas d'arrestation, de faire apparaître un faux écran de téléphone

[2] Avec une exception notable pour la Tunisie, mais la Tunisie ne fait pas partie des pays ayant coupé l'accès à Internet à l'échelle du pays.
[3] http://www.wired.com/dangerroom/2011/02/secret-tools-force-net/
[4] http://gcn.com/Articles/2011/06/14/Internet-in-a-suitcase-mobile-network-for-protesters.aspx?Page=1
[5] http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/#ixzz1xmJH3W7V
[6] http://www.lemonde.fr/international/article/2012/04/21/le-logiciel-de-telephonie-mobile-qui-defie-le-controle-des-etats_1688852_3210.html
[7] http://abonnes.lemonde.fr/technologies/article/2011/08/30/commotion-le-projet-d-un-internet-hors-de-tout-controle_1565282_651865.html
[8] http://www.lefigaro.fr/international/2011/02/21/01003-20110221ARTFIG00670-les-cyberactivistes-egyptiens-formes-par-les-americains.php
[9] http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/#ixzz1xmJH3W7V
[10] Notamment le logiciel canadien Psiphon , visant à contourner les mesures de censure de l'Etat syrien. Ce programme a bénéficié de fonds du gouvernement américain.

lors de l'enregistrement d'un mauvais mot de passe, ou encore de flouter le visage des manifestants sur les photos qu'ils prennent pour garantir la sécurité des manifestants[11].

Outre le matériel informatique, les téléphones prennent une place de plus en plus importante dans les conflits actuels. Les plus modernes peuvent filmer, photographier, partager leur contenu, communiquer sur les réseaux sociaux, naviguer sur Internet, etc. Plusieurs projets visent à permettre à ces appareils de fonctionner même en cas de coupure du réseau ou de contourner les éventuelles censures : c'est le cas de Serval[12], déjà mentionné plus haut, qui mise sur un réseau décentralisé fonctionnant sur le principe du maillage[13]. Les téléphones, affranchis des verrouillages imposés par les opérateurs, communiquent directement les uns avec les autres.

- **Permettre aux soutiens occidentaux de communiquer avec les dissidents**

Quand on évoque la stratégie américaine de défense de la liberté d'Internet, on pense spontanément aux multiples vidéos filmées par les combattants et retransmises dans les médias occidentaux. Pourtant, il ne faut pas oublier que le réseau permet une communication dans les deux sens, des dissidents vers l'extérieur mais aussi de l'extérieur vers les dissidents. Par exemple, plusieurs commentateurs ont émis l'hypothèse que certaines vidéos prétendument filmées par des rebelles syriens aient en réalité été tournées aux Etats-Unis ou au Canada[14]. Ils expliquent en effet que l'impressionnant arsenal que l'on apprend à manier dans ces vidéos (parmi lesquels un pistolet Kel-Tec, un Sig 9mm, un Glock Gen4, ainsi qu'un fusil Smith and Wesson M&P AR-15) ne peut se retrouver simultanément au même endroit que dans très peu de pays. De plus, le montage relativement professionnel tranche avec les vidéos assez rudimentaires habituellement postées. Certains y voient donc une formation virtuelle à la guérilla par des occidentaux à destination des dissidents syriens. Les contenus à destination des pays victimes de troubles peuvent également être plus officiels, comme le message envoyé par Robert Ford[15], ambassadeur américain en Syrie, appelant les soldats fidèles au régime à faire défection.

**Fiche programme : Internet in a suitcase**

**Titre** : « Internet in a suitcase »

**Année de création** : 2011

**Contexte de création** : Internet et les réseaux mobiles occupent une place de plus en plus importante dans le cadre des mouvements populaires à travers le monde. L'administration américaine estime qu'il est dans son intérêt de permettre à des opposants aux régimes autoritaires du monde entier, en particulier ceux hostiles aux Etats-Unis, de s'exprimer et d'utiliser Internet comme un outil dans leurs luttes. Internet in a suitcase a été pensé alors que les coupures et autres limitations étatiques d'Internet se multipliaient : Egypte, Syrie, Bahreïn, Iran, etc.

[11] Ibid
[12] http://www.servalproject.org/
[13] http://www.lemonde.fr/international/article/2012/04/21/le-logiciel-de-telephonie-mobile-qui-defie-le-controle-des-etats_1688852_3210.html
[14] http://www.wired.com/dangerroom/2012/07/syria-youtube-facebook/
[15] http://allfacebook.com/robert-ford-syria_b92696

**Objectif** : Internet in a suitcase est, comme son nom l'indique, un projet qui permettrait de recréer un réseau Internet localement en cas de coupure généralisée ou de censure importante. Le système repose sur le principe de maillage, ou « mesh », qui transforme chaque utilisateur de terminal en partie active du réseau : l'appareil ne se contente pas de recevoir mais émet et transmet aux autres appareils du réseau. Avec quelques ordinateurs portables et des antennes WiFi, un réseau pourrait être recréé sans besoin de grosses infrastructures.

**Soutiens** : Le Département d'Etat américain a financé à hauteur de 2 millions de dollars le projet développé par l'Open Technology Institute, branche du think tank « New America Foundation ». La direction du projet a été confiée à Sascha Meinrath, l'un des directeurs de la fondation, notamment connu pour être à l'origine du projet « Indymedia ».

**Public visé** : les opposants aux régimes autoritaires soutenus par les Etats-Unis.

**Prévisions** : Aucun exemple d'utilisation d'Internet in a suitcase n'a pour le moment été publié. Il n'est donc pas possible de fournir un premier retour sur expérience.

## II – Les programmes d'influence

***« Prendre soin des alliés de demain en les formant aujourd'hui. »***

L'objectif de ces programmes est de familiariser les participants avec le mode de vie et les valeurs occidentales afin de favoriser le dialogue entre les cultures. Ces programmes sont moins médiatisés que les programmes opérationnels car moins « spectaculaires », mais n'en constituent pas moins une pierre essentielle de la diplomatie numérique. Alors que les programmes opérationnels interviennent dans une situation déjà conflictuelle, les programmes d'influence se positionnent plus dans une logique de soft power, incitant les participants à suivre l'exemple américain. Les Etats-Unis cherchent ainsi à prendre soin de leurs alliés de demain en les formant aujourd'hui.

Ces programmes sont assez variés : le site du Département d'Etat en recense un certain nombre[16], la plupart assez peu connus, dont l'ambition est d'engager le dialogue et de favoriser les échanges sous toutes ses formes : e-stage (stage virtuel au Département d'Etat), rencontre dans le monde entier entre des acteurs de la société numérique locale avec des experts américains, etc.

**Fiche programme : Techwomen**

**Titre** : « Techwomen »

**Année de création** : 2011

[16] http://www.state.gov/m/irm/ediplomacy/c23840.htm

**Contexte de création** : Le projet Techwomen a été pensé dans la continuité du discours que le président Barack Obama a tenu au Caire en 2009 et dans lequel il appelait de ses vœux une plus grande coopération entre le Moyen-Orient, l'Afrique du Nord et les Etats-Unis.

**Objectif** : Le programme permettra de structurer une communauté pérenne ; de « *fédérer et nouer des liens forts avec la future élite féminine 2.0 de ces régions [Moyen-Orient et Afrique du Nord], réunie autour des nouvelles technologies »*[17].

**Soutiens** : C'est le département « éducation et affaires culturelles » du Département d'Etat qui est à l'origine de cette initiative. Le projet se déroule en partie dans les locaux de *l'Institute of International Education*, en partenariat avec l'institut Anita Borg pour les femmes et la technologie. En outre, le programme s'appuie sur la participation d'une multitude d'entreprises : *« AT&T, Google, Facebook, CA Technologies, Carnegie Mellon University Silicon Valley, Cisco Systems, eBay, Ericsson, Global Impact, Huawei, HP Labs, Intel, Internet Systems Consortium, Juniper Networks, Microsoft Corporation, mPay Connect, NetApp, Newcomb Anderson McCormick, Oracle, Parallel Earth, SAP Labs, Symantec, Talkfree.com, TechSoup Global, ThoughtWorks, Yahoo!, ZaReason, Catapult Design »*[18].

**Public visé** : Une quarantaine de femmes entre 25 et 42 ans, qui apparaissent comme des leaders en devenir dans le domaine des nouvelles technologies.

**Déroulement du programme** : Le programme dure 5 semaines au total. Pendant 3 semaines en Californie, les participantes rencontrent leurs homologues de la Silicon Valley et sont chacune encadrées par un mentor pour travailler sur des projets professionnels. Les deux dernières semaines se tiennent à Washington et permettent aux participantes de rencontrer des représentants du Département d'Etat ainsi que des représentants d'associations et d'entreprises situées à Washington.

**Prévisions** : Visiblement satisfait des retombées du programme, le Département d'Etat a annoncé le 13 mars 2012 que celui-ci allait s'étendre à l'Afrique sub-saharienne à partir de 2013.

## Conclusion

Précurseurs de la diplomatie numérique, les Etats-Unis cherchent à conserver une longueur d'avance sur les autres Etats en la matière. Mais les nombreuses critiques dont ces opérations font l'objet, mettent en péril la crédibilité de telles actions, tant auprès de l'opinion internationale, que des populations cibles. L'opinion internationale d'abord, qui peut observer la stratégie américaine avec méfiance, à l'image de Moscou qui n'a pas hésité à exprimer ses craintes quant à un éventuel effet de contagion sur son territoire de ce *« concept de promotion de la démocratie »* et du *« changement de pouvoir par une révolution pacifique »*[19]. Les populations cibles ensuite, de plus en plus enclines à plaider pour un cyberactivisme indépendant de toute forme de contrôle, considèrent en effet que l'aide américaine peut, dans certains cas, confisquer la révolution, voire donner l'impression que les dissidents ne peuvent agir seuls.

[17] http://blog.slateafrique.com/africa-tech/2011/07/28/techwomen-la-diplomatie-digitale-us-en-afrique/
[18] http://anitaborg.org/initiatives/techwomen/
[19] http://globe.blogs.nouvelobs.com/archive/2012/06/19/la-syrie-theatre-d-une-nouvelle-guerre-froide.html

# Le portail OMC
# La nouvelle plateforme de la DAS

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

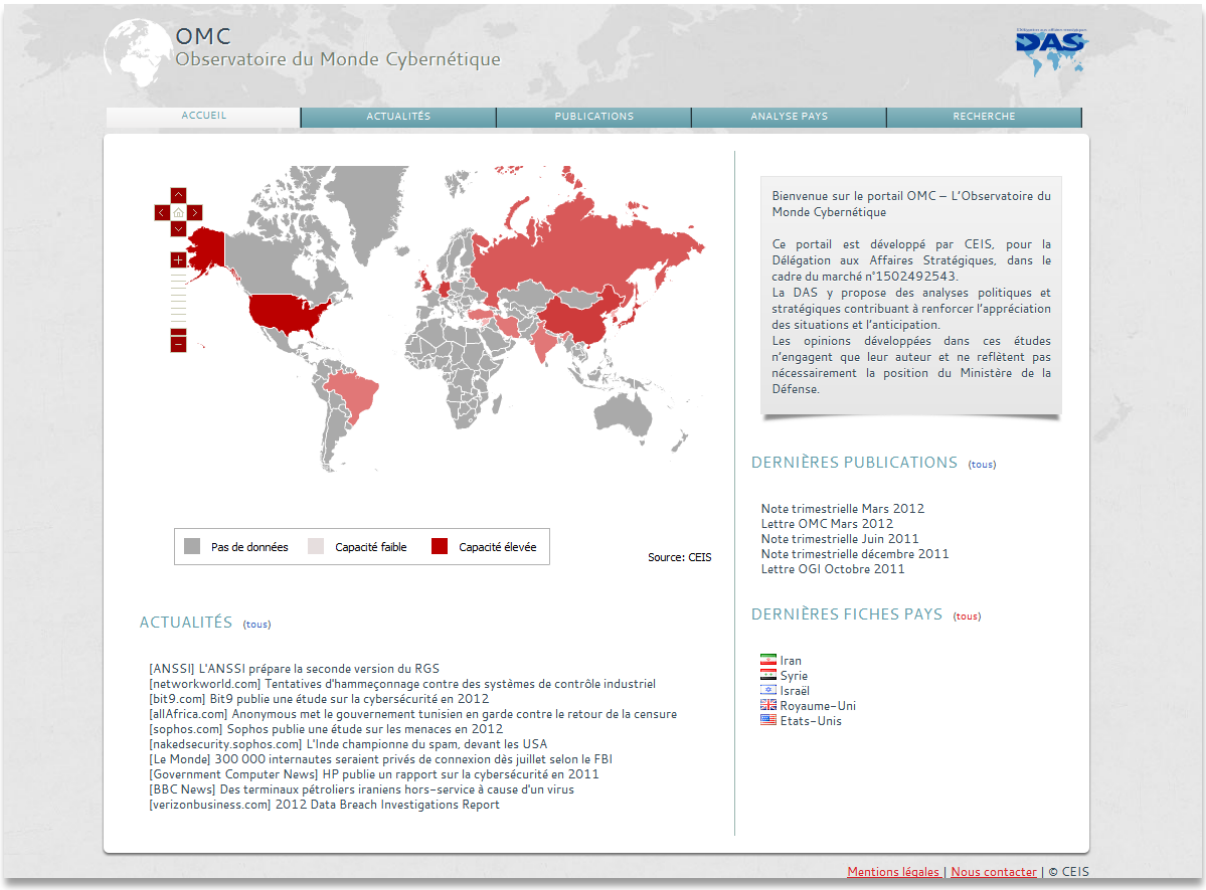


**Figure 1. Page d'accueil du portail OMC - https://omc.ceis.eu/**

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

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

| | | |
|---|---|---|
| **VMworld EMEA** | Barcelone (Espagne) | 9 – 11 octobre |
| **Workshop ENISA Cybersécurité & Smart Grids** | Amsterdam | 15 octobre |
| **Workshop EDA Cyberdéfense** | Bruxelles | 23 octobre |
| **Cyber Warfare & Security Forum** | Brasilia | 30 et 31 octobre |
| **SC12** | Salt Lake City (Etats-Unis) | 10 – 16 Novembre |
| **Forum pour la Gouvernance d'Internet** | Bakou (Azerbaïdjan) | Novembre |
| **Conférence mondiale des télécommunications internationales** | Dubai | 03 – 14 décembre |
| **Colloque CDSE / Europol : "Les entreprises et l'Etat face aux cybermenaces "** | Paris | 6 décembre |
| | | |

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