Observatoire du Monde Cybernétique

Lettre n°8 – Août 2012

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

[globalsecuritymag.fr] L'ISC souhaite renforcer la lutte contre la cybercriminalité au Royaume-Uni

L'Intelligence and Security Committee (ISC) britannique a appelé à un renforcement de la lutte contre la cybercriminalité visant le Royaume-Uni. Selon le directeur européen de FireEye, Paul Davis, les remarques de l'ISC témoignent d'une meilleure prise en compte des cybermenaces, et permettront peut-être la mise en place de stratégies de cybersécurité.

[Foreign Policy] Gouvernance d'Internet : vers une refonte du système actuel ?

Rebecca MacKinnon, membre de la New America Foundation, revient sur les débats qui entourent le prochain sommet de l'UIT qui se tiendra en décembre à Dubaï. La volonté de certains pays, comme la Russie et la Chine, de confier la gouvernance d'Internet à cette organisation onusienne s'est heurtée à la résistance de la plupart des pays occidentaux. Listant les nombreuses qualités du système multipartite ouvert actuel, qui s'est révélé très efficace pour accompagner l'importante croissance d'Internet, elle rappelle que ce système n'est pas non plus exempt de défauts, notamment en ce qui concerne la protection des droits de l'Homme et la diversité des représentants. Elle explique en effet que si le système est ouvert en apparence, en réalité les barrières financières et linguistiques réservent de fait cette gouvernance à une minorité d'acteurs. La participation d'une agence de l'ONU à la gouvernance d'Internet pourrait à ce titre être intéressante.

[The Washington Post] Un officier américain révèle l'existence de cyberattaques en Afghanistan

Lors d'un discours à Baltimore, le lieutenant général Richard Mills a déclaré qu'en tant que commandant des forces internationales dans le sud-ouest de l'Afghanistan entre 2010 et 2011, il avait utilisé des cyberattaques contre les insurgés, sans pour autant préciser la nature de ces attaques. Alors que le livre du journaliste David Sanger a provoqué d'intenses débats lors de sa sortie, cette annonce assez inhabituelle semble indiquer que les forces américaines tendent à lever une partie du voile sur leurs opérations dans le cyberespace.

[wired.com] La DARPA lance son nouveau projet de cyberdéfense : « Plan X »

Aux Etats-Unis, le département du Pentagone pour la recherche, DARPA, a lancé son nouveau programme de cyberdéfense baptisé « Plan X ». Cet effort de 100 millions $ sur les cinq prochaines années n'est pas destiné à développer une nouvelle cyberarme telle que Stuxnet. Il doit plutôt permettre à l'US Cyber Command d'assembler et de lancer des attaques en urgence, d'avoir une cartographie en temps réel de l'évolution du combat et de gérer l'automatisation des missions de cyberattaques depuis les machines du Cyber Command. Pour Daniel Roelker, à l'origine du projet, *« on ne gagne pas des guerres avec plus d'hommes, on les gagne avec plus de technologies ».*

[zdnet.com] Le Sénat américain bloque le Cybersecurity Act

Le Sénat américain a bloqué le « Cybersecurity Act », malgré le soutien du Président Obama au texte. La loi, introduite en février 2012, aurait confié au DHS la mission d'évaluer les risques et vulnérabilités des systèmes informatiques présents dans les infrastructures critiques. Le texte aurait également introduit une grande transparence concernant le traitement des données par les agents fédéraux, et donné aux citoyens américains la possibilité de poursuivre en justice l'Etat en cas d'utilisation inappropriée de ces données.

[stefanomele.it] Israël envisagerait le lancement d'une cyberattaque sans précédent sur l'Iran

Selon les informations auxquelles auraient eu accès le journaliste et blogueur Richard Silverstein, une attaque d'Israël sur l'Iran se traduirait avant tout par une cyberattaque massive contre les infrastructures iraniennes. Cette information intervient alors que les rumeurs d'opérations militaires israéliennes se font de plus en plus fortes.

[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. Objectif : 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 un certain nombre de préconisations concernant 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.

[Renesys] La Syrie s'en remet à la Chine pour se connecter à Internet

La société Renesys a constaté que le trafic Internet syrien transitait quasi exclusivement par PCCW, un opérateur basé en Chine, qui n'est donc pas concerné par les sanctions imposées aux opérateurs occidentaux par leurs gouvernements.

[cnet.com] AntiHacker, outil de surveillance des activistes syriens

D'après le groupe Electronic Frontier Foundation (EEF), les activistes syriens seraient la cible de nombreuses cyberattaques de la part du gouvernement syrien, notamment d'un logiciel nommé AntiHacker, qui réalise une surveillance avancée du poste de l'utilisateur sous prétexte de le protéger d'éventuels virus. Grâce à un outil appelé DarkComet RAT, AntiHacker désactive les antivirus présents sur le poste utilisateur, vole ses mots de passe et supprime des données. Les modes d'infection par AntiHacker sont divers et incluent une diffusion par un groupe Facebook. La version de DarkComet RAT ne serait actuellement détectable par aucun antivirus, selon l'EEF, mais il existe un outil de suppression du malware.

[allvoices.com] Le secteur saoudien de l'énergie victime d'une attaque

L'éditeur de solutions de sécurité Symantec a révélé dans un rapport que le secteur de l'énergie saoudien a été victime d'une attaque informatique, baptisée « Shamoon ». Selon une entreprise de sécurité basée en Israël, le code du maliciel présenterait certaines spécificités, en particulier celle de rendre inaccessible la machine infectée.

[Atlantico] Le projet iranien de « réseau national d'informations » progresse

Au début du mois d'août, le ministre des Télécommunications iranien, Reza Taghipour, annonçait lors d'une conférence de presse que l'Iran développait un intranet national afin de se prémunir contre les cyberattaques venant selon lui d'Israël et des Etats-Unis. De nombreux experts en sécurité y voient surtout le moyen de prévenir une éventuelle révolte du peuple iranien que la Syrie pourrait inspirer. La mise en place d'un intranet permettrait ainsi une surveillance simplifiée des internautes iraniens.

[spbit.ru] Les services de renseignement pourront accéder aux données échangées par Skype

Microsoft a donné son accord officiel pour que des représentants des services de renseignement aient accès aux conversations et échanges de messages des utilisateurs de Skype. Microsoft assure qu'il ne s'agit que d'une mesure habituelle et destinée à améliorer l'efficacité de ses services, tandis que Skype assure qu'il ne s'agit pas de « copier les conversations » mais d'accorder un accès aux forces de l'ordre « en certaines occasions ».

[EurasiaNet.org] Censure du net au Tadjikistan

Les autorités tadjiks ont coupé les télécommunications pendant au moins trois jours dans la région de Gorno-Badakhshan en réaction aux mouvements qui agitent la région autonome. Les accès à plusieurs sites, dont YouTube et Asia-Plus, la plus grande agence de presse indépendante du pays, ont été bloqués.

[The Diplomat] Appels à la violence interethnique et censure d'Internet en Inde

Alors que des menaces en ligne de violences interethniques ont provoqué des scènes de panique en Inde, le gouvernement a demandé à certains géants d'Internet, comme Facebook, Twitter ou Google, de retirer certains contenus.

[Cyberwarzone] Le Brésil se prépare pour la cyberguerre

L'armée brésilienne a récemment annoncé le développement d'un nouveau logiciel pour la sécurité et la prévention des cyberattaques. Cette démarche s'inscrit nettement dans la volonté du gouvernement brésilien de développer la cyberdéfense du pays. Le général Antonio Santos, directeur du centre de communication des forces armées et de la guerre électronique (Ccomgex) estime en ce sens que le Brésil n'est que faiblement préparé à faire face à des cyberattaques. Le Brésil a en outre été la cible de nombreuses cyberattaques contre ses banques au cours de ces dernières semaines.

[Global Voices] Le président du sénat nigérian souhaite « réguler » les réseaux sociaux

David Mark, président du sénat nigérian, a déclaré vouloir réguler les contenus circulant sur les réseaux sociaux, notamment en ce qui concerne le dénigrement des dirigeants. Militant de longue date pour l'adoption d'un traité contre la cybercriminalité en Afrique de l'Ouest, il semble désormais s'intéresser à la question de la régulation des contenus.

[watoday.com] Adoption d'une loi en Australie autorisant la conservation des données de connexion

L'Australie a adopté une loi permettant aux autorités de collecter et de conserver certaines données en ligne des citoyens, comme leur historique, leurs mails ou les contenus publiés sur les réseaux sociaux. Selon le Général Nicola Roxon, cette loi devrait aider les forces de police à lutter contre la cybercriminalité en permettant une identification plus rapide des cybercriminels. Cette loi autorise la ratification de la Convention de Budapest sur la cybercriminalité, et permet également aux autorités fédérales de collaborer avec les services de Police étrangers dans le cadre d'enquête sur des réseaux cybercriminels mondiaux.

[PandaLabs] Classement des pays en fonction du nombre d'ordinateurs infectés

D'après une étude de PandaLabs menée d'avril à juin 2012, la Corée du Sud compte 57,3% d'ordinateurs infectés, devant la Chine à 52%, et Taïwan à 42%. La Bolivie, le Honduras, la Turquie, l'Équateur, la Russie, la Slovaquie et la Pologne se trouvent également parmi les pays les plus infectés, tandis les pays les mieux protégés sont la Suisse (18,4%), la Suède (19%), la Norvège, le Royaume-Uni, l'Uruguay, l'Allemagne, l'Irlande, la Finlande, la Hongrie, et les Pays-Bas. Durant ce trimestre, 6 millions de maliciels ont été générés, dont 76% de troyens, 11% de vers et 7,4% de virus. Selon le directeur technique de PandaLabs Luis Corron, cette nette tendance à l'infection par des troyens témoigne des motifs économiques de la génération de programmes malveillants.

[F-Secure] Rapport semestriel de F-Secure

F-Secure a publié son rapport semestriel sur l'état des cybermenaces. L'accent est mis sur le rôle croissant des Etats dans la mise en œuvre de certaines attaques. Mikki Hypponen, directeur des recherches chez F-Secure, a constaté que Stuxnet et ses successeurs (Flame, Gauss) constituent des tournants dans l'évolution des menaces. Il en a conclu que nous étions à l'aube d'une nouvelle course au cyber-armement. Le rapport s'est également attardé sur l'accroissement des maliciels visant les Macs depuis plusieurs mois.

[Enisa] Etude sur les notifications d'incidents dans l'Union Européenne

L'ENISA publie une étude sur la législation actuelle (comme l'article 13a du paquet télécoms ou l'article 4 de la directive e-privacy) et future (notamment la proposition de directive sur l'identité électronique) en matière de notifications d'incidents à l'échelle de l'Union Européenne. Le constat général est que les pratiques ne sont pas harmonisées entre les différents États-membres et que la majorité des incidents ne sont pas notifiés.

[Symantec] Nouveau rapport Symantec sur l'état des cybermenaces

Symantec a publié début août son rapport couvrant la première moitié de l'année 2012. Les rédacteurs ont constaté le foisonnement des menaces utilisant les Jeux Olympiques de Londres pour appâter leurs victimes. Les moyens sont variés : spams, scams, liens sur Twitter, applications pour téléphone mobile, etc. On remarque également l'accroissement des « attack toolkits », qui sont en moyenne trois fois plus actifs ces six derniers mois qu'à l'accoutumée.

[Strategic Studies Institute] Publication des sujets d'études stratégiques clés pour l'armée américaine

L'institut d'études stratégiques a publié la liste des sujets de recherche intéressant particulièrement l'US Army pour l'année à venir. Plusieurs sujets concernent les cyberattaques et la cyberdéfense, parmi lesquels : à quel moment peut-on considérer une cyberattaque comme un acte de guerre ? Comment distinguer les activités criminelles et les actes de guerre dans le cyberespace ? A qui revient la défense du cyberespace ? Y-a-t-il un risque à utiliser du matériel fabriqué à l'étranger ? La doctrine Monroe doit-elle être transposée dans le cyberespace ?

L'e-Diplomacy américaine

Une stratégie assumée, mais encore largement contestée

Les Etats-Unis ont très tôt annoncé leurs intentions en matière de stratégie numérique. En effet, les initiatives de l'Administration Obama en matière de diplomatie publique sont le prolongement d'idées développées au cours du second mandat de G. W. Bush[1]. La voie avait été ouverte dès octobre 2003, avec la création d'un « Office of eDiplomacy » chargé de faciliter le dialogue entre les Etats-Unis et les peuples du monde entier.

La liberté de connexion comme justification à l'intervention numérique

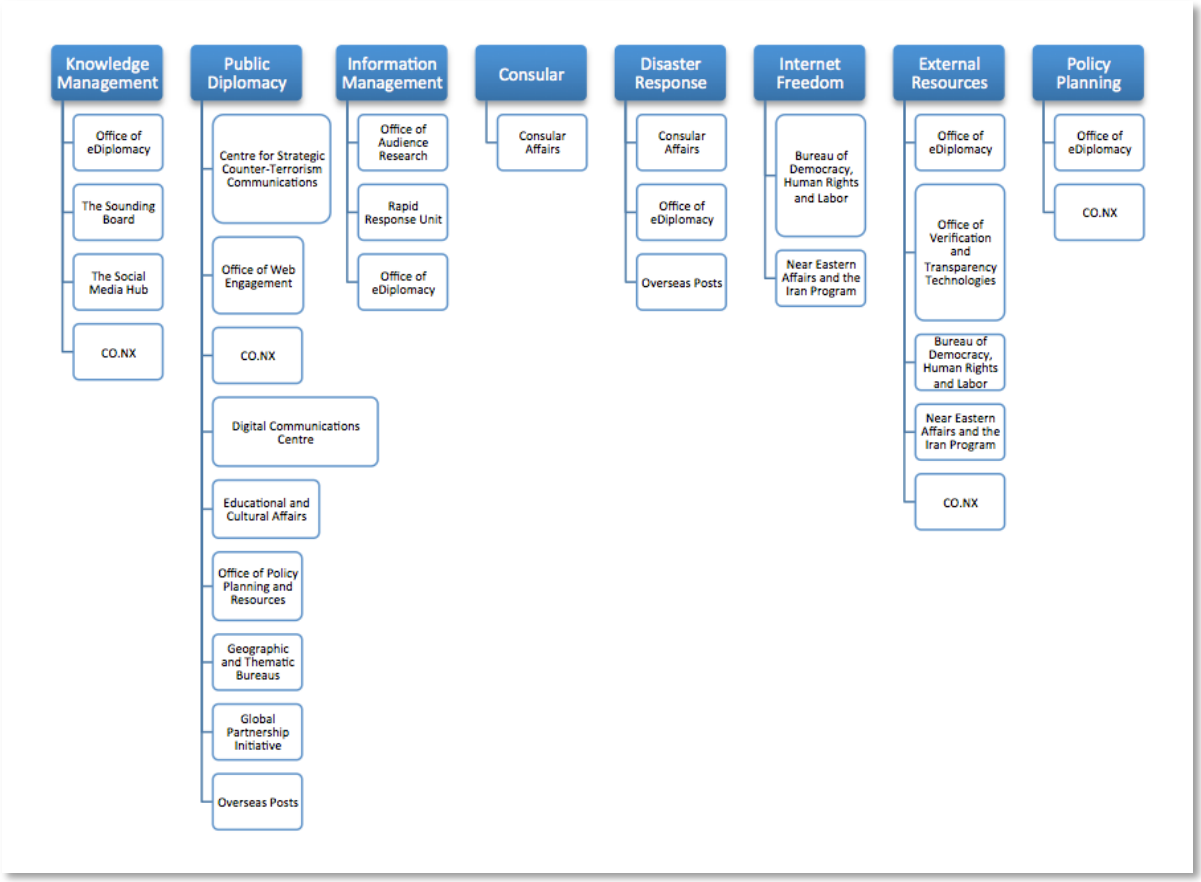

Figure 1. Principaux programmes de l'e-Diplomacy américaine[2]

[1] Julien Nocetti, La diplomatie d'Obama à l'épreuve du Web 2.0, Politique Etrangère 1 :2011

[2] http://lowyinstitute.richmedia-server.com/docs/Hanson_Revolution-at-State.pdf

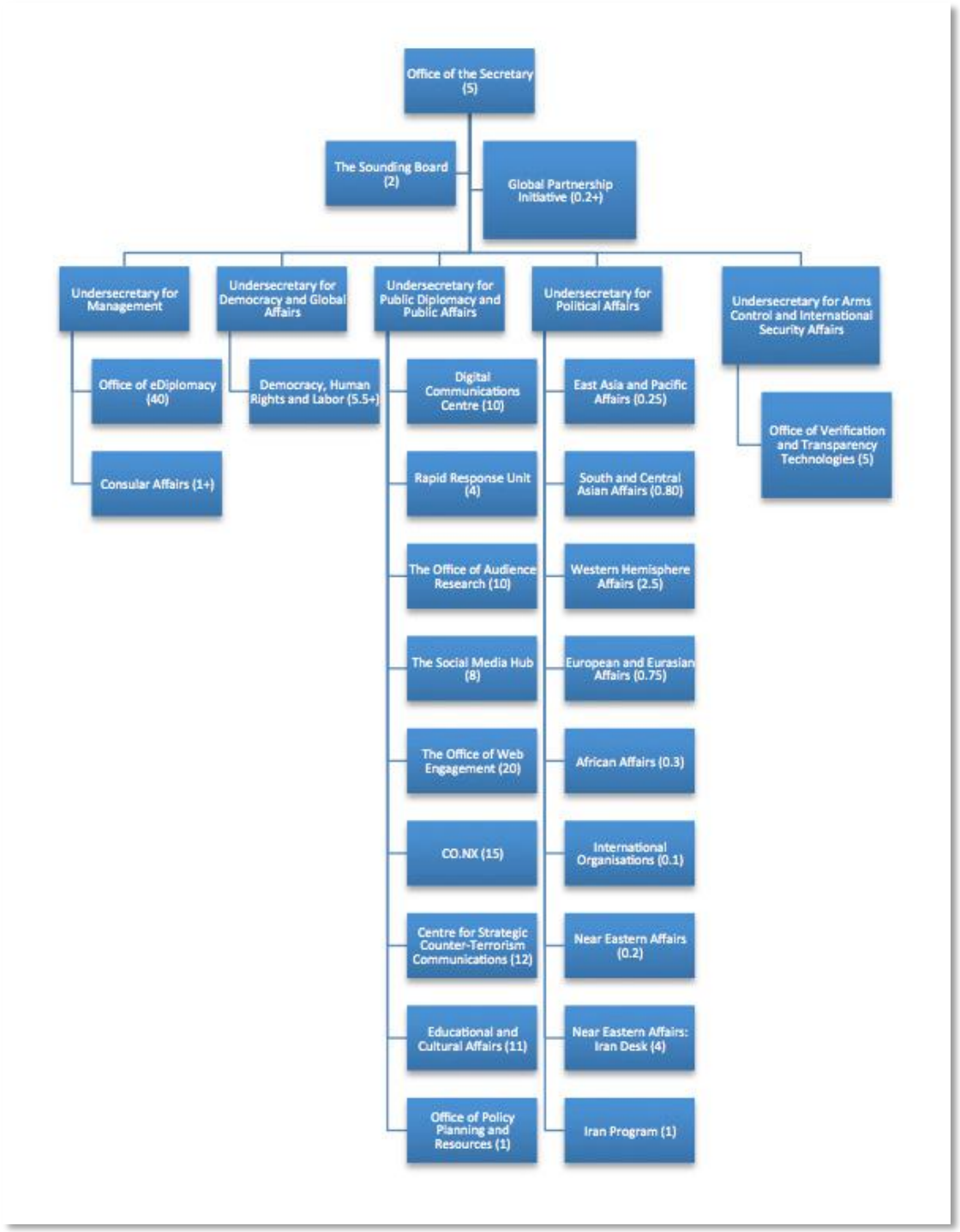

Figure 2. Schéma organisationnel de l'e-diplomacy américaine[3]

[3] http://lowyinstitute.richmedia-server.com/docs/Hanson_Revolution-at-State.pdf

En 2010, « *le Département d'Etat gérait environ 230 comptes Facebook, 80 comptes Twitter, 55 chaînes YouTube et 25 blogs actifs* »[4]. En 2011, la DARPA (Defense Advanced Research Projects Agency) lançait un appel d'offres[5] pour la réalisation d'un programme permettant d'identifier les tendances sur les réseaux en temps réel et de faciliter la diffusion d'informations sur les réseaux sociaux[6], témoignant de l'intérêt des militaires américains pour ce qui s'y déroule. Les nouvelles technologies de l'information et de la communication ont donc été identifiées depuis longtemps comme un enjeu stratégique, un outil de diffusion du « smart power » américain.

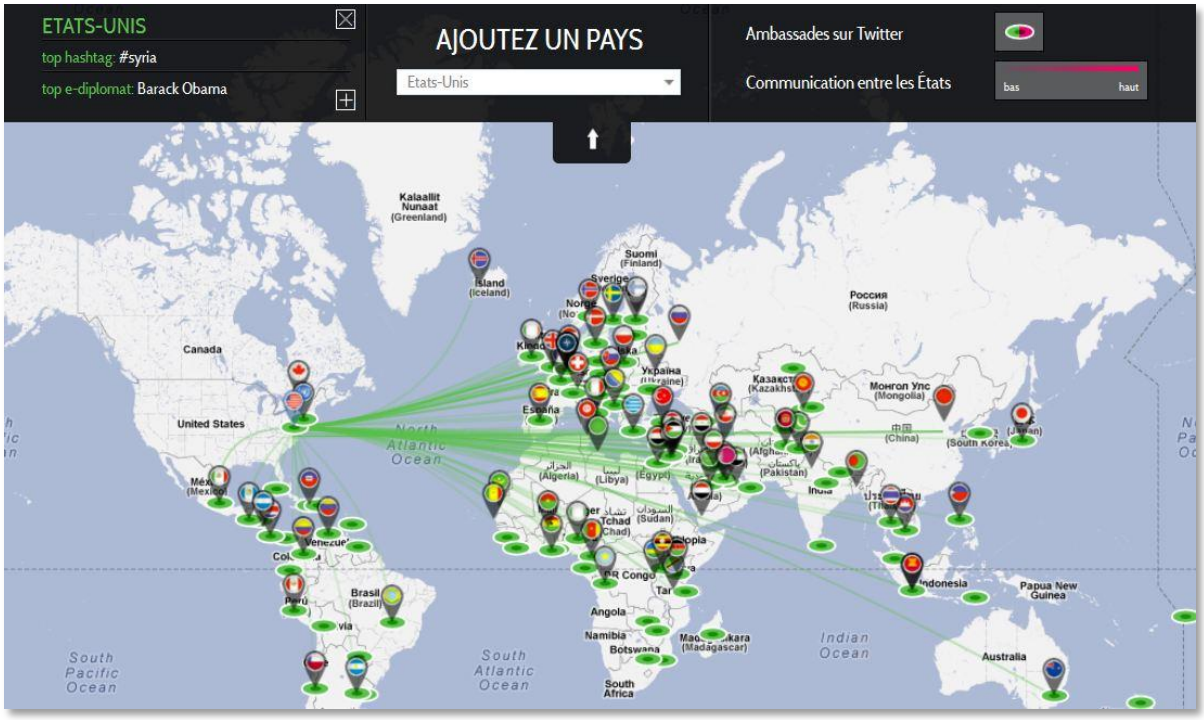

Figure 3. ***Capture d'écran du portail e-Diplomacy de l'AFP[7], illustrant l'omniprésence de la diplomatie numérique américaine***

[4] Ibid

[5] https://www.fbo.gov/index?s=opportunity&mode=form&id=6ef12558b44258382452fcf02942396a&tab=core&_cview=0

[6] http://www.wired.com/dangerroom/2011/07/darpa-wants-social-media-sensor-for-propaganda-ops/

[7] http://www.lemonde.fr/actualite-medias/article/2012/06/21/l-afp-lance-e-diplomacy_1722673_3236.html

Le 21 janvier 2010[8], alors que les cendres de la « *révolution verte* » iranienne fumaient encore et que Google avait cessé quelques jours avant toute censure des contenus sur son portail chinois[9], la Secrétaire d'Etat Hillary Clinton prononçait un discours fondateur, inspiré des thèses d'Alec Ross et de Jared Cohen[10]. Ne se contentant pas d'un plaidoyer en faveur de la liberté d'expression et, plus largement, de la liberté de connexion, Mme Clinton a affirmé que les Etats-Unis comptaient défendre activement ces droits à travers le monde[11] : « *Les Etats-Unis sont déterminés à consacrer les ressources diplomatiques, économiques et technologiques nécessaires pour favoriser la réalisation de ces libertés et de ces droits (…) étant donné le grand nombre de ces technologies qui ont vu le jour chez nous, [y compris Internet lui-même], nous avons la responsabilité de veiller à ce qu'elles soient utilisées pour le bien* ».

Cette défense des droits n'est visiblement pas nouvelle, puisqu'à l'époque du discours, le Département d'Etat avait déjà œuvré « *dans plus de 40 pays pour venir en aide aux particuliers muselés par des gouvernements oppresseurs* », et qu'il travaillait à l'élaboration de nouveaux outils permettant de contourner « *la censure à motivation politique* ». Environ 20 millions de dollars avaient été alors investis jusqu'en 2010, auxquels il faut ajouter un budget de 25 millions de dollars pour 2011. Au total, le Congrès a alloué, entre 2008 et 2012, 95 millions de dollars aux différents programmes de promotion de la liberté sur Internet. L'objectif affiché est donc de « *faire usage de la puissance des technologies connectives et les appliquer à la réalisation de nos objectifs diplomatiques* », mais pas seulement, car ces principes ont une « *portée universelle et sont bons pour les affaires* ». De ce fait, la secrétaire d'Etat a invité les entreprises américaines à adopter une position ferme en faveur de la liberté d'expression. La posture américaine a donc plusieurs fondements, comme le résume Hillary Clinton en conclusion : « *en œuvrant dans ce sens, nous alignons nos principes, nos objectifs économiques et nos priorités stratégiques* ». Certains ont observé « *une rhétorique à l'accent de guerre froide* »[12] dans ce discours, avec des références au mur de Berlin, aux samizdats et à la notion de « rideau de fer de l'information ».

Un an plus tard, le 15 février 2011, la Secrétaire d'Etat prononçait un second discours[13] reprenant les grandes lignes du précédent. Mme Clinton y a notamment défendu la stratégie consistant à soutenir une multitude de projets en faveur de la liberté d'Internet, car il n'existe pas un seul moyen miraculeux permettant de lutter contre l'oppression, « *there's no app for that* ». Au contraire, soutenir plusieurs projets permet d'avoir toujours une solution de rechange si l'un d'eux est contré par un censeur.

[8] http://www.state.gov/secretary/rm/2010/01/135519.htm

[9] Le 13 janvier 2010, le Chief Legal Officer de Google, David Drummond, a expliqué que la société avait été victime d'attaques informatiques visant à accéder à des données de militants pour les droits de l'homme chinois. Le moteur de recherche a par conséquent décidé de suspendre la censure des contenus sur son portail chinois. Pour lire l'article en intégralité : http://googleblog.blogspot.fr/2010/01/new-approach-to-china.html

[10] http://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html?_r=2&pagewanted=all

[11] Le discours dans son ensemble ne traitait pas uniquement des luttes politiques, mais dressait le portrait des bienfaits que les TIC pouvaient apporter à l'humanité : télémédecine, organisation en cas de catastrophe naturelle, lutte contre la pauvreté, développement économique, etc. Notre propos se concentrera sur les aspects diplomatiques du discours.

[12] Julien Nocetti, La diplomatie d'Obama à l'épreuve du Web 2.0, Politique Etrangère 1 :2011

[13] http://www.state.gov/secretary/rm/2011/02/156619.htm

Cette stratégie n'a pas été démentie depuis, et, dans une tribune parue au mois de juin 2012[14] intitulée « *How connective tech boosts political change* »[15], Alec Ross, le « stratège numérique » d'Hillary Clinton, tire trois conclusions des récents évènements au Moyen-Orient. Premièrement, ces technologies précipitent les mouvements sociaux et politiques. Elles permettent également d'enrichir le paysage informationnel, en multipliant les sources d'informations et les possibilités de partage de documents. Enfin, elles permettent une redistribution des pouvoirs en faveur des citoyens, favorisant les organisations décentralisées au détriment de la structure pyramidale classique.

Une instrumentalisation des réseaux source de critiques

Cette stratégie a reçu un accueil mitigé parmi les différents spécialistes d'Internet et autres activistes, autant sur la forme que sur le fond.

Evgeny Morozov[16] est le plus célèbre critique de la vision de ceux qu'il appelle les « cyberutopistes ». Selon lui, en associant si étroitement la liberté d'Internet à la stratégie américaine, on fait de cette liberté une sorte de « cheval de Troie de l'impérialisme américain », ce qui dessert le projet initial. Détournant la célèbre réplique du roman de Chuck Palahniuk *Fight Club*, il déclare : « *first rule of promoting Internet freedom: don't talk about promoting Internet freedom* ». Il explique également que la proximité affichée par le gouvernement avec les géants américains d'Internet a desservi ces derniers en les déligitimant[17], car les soupçons de connivence avec les autorités ont fait que désormais, lorsqu'une entreprise s'exprime, on ne manque pas d'y deviner la main de Washington. Un rapport du Congressional Research Service émet d'ailleurs des doutes sur la perception de la politique américaine à l'étranger : « *Focusing Internet freedom efforts on priority countries such as China and Iran has led some to question whether the United States considers Internet freedom a* ***global principle*** *or merely a* ***selective tool*** *of U.S. foreign policy* »[18].

Julien Nocetti, chercheur à l'IFRI, ne dit pas autre chose lorsqu'il explique qu'« au fil de ces débats se profile le concept de souveraineté de l'information »[19]. L'omniprésence des acteurs américains[20] dans le secteur IT entraîne une frilosité de plus en plus grande parmi les autres Etats, qui cherchent à affirmer leur indépendance. Ainsi, Google apparaît *« chez un nombre croissant de dirigeants russes comme une extension du département d'Etat américain »*[21]. Cette crainte pousse un grand nombre de pays à vouloir étendre leur souveraineté sur une partie du web. Ils tentent pour cela de fragmenter le web mondial afin d'en extraire une part nationale – si tant est que ce soit possible -, qui pourrait progressivement être isolée du reste du monde. En témoigne les exemples de projets de moteur de recherche national en Turquie, en Russie, d'Intranet national en Iran, etc.

[14] http://edition.cnn.com/2012/06/20/opinion/opinion-alec-ross-tech-politics/index.html?
[15] Traduction : Comment des TIC accélèrent les changements politiques ?
[16] http://www.foreignpolicy.com/articles/2011/01/02/freedomgov?page=full
[17] http://www.fas.org/sgp/crs/row/R42601.pdf
[18] Ibid
[19] www.ifri.org/downloads/pe22011articlejuliennocetti.pdf
[20] Citant Steve Rubel, expert en nouveaux médias chez Edelman, Eric Scherer explique que « cinq sociétés technologiques américaines influent ensemble sur toute l'offre d'information en ligne : Twitter, Facebook, Apple, Google et Amazon ». Voir : http://meta-media.fr/2012/08/10/cinq-societes-us-controlent-lacces-a-linfo/
[21] www.ifri.org/downloads/ifrinocettiweb**russe**fra30mars2011.pdf

A ceux qui, comme Jared Cohen, fustige l'excès de prudence de M. Morozov en expliquant qu'il néglige le fait que ces technologies vont se répandre de plus en plus, et que d'une manière ou d'une autre, la diplomatie doit utiliser ces nouveaux outils[22], il ne manque pas de rappeler l'échec de la technologie Haystack[23] (technologie anti-censure) en Iran, signifiant par là qu'à ses yeux la technologie ne peut pas tout. Quoiqu'il en soit, il est clair que pour Hillary Clinton et ses conseillers, les bénéfices excèdent largement les risques encourus[24].

Sur le fond, certains se sont interrogés sur le caractère libérateur des outils numériques. Dans son article éponyme, Larry Diamond définissait les *liberation technologies* comme « *les technologies de l'information et de la communication qui permettent de développer la liberté politique, sociale et économique* ». Soulignant l'importance du contrôle de l'information dans le maintien des régimes autoritaires, il explique que les « *technologies libératrices* » peuvent affaiblir l'emprise des Etats sur ce contrôle, créer une sphère publique, introduire de la transparence pour finalement donner aux citoyens la possibilité de se mobiliser.

Mais cette thèse ne fait pas l'unanimité. Dès 2007, Joshua Goldstein[25] s'interrogeait, à propos de la révolution Orange ukrainienne de 2004, sur un potentiel retournement des nouveaux medias contre les mouvements d'opposition : « *are these tools [communication tools] inherently conducive to the expansion of civic engagement and democratization or will authoritarian governments adapt the technology to their own advantage?* »[26].

De son côté, Julien Nocetti estime que les régimes autoritaires s'adaptent aux NTIC[27] et que ces derniers *« pourraient se retourner contre les pays occidentaux* ». Il explique plus loin que « *le Web permet certes d'élargir le champ d'action de la pratique diplomatique, mais reste un simple outil. Et cet outil est disponible pour tous : ceux qui œuvrent pour étendre la « démocratie participative », ceux qui cherchent à manipuler les gouvernements, ceux qui ambitionnent de consolider leur pouvoir. Ce qui conduit à s'interroger : qui peut utiliser au mieux ces outils ?* ».

De son côté, Pékin reste sceptique face aux intentions américaines[28]. Les Chinois ont surtout retenu que Washington se réservait le droit d'utiliser « tous les moyens nécessaires »[29] et appropriés pour se défendre. Le cyberespace est donc bien, même s'il ne s'y limite pas, un espace d'affrontement, et pas seulement un espace commun d'échange et d'innovation. De plus les Etats-Unis mettent tous les moyens en œuvre pour conserver une avance significative en matière technologique, et ce malgré les appels à coopération affichés. Ce qui est présenté côté américain comme une volonté de coopération pacificatrice est perçue par les Chinois comme une tentative de consolidation de la puissance technologique américaine. Enfin, certains observateurs chinois estiment que la défense de la liberté d'Internet va exacerber les tensions existantes et provoquer une augmentation des conflits.

[22] Un des initiateurs de la stratégie numérique du Département d'Etat et aujourd'hui directeur de Google Ideas.
[23] http://www.guardian.co.uk/technology/2010/sep/17/haystack-software-security-concerns
[24] http://www.nytimes.com/2010/07/18/magazine/18web2-0-t.html?_r=2&pagewanted=all
[25] Chercheur du *Berkman Center for Internet and Society* de l'Université de Harvard.
[26] http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf
[27] Il rappelle la thèse défendue dès 2003 par S. Kalathil et T. Boas dans leur ouvrage *Open Networs, Closed Regimes : The Impact of the Internet on Authoritarian Rule*
[28] http://blogs.cfr.org/asia/2011/05/23/chinese-responses-to-the-international-strategy-for-cyberspace/
[29] http://www.whitehouse.gov/sites/default/files/rss_viewer/International_Strategy_Cyberspace_Factsheet.pdf

De multiples transpositions dans les faits

La position américaine de soutien au contournement de la censure a été illustrée par plusieurs exemples ou projets, toujours sous couvert de soutiens à différentes organisations non gouvernementales comme l'*Institute for War & Peace Reporting* et *Freedom House*[30]. Le lien n'est jamais direct entre les activités des dissidents et le soutien américain, car cela pourrait être perçu comme de l'ingérence dans des affaires internes au pays, voir comme un acte hostile[31].

La Syrie est le dernier terrain d'opérations en date de la stratégie numérique américaine, même si, à l'origine, c'était la Chine qui était la première « cible » des américains. En outre, les précédentes révolutions arabes ont été riches d'enseignements pour les têtes pensantes américaines. Le cœur de la lutte numérique consiste à donner aux insurgés la possibilité de communiquer sur leur lutte. Une démarche qui passe par plusieurs étapes :

- 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,

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

- 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,

- former les utilisateurs à l'utilisation des outils numériques en toute sécurité. Il s'agit d'initier les utilisateurs aux techniques de chiffrement et d'anonymisation des connexions, ainsi qu'aux techniques permettant de déjouer la surveillance des Etats.

[30] http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/#ixzz1xmJH3W7V

[31] En effet, l'arrêt des télécommunications et la suspension du service internationale sont prévues aux articles 34 et 35 de la Constitution internationale de l'Union Internationale des Télécommunications (UIT). Ainsi, l'article 34-2 autorise les Etats Membres, sous réserve de conformité à la législation nationale, à interrompre toute « télécommunication privée qui peut paraître dangereuse pour la sûreté de l'Etat ou contraire à ses lois, à l'ordre public ou aux bonnes mœurs ». De même, l'article 35 permet aux Etats Membres « de suspendre le service international de télécommunication » de manière générale ou particulière, à condition de prévenir le Secrétaire général de l'UIT.

Le portail OMC
La nouvelle plateforme de la DAS

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

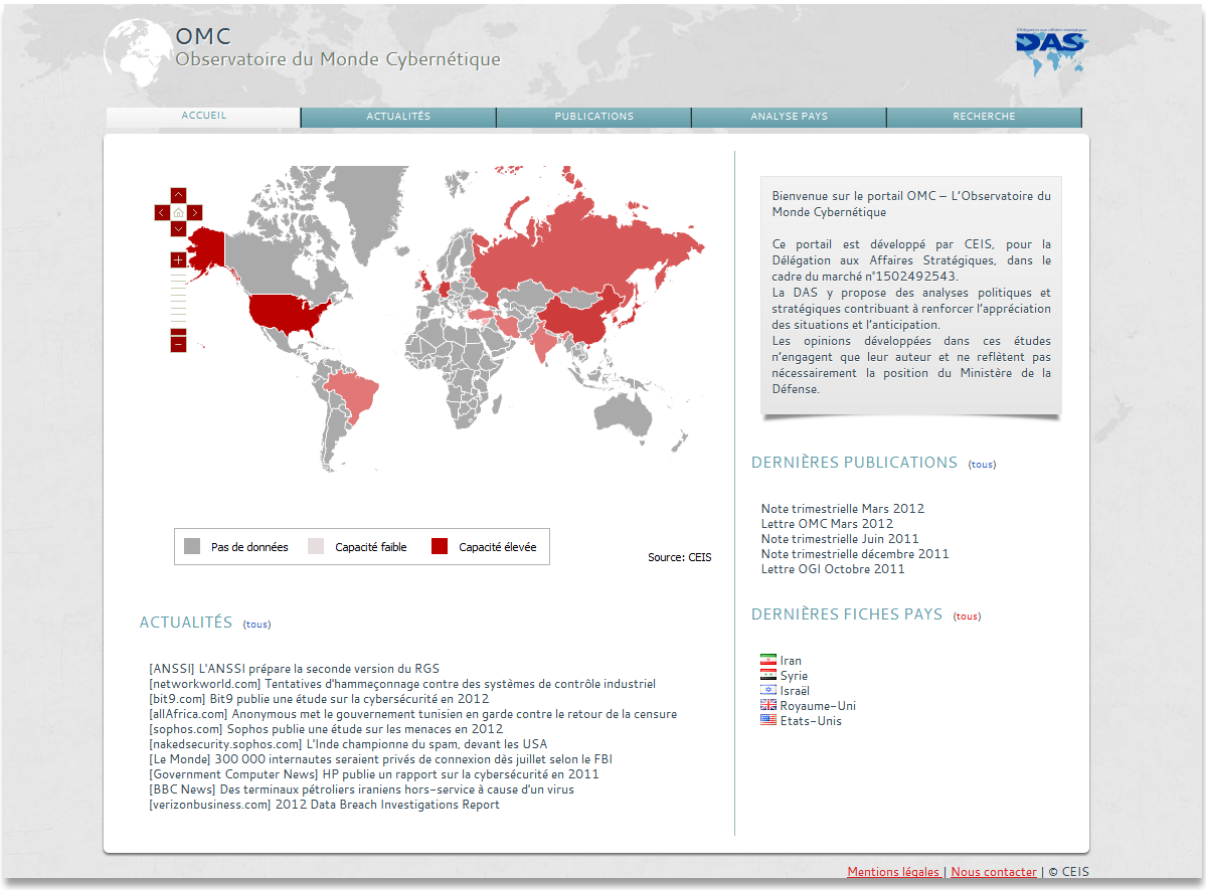

Figure 4. Page d'accueil du portail OMC - https://omc.ceis.eu/

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

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

Petit Déjeuner SecurityVibes	Paris	20 septembre
InfoSecurity International Summit 2012	Allemagne	24 – 25 septembre
InfoSecurity International Summit 2012	Shanghai	25 – 26 septembre
VMworld EMEA	Barcelone (Espagne)	9 – 11 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

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