Observatoire du Monde Cybernétique
Trimestriel

Juin 2012

DELEGATION AUX AFFAIRES STRATEGIQUES
MINISTERE DE LA DEFENSE

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.

Sommaire

1 Syrie, capacités et rôles dans le conflit actuel

1.1 Introduction

L'effet de contagion du Printemps arabe peine à s'étendre à la Syrie. Le conflit syrien, qui dure maintenant depuis plus d'un an oppose d'un côté les opposants au régime baasiste, qui réclament des réformes démocratiques et le départ du président Bachar Al-Assad, à Bachar Al-Assad lui-même qui, refusant de quitter son poste met tout en œuvre pour enrayer, écraser la rébellion. Violences, arrestations et tortures de dissidents sont rapportées par les médias qui tentent, malgré la réticence de Damas, de couvrir la crise. Et si les arrestations de bloggeurs, de journalistes et de net-citoyens se multiplient[1], les dissidents ne cessent pourtant de s'organiser et de défier le pouvoir en place tant dans la rue que dans le cyberespace.

Mais le gouvernement, qui a toujours eu la main mise sur les médias et les réseaux de communication[2], les contrôle aujourd'hui plus étroitement que jamais depuis le début des contestations dans le pays, en mars 2011. Population et gouvernement syrien se livrent ainsi à une incontestable guerre de l'information, en exploitant ou en instrumentalisant Internet, faisant de ce réseau l'un des pivots du succès de leurs actions.

Aussi, plus qu'un simple moyen de communication et d'organisation, Internet est devenu un véritable enjeu stratégique pour les dissidents et le gouvernement. Les premiers tiennent à témoigner des massacres et à mobiliser l'opinion publique internationale pour accentuer la pression sur Bachar Al-Assad (1.1.) tandis que celui-ci tente d'étouffer la contestation qui se prolonge sur Internet (1.2.).

Ce dossier se propose de passer en revue, à l'aide de sources ouvertes[3] et en langue native[4] l'étendue du rôle et des capacités de chacun (acteurs, objectifs, moyens d'action, etc.) sur Internet, et leurs conséquences dans le cadre du conflit syrien actuel.

1.2 Capacités et rôle de la dissidence syrienne

> « *On ne gagne pas de guerre sans d'abord gagner la guerre des médias* »
> Shakeeb al-Jabri (blogueur syrien exilé à Beyrouth, Liban), au Figaro[5]

---

[1] Depuis le début du soulèvement pro-démocratique, 15 journalistes ont été emprisonnés, 4 tués et 18 net-citoyens sont également en prison. http://fr.rsf.org/report-syrie,163.html

[2] Voir infra

[3] Et donc exhaustives dans la mesure du possible.

[4] Arabe, anglais et français.

[5] http://www.lefigaro.fr/international/2012/06/18/01003-20120618ARTFIG00820-en-syrie-la-guerre-passe-aussi-par-les-images.php

C'est dans la rue que les manifestations anti-gouvernementales sont nées et continuent de se dérouler. Néanmoins, à l'instar des évènements du « Printemps arabe », les opposants au régime se sont vite emparés d'Internet pour s'organiser et témoigner. De nombreux dissidents évoquent ainsi le massacre de Hama en 1982[6], largement méconnu du reste du monde, pour expliquer le recours à Internet et, notamment, aux réseaux sociaux. « *Sans Internet, nous mourrions en silence* », explique ainsi une cyberdissidente syrienne[7] : le Web est « *la fenêtre du monde sur la Syrie* » et les opposants au régime refusent que les massacres se déroulent à huis-clos. Dans une vidéo diffusée dès le début des manifestations[8], le message est clair : « *Votre silence est leur arme la plus redoutable* ».

1.2.1 Internet, une fenêtre sur le monde

Le réseau des réseaux joue un rôle essentiel dans le soulèvement pro-démocratique. Mais il convient de ne pas tomber dans l'angélisme au sujet des vertus libératrices des réseaux sociaux, en affirmant simplement que la Syrie connaît une « révolution 2.0 ». Comme le montre le nombre d'arrestations de bloggeurs et cyber-activistes, les liens entre le cyberespace et le monde réel sont étroits et nul ne fait la révolution tranquillement assis derrière son écran d'ordinateur. Les risques existent bel et bien pour celui qui diffuse des vidéos ou des appels à manifester, au même titre que pour celui qui défile dans la rue.

Et c'est là que réside sans doute un des aspects essentiels de ces contestations nées en Afrique et au Moyen-Orient : désormais, « online » et « offline » sont imbriqués et leur articulation vise à renforcer l'action des manifestants. Ainsi, les dissidents utilisent Internet tant pour s'organiser dans la rue que pour témoigner de la répression gouvernementale. En Syrie, néanmoins, les opposants au régime n'ont pas eu tout à fait le même usage des réseaux sociaux que leurs voisins.

1.2.1.1 Le conflit syrien : un usage atypique des réseaux sociaux

Selon le blogueur syrien Shakeeb Al-Jabri, la Syrie est « *complètement dépendante des médias sociaux* »[9]. S'il est vrai que le Web 2.0 joue un rôle essentiel dans la guerre de l'information que se livrent le gouvernement syrien et les dissidents[10], il convient néanmoins de souligner que les réseaux sociaux n'ont pas été utilisés comme en Egypte ou en Tunisie. Véritables outils d'organisation pour les manifestants de ces pays, l'usage de Facebook et Twitter a mené certains observateurs à qualifier le « Printemps arabe » de « révolution 2.0 »[11]. L'opposition en Egypte était déjà présente sur Internet depuis plusieurs années[12], mais c'est le groupe Facebook « *Nous sommes tous des Khaled Saïd* », créé en juin 2010 suite à la mort de Khaled Saïd[13], qui a été utilisé pour organiser les premières

---

[6] Le président Hafez El-Assad avait alors ordonné la répression massive et sanglante des manifestants

[7] http://obsession.nouvelobs.com/high-tech/20120312.OBS3577/jasmine-cyber-dissidente-syrienne-et-prix-rsf-sans-internet-nous-mourrions-en-silence.html

[8] http://globalvoicesonline.org/2012/01/07/syria-the-struggle-for-freedom-and-the-end-of-silence/

[9] http://www.courrierinternational.com/article/2012/01/25/sans-internet-la-revolution-aurait-ete-immediatement-ecrasee

[10] Voir infra

[11] http://www.iris-france.org/docs/kfm_docs/docs/2011-04-04-facebook-twitter-al-jazeera-et-le-printemps-arabe.pdf

[12] IFRI, « La révolte en réseau : le printemps arabe et les médias sociaux » par David M.FARIS, Politique étrangère 1 :2012, pp.101-103

[13] Ce groupe a été créé par Abdel RAHMAN MONSOUR, journaliste et militant basé au Caire, et Wael GHONIM, cadre de Google installé à Dubaï.

manifestations égyptiennes au cours de l'été et de l'automne 2010. C'est sur la page de ce groupe, encore, que les appels à manifester le 25 janvier 2011 ont commencé à circuler auprès de ses membres, au nombre de 380 000 à la veille de la révolution[14]. En Egypte, les évènements de 2011 ont donc été ouvertement préparés, annoncés et organisés sur Facebook. En Tunisie, si les médias sociaux n'ont pas été à l'origine même des premières manifestations, certains bloggeurs témoignent tout de même du rôle des réseaux sociaux, qui sont devenus « *très important une fois la révolution lancée* »[15]. Selon Lina Ben Mhenni[16], « *beaucoup de manifestations ont été organisées sur Facebook et Twitter* ».

Dès lors, il aurait pu sembler évident que ces médias sociaux jouent le même rôle dans l'organisation de l'opposition syrienne. Et ce d'autant plus que, après trois années de censure, la Syrie autorise enfin l'accès à Facebook en février 2011. Alors que certains dissidents, ainsi que la communauté internationale[17], ont salué cette ouverture qui intervient peu de temps après le début des manifestations égyptiennes[18], il est apparu très vite que le gouvernement syrien avait mis en place un important système de surveillance du réseau social.

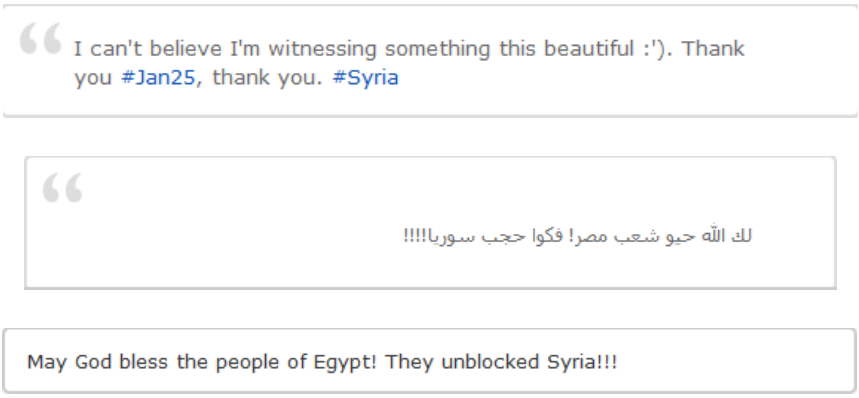
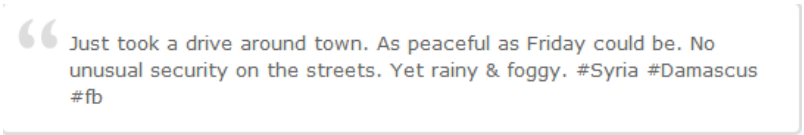


Figure 1. Tweets postés par des syriens lors de l'ouverture de Facebook[19]

Les appels au rassemblement rapidement diffusés sur Facebook n'ont, de ce fait, pas reçu l'écho escompté en Syrie. À titre d'exemple, l'appel à manifester le vendredi 4 février 2011 contre *« la monocratie, la corruption et la tyrannie »,* qui avait pourtant rassemblé plusieurs milliers de soutiens sur la page Facebook dédiée, n'a pas été suivi dans les faits[20].



[14] http://www.pbs.org/wgbh/pages/frontline/revolution-in-cairo/inside-april6-movement/
[15] IFRI, « La révolte en réseau : le printemps arabe et les médias sociaux » par David M.FARIS, Politique étrangère 1 :2012 p.106
[16] IFRI, « La révolte en réseau : le printemps arabe et les médias sociaux » par David M.FARIS, Politique étrangère 1 :2012 p.106
[17] Voir infra
[18] http://globalvoicesonline.org/2011/02/08/syria-facebook-and-youtube-unblocked-among-others/
[19] http://globalvoicesonline.org/2011/02/08/syria-facebook-and-youtube-unblocked-among-others/
[20] http://www.france24.com/fr/20110204-syrie-facebook-mobilisation-manifestation-appel-calme-damas

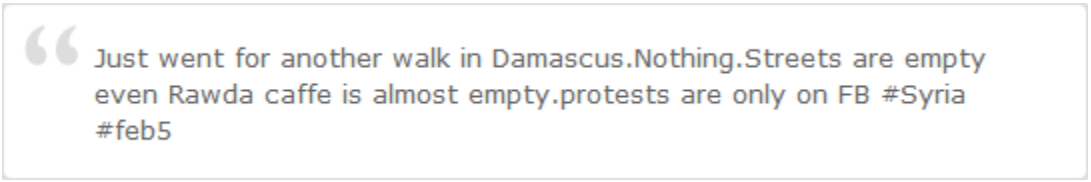


Figure 2. Tweets de dissidents syriens

Les enjeux ne sont en effet plus les mêmes. D'un côté, l'appel à manifester diffusé par Facebook expose tant l'émetteur de l'appel que les centaines de manifestants qui se rendront sur place. De l'autre, le fait de diffuser des informations réduit le périmètre de risques : le principal enjeu pour l'émetteur sera de dissimuler son identité afin de se protéger d'éventuelles représailles.

Ce sont les Comités locaux de coordination qui ont joué ce rôle de fédérateurs et d'organisateurs de manifestations[21].

S'il est donc difficile d'affirmer que l'opposition au régime a eu recours à Facebook ou Twitter pour s'organiser et se coordonner, il est néanmoins incontestable qu'elle s'est emparée du Web 2.0 pour diffuser vidéos et témoignages des évènements et de leur répression.

1.2.1.2 Témoigner à tout prix : une logique de diffusion de l'information

Alors que la presse locale est muselée et les correspondants étrangers expulsés, de nombreux Syriens s'improvisent journalistes afin de « *faire connaître, à travers Internet, à travers Skype, à travers les communications satellitaires, l'ampleur de la répression (…)* »[22]. C'est pourquoi le faible taux de pénétration syrien n'est pas un obstacle à cette démarche. En effet, les syriens ne sont pas les premiers destinataires des informations diffusées par les cyberdissidents : d'une part, les appels à manifester sont véhiculés par les centres locaux de coordination et non par les réseaux sociaux ; d'autre part, l'enjeu majeur est justement de parvenir à « *faire sortir l'information de Syrie* » et à mobiliser l'opinion internationale. Il s'agit avant tout de « *faire pression sur les gouvernements pour qu'ils s'engagent pour le départ de Bachar Al-Assad*[23] ». Et pour ce faire, les opposants au régime se sont emparés du Web.

1.2.1.2.1 Les réseaux sociaux tout de même plébiscités

Depuis les blogs[24] [25], Twitter[26], Youtube[27] ou encore Facebook[28] [29] [30] [31] [32], les opposants au régime relaient massivement des vidéos amateurs filmant les manifestations qui ont eu lieu et révélant la répression qui s'en est suivie.

---

[21] http://www.letemps.ch/Page/Uuid/71333062-a5db-11e1-9fa9-143c3f93e20d/Divis%C3%A9e_lopposition_syrienne_cherche_sa_strat%C3%A9gie

[22] http://obsession.nouvelobs.com/high-tech/20120312.OBS3577/jasmine-cyber-dissidente-syrienne-et-prix-rsf-sans-internet-nous-mourrions-en-silence.html

[23] http://obsession.nouvelobs.com/high-tech/20120312.OBS3577/jasmine-cyber-dissidente-syrienne-et-prix-rsf-sans-internet-nous-mourrions-en-silence.html

[24] http://bambuser.com/channel/baba-omer. Depuis le 16 février 2012, le site suédois Bambuser, qui permet de diffuser des vidéos prises avec un téléphone portable, est bloqué en Syrie.

Figure 3. Page Facebook du Comité de coordination de Rastan[33]

« Rastan – Bombardement par hélicoptère et artillerie pour empêcher la manifestation 29 juin 2012 »

1.2.1.2.2 Les Comités locaux de coordination et leurs « centres des médias »

Certains « net-citoyens », ces anonymes qui postent sur le Web les évènements dont ils sont témoins, se sont peu à peu organisés autour de Comités locaux de coordination[34], chacun pourvu d'un Centre des médias. Ces Centres des médias fonctionnent comme une agence de presse, proposant un flux RSS à ses visiteurs, compilant témoignages, images et vidéos. Dotés de PC portables, de clefs 3G, de clefs USB ou encore d'iPhone[35], les contributeurs de ces cellules rassemblent ainsi et diffusent, en temps réel, les informations relatives au conflit syrien. Celles-ci constituent donc une ressource phare pour les médias internationaux tenus à l'écart du territoire.

1.2.1.2.3 Des méthodes de contournement atypiques

Face aux tentatives de Damas de contrôler Internet et les mobilisations, les « net-citoyens » ont parfois recours à des procédés originaux pour relayer au mieux leurs informations : en réponse aux nombreuses coupures de réseau, certains citoyens font appel à des pigeons voyageurs pour

---

[25] http://7urreya.wordpress.com/tag/english-post/
[26] Source : http://twitter.com/#!/RevolutionSyria
[27] Source : http://www.youtube.com/watch?v=SPd3yCcIE1U
[28] Source : http://ar-ar.facebook.com/ShaamNews
[29] Source : http://ar-ar.facebook.com/UgaritNEWS
[30] Source : http://ar-ar.facebook.com/syria.news.F.N.N
[31] Source : http://www.facebook.com/pages/Syrian-Revolution-News-Round-ups/108855819196476
[32] Source : https://www.facebook.com/SuriyeDevrimi?ref=ts
[33] Source : http://www.facebook.com/RSTN.Coor
[34] Local Coordination Comittees of Syria, LCCSyria, http://www.lccsyria.org/
[35] Source : http://owni.fr/2012/03/08/syrie-liberation-freedom-4566-turquie/

communiquer entre eux[36], tandis que d'autres, situés aux frontières du pays, utilisent des serveurs libanais ou turques. Mais au-delà d'une stratégie de contournement et de diffusion de l'information, l'opposition adopte peu à peu une logique plus offensive à l'égard du pouvoir en place.

1.2.1.2.4 Le recours symbolique à l'offensif

En mars 2012, plus de 3 000 mails[37] échangés entre Bachar Al-Assad et sa femme ont ainsi été interceptés par des dissidents syriens, qui avaient mis sous surveillance leurs boites mails. Cette correspondance, transmise aux médias internationaux, a entamé encore un peu plus l'image du dirigeant syrien auprès de son peuple et de la communauté internationale. De très nombreuses voix se sont fait entendre, indignées par les téléchargements musicaux et les achats de diamants du couple, alors que des milliers de syriens « se font massacrer »[38].

Figure 4. Extraits de presse sur les emails de Bachar Al-Assad[39]

Immédiatement après ces fuites, le gouvernement s'est attelé à une véritable opération de propagande, selon laquelle il était très facile de produire de faux emails. Dans le même temps, The Guardian, le premier journal à avoir révélé l'affaire, a été bloqué sur le territoire syrien. Mais plus que la réaction de Damas, ce sont les procédés techniques utilisés par les dissidents syriens qu'il faut retenir ici. En effet, les mails n'ont pas été obtenus pas un piratage « hautement élaboré »[40] mais simplement grâce aux adresses et aux mots de passes divulgués par un sympathisant travaillant au ministère de l'Intérieur.

Aussi cette affaire souligne-t-elle l'un des aspects essentiels des capacités des cyberdissidents syriens : ceux-ci ont peu de connaissances informatiques et de savoir-faire technique, ce qui les rend très vulnérables aux diverses attaques menées par le gouvernement[41]. Face à la véritable traque dont ils

[36] Source : http://www.france24.com/fr/20120215-syrie-internet-homs-pigeons-voyageurs
[37] Source : http://www.arte.tv/fr/6536018,CmC=6536372.html
[38] Source : http://www.guardian.co.uk/world/middle-east-live/2012/mar/15/syria-assad-emails-aftermath-live#block-18
[39] Source : http://www.guardian.co.uk/world/middle-east-live/2012/mar/15/syria-assad-emails-aftermath-live#block-18
[40] Source : http://www.lemonde.fr/technologies/article/2012/03/15/les-codes-du-compte-email-d-assad-sur-un-simple-bout-de-papier_1669394_651865.html
[41] Voir infra (trojan, virus…)

font l'objet, ces cyberdissidents reçoivent alors de plus en plus de soutiens extérieurs, notamment pour sécuriser leurs communications sur Internet et préserver leur anonymat.

1.2.2 La communauté internationale solidaire des Syriens sur Internet

En diffusant sur Internet l'ampleur de la répression dont ils sont victimes, les opposants au régime sont parvenus à mobiliser la communauté internationale : syriens expatriés, sympathisants, hackers ou même gouvernements étrangers adoptent diverses méthodes pour venir en aide aux dissidents.

1.2.2.1 La diaspora syrienne s'investit dans le conflit

Les syriens exilés à l'étranger, s'ils ne peuvent participer directement au soulèvement démocratique, cherchent néanmoins à soutenir les leurs et à les aider dans leur combat.

1.2.2.1.1 Crowdmapping et géolocalisation

Le 25 mars 2012 a été mise en ligne la crowdmap[42] Syria Tracker[43], qui permet de recueillir des chiffres directement auprès de la population syrienne, via Internet et les téléphones portables. Syria Tracker permet de cartographier ainsi un bilan précis des exactions commises sur le territoire.

Lancé par un groupe d'activistes syriens exilés aux États-Unis, le site permet de géolocaliser ville par ville les meurtres, arrestations, disparitions, etc. : au 9 juin 2012, plus de 16 250 évènements ont ainsi été répertoriés sur Syria Tracker. Ici encore, grâce à une technologie développée par la plateforme open source Ushahidi[44], les activistes dénoncent la répression gouvernementale et alertent l'opinion publique internationale sur l'ampleur des massacres.

Figure 5. Carte crowdsourcée des exactions commises en Syrie[45]

[42] Source : Crowdsourcing : méthode collaborative permettant de fédérer les informations issues d'un grand nombre de personnes afin d'alimenter un projet.

[43] Source : https://syriatracker.crowdmap.com/

[44] Source : Créé au Kenya pendant les violences postélectorales de 2008, Ushahidi est un projet de crowdsourcing d'informations de crise (crise migratoire en Lybie, coupures d'électricité en Inde, trafic de drogues au Mexiques…). http://ushahidi.com/

[45] Source : https://syriatracker.crowdmap.com/

1.2.2.1.2 Les actions de sympathisants

Les syriens de l'étranger, ainsi que de nombreux sympathisants, sont à l'origine de diverses campagnes de soutien en ligne. Grâce aux réseaux sociaux et à leur viralité, plusieurs initiatives ont été élaborées pour soutenir et encourager la population syrienne. En mobilisant des citoyens du monde entier, ces campagnes visent à sensibiliser les gouvernements et à les amener à condamner le régime syrien. En novembre 2011, la campagne « Call Homs » invitait chacun à composer l'indicatif téléphonique de la ville de Homs afin de souhaiter à des familles syriennes de passer un « *joyeux Aïd* »[46]. Sur Facebook et sur Twitter, la campagne a reçu un vaste écho :

Figure 6. Tweets postés en soutien des Syriens

Toujours dans cette logique de soutien au peuple syrien, YouTube a également été utilisé pour diffuser un **sit-in virtuel mondial**, « Syrian sit-in in YouTube »[47]. Au travers de courtes vidéos, des individus du monde entier ont déclaré leur soutien aux dissidents et condamné la violence gouvernementale. En outre, comme de nombreux dissidents le soulignent, « *le régime fait toujours plus attention quand il s'agit de gens connus* »[48] : aussi, de plus en plus de campagnes sont lancées par des syriens ou des sympathisants pour attirer l'attention sur l'arrestation d'un bloggeur ou d'un manifestant et pour réclamer sa libération. À titre d'exemple, l'opposante Yasmin Bakaji a ainsi été libérée 24 heures après son arrestation, la page Facebook lancée pour l'occasion ayant rassemblé plus de 1 140 membres en quelques heures[49].

Ces différents exemples de mobilisation montrent que la chaîne de solidarité internationale, souhaitée par les dissidents syriens, s'est peu à peu mise en place. Certains acteurs vont même encore plus loin dans l'aide apportée aux opposants du régime, pour notamment leur permettre d'échapper à la traque gouvernementale dont ils font l'objet.

---

[46] Source : http://globalvoicesonline.org/2011/11/09/global-campaigns-in-solidarity-with-syria-keep-growing/
[47] Source : http://www.syriansitin.com/
[48] Source : http://owni.fr/2012/03/08/syrie-liberation-freedom-4566-turquie/
[49] Source : http://cyberdissidents.org/bin/content.cgi?ID=1112&q=1&s=16

1.2.2.2 Des hackers engagés aux côtés des dissidents

Le soulèvement pro-démocratique en Syrie, au même titre que les autres révolutions du « Printemps arabe », ne peut être qualifié de simple révolution 2.0 dans la mesure où les actions menées sur le Web sont relayées dans la rue mais donnent également lieu à de nombreuses arrestations de bloggeurs et cyber-activistes. Damas a en effet mis en place une véritable stratégie de cybersurveillance et les dissidents ne sont pas toujours armés pour y échapper. Aussi, plusieurs groupes de hackers politiques, des hacktivistes, se sont organisés pour apporter leur expertise et leur savoir-faire aux opposants syriens.

1.2.2.2.1 #OpSyria

Telecomix, un cluster d' hacktivistes réunissant informaticiens, professeurs, étudiants et autres types de profils variés pour la défense d'un « Internet libre », s'est ainsi le premier engagé aux côtés des dissidents syriens. Dans la nuit du 4 au 5 septembre 2011, l'opération #OpSyria a ainsi été lancée pour permettre aux opposants à Damas de contourner la censure gouvernementale sur la Toile. Telecomix est parvenu à détourner tout le trafic Internet du pays vers une page spéciale proposant des conseils pour naviguer sur le Web en toute sécurité. Les dissidents ont ainsi pu apprendre à installer le logiciel d'anonymisation Tor ou à utiliser une connexion sécurisée en https. Une véritable formation des dissidents aux outils de chiffrement est ainsi dispensée par les « agents » de Telecomix, qui se relaient également sur leur canal IRC dédié à la Syrie pour directement discuter avec les opposants au régime et faciliter la diffusion de vidéos, de photos et de témoignages. Un site de dépêches mis à jour en temps réel a également été mis en ligne[50], accompagné de la plateforme Syrian Stories[51] qui éditorialise le contenu du premier site.

1.2.2.2.2 La créativité technologique mise au service des dissidents

En outre, Telecomix serait actuellement en train de travailler à la construction de drones miniatures dotés de caméras, qui seraient pilotés à vue et permettraient la récolte des informations sans mettre en danger la vie des dissidents[52]. L'entrée sur le territoire de ces drones serait organisée par les réseaux des ONG, via la Turquie, le Liban ou la Jordanie. Dans le même ordre d'idées, enfin, le cluster de hacktivistes réfléchirait à un détournement de la célèbre Pirate Box, outil de partage de fichiers en tout anonymat : plutôt que de servir à partager de la musique, Telecomix souhaiterait que la Pirate Box, alimentée par panneaux solaires, serve à « *communiquer dans un périmètre critique* »[53], grâce notamment à un module de chat anonymisé.

[50] Source : http://broadcast.telecomix.org/syria/
[51] Source : http://syrianstories.org/
[52] Source : http://owni.fr/2012/06/03/telecomix-syrie-ong-drone/
[53] Source : http://owni.fr/2012/06/03/telecomix-syrie-ong-drone/

Figure 7. Des drones miniatures pour filmer en toute sécurité en Syrie[54]

1.2.2.2.3 Piratage et défaçage

Telecomix n'est cependant pas le seul groupe de hackers engagé aux côtés des dissidents syriens. Dans un tout autre registre, les Anonymous se sont également fait entendre en défigurant divers sites officiels pour y laisser un message de soutien aux opposants[55] ou encore en piratant les mails de plusieurs collaborateurs du chef de l'État syrien[56].

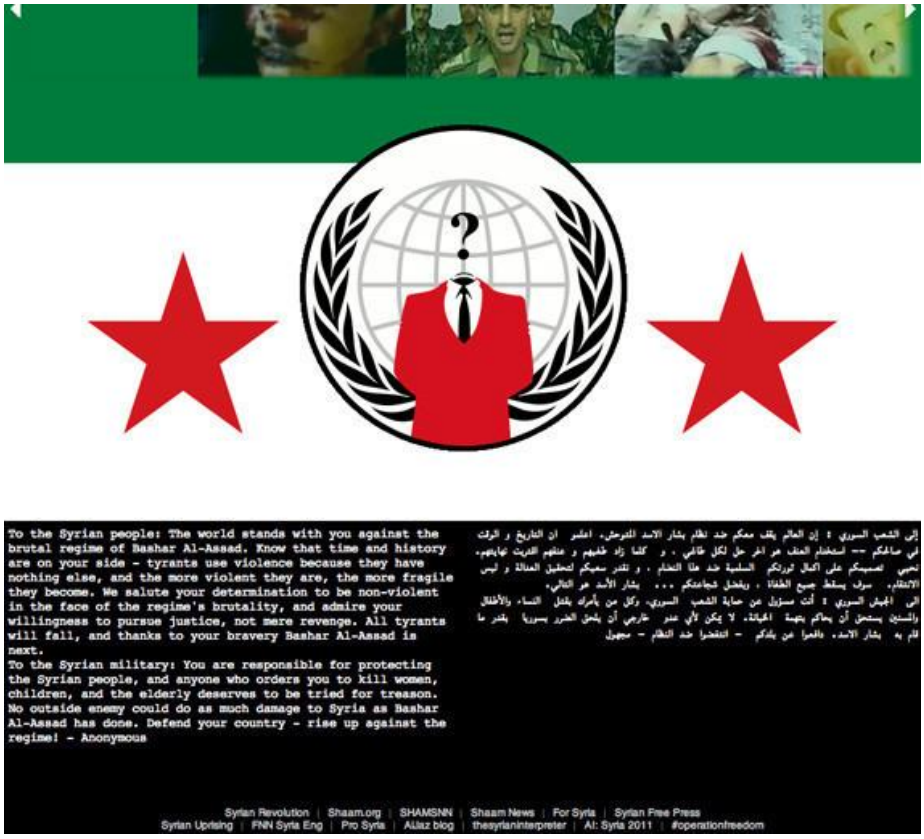


Figure 8. Le site du ministère syrien de la Défense défacé par les Anonymous[57]

---

[54] Source : http://owni.fr/2012/06/03/telecomix-syrie-ong-drone/

[55] Source : http://www.huffingtonpost.com/2011/08/08/syria-ministry-of-defense-hacked-anonymous_n_920733.html

[56] Source : http://www.lefigaro.fr/international/2012/02/12/01003-20120212ARTFIG00187-des-hackers-devoilent-les-mails-secrets-entre-damas-et-teheran.php

[57] Source : http://www.huffingtonpost.com/2011/08/08/syria-ministry-of-defense-hacked-anonymous_n_920733.html

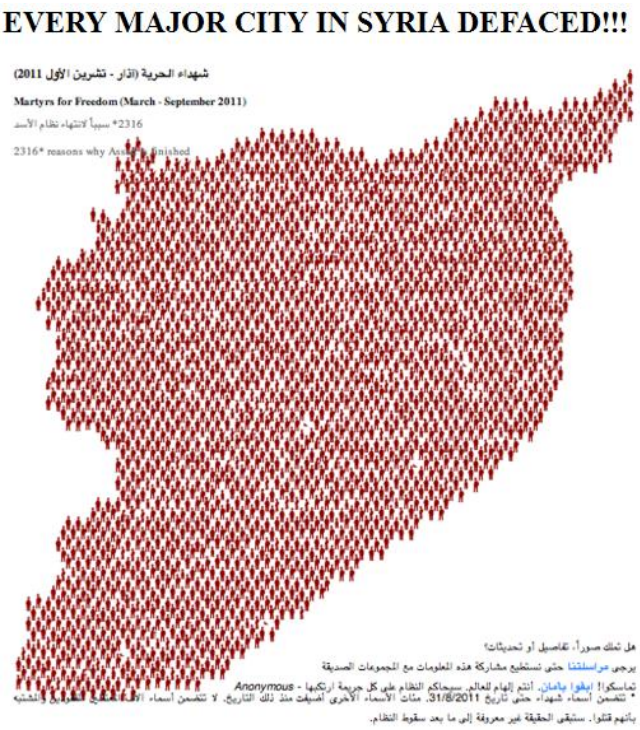


Figure 9. Les sites Internet officiels défigurés par une carte interactive de la Syrie, montrant les noms, les âges et les dates de décès des victimes du régime de Bachar Al-Assad[58]

1.2.2.2.4 L'Electronic Frontier Foundation

Enfin, l'Electronic Frontier Foundation[59] réalise une veille active de l'Internet syrien et lance de nombreuses alertes relatives aux attaques du gouvernement. L'association de défense des libertés numériques a ainsi prévenu les dissidents de la circulation d'un faux programme de chiffrement pour Skype[60] (en réalité un programme malveillant d'espionnage), de la mise en ligne d'un faux Youtube[61] ou encore de la multiplication de tentatives de phishing sur Facebook[62].

Face à l'arsenal déployé par le gouvernement syrien sur Internet, les dissidents sont peu armés et l'aide de ces hacktivistes leur est plus que nécessaire. Néanmoins, ces hackers ne sont pas les seuls à intervenir pour former les opposants à Bachar Al-Assad : certains États s'emploient également à soutenir le soulèvement pro-démocratique.

1.2.2.3 Les dissidents syriens équipés et entraînés par certains États

1.2.2.3.1 L'exemple de Psiphon, un outil canadien financé par les Etats-Unis

---

[58] Source : http://youranonnews.tumblr.com/post/10622268842/every-major-city-in-syria-defaced

[59] Source : https://www.eff.org/

[60] Source : http://www.lemonde.fr/technologies/article/2012/05/03/les-utilisateurs-syriens-de-skype-de-nouveau-vises-par-un-logiciel-espion_1694880_651865.html

[61] Source : http://www.lemonde.fr/technologies/article/2012/03/15/un-faux-youtube-pour-pieger-les-activistes-syriens_1669410_651865.html

[62] Source : http://www.lemonde.fr/technologies/article/2012/03/30/les-opposants-syriens-vises-par-du-phishing-sur-les-reseaux-sociaux_1678017_651865.html

En novembre 2011, les dissidents syriens ont pu utiliser le logiciel canadien Psiphon afin de contourner la censure et la surveillance du gouvernement sur Internet. Cet outil permet de créer un réseau privé virtuel (VPN) entre l'ordinateur de l'internaute soumis à la censure et un serveur distant situé en « zone libre »[63]. Développé sous licence GPL et multiplateforme, l'outil serait indétectable. Après obtention d'un identifiant et d'un mot de passe, les échanges des internautes sont automatiquement chiffrés en utilisant le protocole SSL sur le port 443, normalement réservé aux transactions financières sécurisées sur Internet. Or, ce nouvel outil de contournement développé en 2006 au sein de Citizen Lab[64], le programme de recherche sur le cyberespace et les droits humains de l'Université de Toronto (Canada), a bénéficié de fonds en provenance du gouvernement américain.

1.2.2.3.2 Un fort engagement de la part des Etats-Unis

En effet, comme le relatent le Time Magazine[65] et Al Monitor[66], si l'État américain a déclaré ne pas soutenir activement les opposants syriens, l'administration Obama a tout de même mis en place à leur attention des programmes de formations en sécurité informatique, au travers notamment d'entités à but non lucratif comme l'Institute for War and Peace Reporting ou la Freedom House[67]. Ainsi, certains dissidents se sont rendus aux États-Unis afin d'y suivre des cours de chiffrement, de contournement de pare-feux gouvernementaux ou encore d'utilisation sécurisée de téléphones portables.

Outre ces différentes formations, les États-Unis travailleraient sur le développement d'un programme appelé *« Internet in the suitcase »* (ou Internet fantôme). Cet outil permettrait notamment d'effacer, grâce à *« un bouton magique »*, toutes les données et les contacts enregistrés dans un smartphone ; de faire apparaître un faux écran de téléphone lors de l'enregistrement d'un mauvais mot de passe ou encore, de flouter les visages des dissidents lors de la rediffusion en ligne des manifestations.

L'ensemble de ces technologies et de ces programmes de formations s'inscrit 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 du gouvernement. Cependant, suite aux manifestations iraniennes de 2009 et aux évènements du Printemps arabe de 2011, le Congrès américain a 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.

Les syriens sont, en somme, épaulés par différents acteurs : Etats, hacktivistes, diaspora et sympathisants s'engagent à leur fournir les moyens nécessaires au contournement de la censure et de la répression de Damas. Et cette aide est loin d'être superflue car seuls, les dissidents ne disposent que de peu de moyens et de compétences pour rivaliser avec les moyens colossaux mis en œuvre par le régime de Bachar Al-Assad.

---

[63] Source : http://www.lemonde.fr/technologies/article/2006/12/04/psiphon-le-briseur-de-censure-du-web_841832_651865.html
[64] Source : https://citizenlab.org/
[65] Source : http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/
[66] Source : http://www.al-monitor.com/pulse/security/01/06/americas-electronic-war-on-syria.html
[67] Source : http://www.al-monitor.com/pulse/security/01/06/americas-electronic-war-on-syria.html

1.3 Capacités et rôle de l'Etat syrien

1.3.1 Le contrôle des infrastructures : outils, technologies et limites

Le secteur des télécommunications en Syrie est l'un des plus réglementés et des moins développés de tout le Moyen-Orient[68]. Le gouvernement syrien possède cependant un atout majeur : le contrôle des infrastructures du réseau. Le principal opérateur mobile et fournisseur d'accès internet (FAI) syrien, l'Etablissement Syrien des Télécommunications (EST), est public. Il bénéficie d'un monopole sur les services Internet câblés et sans fil partout en Syrie[69]. Le second opérateur d'importance, Syriatel, est dirigé par le cousin du président Bachar Al-Assad. Les autres opérateurs comme MTN ou Aya, d'une taille plus modeste, sont plus ou moins directement sous contrôle du pouvoir central.

De façon générale, la Syrie n'est pas un pays très connecté. L'Internet n'a été proposé au grand public qu'à l'accession de Bachar Al-Assad en 2000 et le taux de pénétration atteignait péniblement les 16,8% en 2008. Un réseau 3G existe, mais les tarifs sont encore trop élevés pour permettre à la majorité de la population d'y avoir accès.

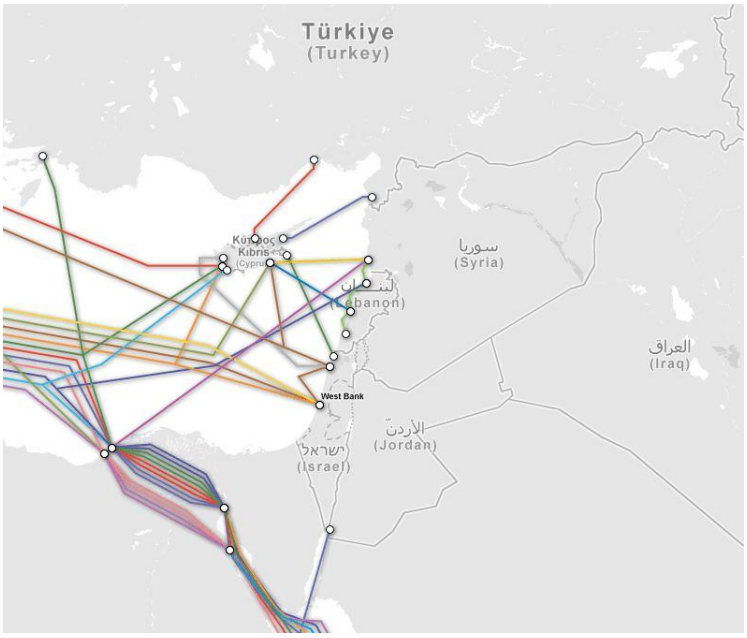


Figure 10. Câbles sous-marins dans la zone Moyen-Orient. La Syrie est reliée par 3 câbles arrivant à Tartous[70]

À l'instar du pouvoir égyptien qui avait coupé physiquement l'accès à Internet du pays, la Syrie a également usé de cette technique pour empêcher les insurgés de s'organiser et de communiquer, mais à une échelle plus locale. Les témoignages rapportent des coupures ponctuelles d'électricité, d'Internet et de téléphone, avec des retours à la normale lorsque la contestation dans la zone semble

[68] Source : http://www.budde.com.au/Research/Syria-Telecoms-Mobile-Broadband-and-Forecasts.html
[69] Rapport Open Net Initiative Syria, 2009
[70] Source : http://www.submarinecablemap.com/

s'atténuer[71]. Parmi les divers incidents relevés, citons : une interruption de plus de 40 jours entre mars et avril 2011 dans la ville de Dara ; presque deux mois dans la ville de Doma, de fin janvier 2012 à fin mars ; interruption du réseau 3G pendant une semaine dans toute la Syrie en juin 2012. Enfin, le réseau est régulièrement coupé le jeudi et le vendredi dans la province de Damas, ainsi que vers Homs, Hama et Alep[72], afin d'empêcher les manifestant de s'organiser[73].

1.3.2 Le contrôle de l'information et des images

« Qui ne sait dissimuler ne sait pas régner »
Louis XI

1.3.2.1 Une censure généralisée

L'information est un élément de pouvoir, par conséquent son contrôle est un enjeu central pour tous les gouvernements. Le cyberespace facilite la propagation des informations mais les problématiques de contrôle de l'information ne sont pas nouvelles, simplement démultipliées. Bachar Al-Assad semble avoir tiré les leçons des précédentes révolutions qui ont secouées le monde arabe. « *Parallèlement aux manifestations et à la répression, la situation en Syrie est en effet devenue l'objet d'une véritable guerre de l'information… et de la désinformation* »[74].

La Syrie possède une solide expérience en matière de censure : classé parmi les 13 pays ennemis de l'Internet en 2006 par Reporter sans frontières (RSF), le pays a été qualifié de plus grande prison du Moyen-Orient pour les cyberdissidents en 2007. Dans le rapport 2011/2012 de l'ONG, la Syrie est située au 176ème rang sur 179 pays classés : « *censure absolue, surveillance généralisée, violences aveugles et manipulations du régime ont rendu impossible le travail des journalistes* ».

1.3.2.2 Une censure légale

Jouant sur la proximité avec Israël et agitant la menace de l'islam radical, le pouvoir baasiste a édicté depuis longtemps une législation d'exception permettant d'institutionnaliser la surveillance des opposants. L'état d'urgence en vigueur depuis 1963 permet de suspendre la plupart des droits constitutionnels des Syriens[75] et de mettre en place un contrôle renforcé de la population. Parmi les autres dispositions fondant la censure, un décret datant de 1965 punit la diffusion de nouvelles visant à ébranler la confiance du peuple dans la révolution, un autre réprime « *l'opposition à la révolution, ses buts, ou au socialisme* »[76]. L'atteinte à *« l'unité nationale »* ou à la *« sécurité nationale »* est également sanctionnée et la presse s'est vue imposée un régime dérogatoire en 2001, mettant l'ensemble des médias sous le contrôle plus ou moins direct du pouvoir central. Ce dernier insiste auprès des agences de presse étrangères pour que leurs correspondants sur place

[71] Source : http://owni.fr/2011/06/07/la-syrie-coupure-net/
[72] Source : http://www.relaystationmedia.com/2012/06/social-media-and-the-arab-summer/
[73] Les manifestations ont en effet lieu le vendredi.
[74] Source : http://syrie.blog.lemonde.fr/2011/08/10/qui-tue-qui-aujourdhui-en-syrie/
[75] Source : http://www.state.gov/r/pa/ei/bgn/3580.htm
[76] Source : http://www.freedomhouse.org/report/freedom-press/2007/syria

soient syriens. La seule agence qui faisait exception, Reuters, a vu son dernier correspondant expulsé dès le début des manifestations. Ignace Leverrier, ancien diplomate, explique ainsi dans son blog[77] que « *le régime détient un monopole sur l'information intérieure (…) dont le contrôle est assuré par les services de renseignements* », les *Moukhabarat*.

1.3.2.3 L'investissement dans des capacités d'écoute

Cherchant à suivre les évolutions technologiques, la Syrie a développé une véritable capacité d'interception électronique au niveau national, comme la Libye de Kadhafi avait pu le faire en son temps. Cette capacité n'est donc pas une réponse à l'insurrection qui a lieu actuellement, mais constitue l'évolution logique d'un Etat qui verrouille depuis des décennies l'information circulant sur son territoire. Damas s'est ainsi montré particulièrement friand de technologies DPI (Deep Packet Inspection)[78], celles-là même qui avaient défrayé la chronique avec le matériel d'Amesys, filiale de Bull, en Libye.

1.3.2.3.1 Blue Coat

Les membres de Telecomix se sont, les premiers, penchés sur le dispositif de surveillance syrien. Ce groupe s'était déjà fait remarquer dans la dénonciation du rôle d'Amesys et de son système Eagle en Libye. Epaulé par des sites assez actifs (comme Reflets.info[79] et Fhimt.com[80]) qui ont rapidement relayé les résultats des investigations menées, Telecomix a diffusé 54 Go de données[81] prouvant la surveillance des communications électroniques syriennes par du matériel de la société américaine Blue Coat. Le graphique ci-dessous a été réalisé par Arturo Filastò[82] grâce aux données publiées par Telecomix, et illustre les différents types de contenus bloqués depuis la Syrie : publicités, réseaux sociaux, logiciels, contenus pour adultes, etc.

[77] Source : http://syrie.blog.lemonde.fr/2011/08/10/qui-tue-qui-aujourdhui-en-syrie/
[78] Source : http://www.monde-diplomatique.fr/2012/01/CHAMPAGNE/47183
[79] Source : http://reflets.info/la-censure-du-net-en-syrie-mise-a-nu/
[80] Source : http://www.fhimt.com/2011/08/11/opsyria-la-censure-du-net-en-syrie-mise-a-nu/
[81] Source : http://reflets.info/opsyria-syrian-censoship-log/
[82] Source : http://hellais.github.com/syria-censorship/

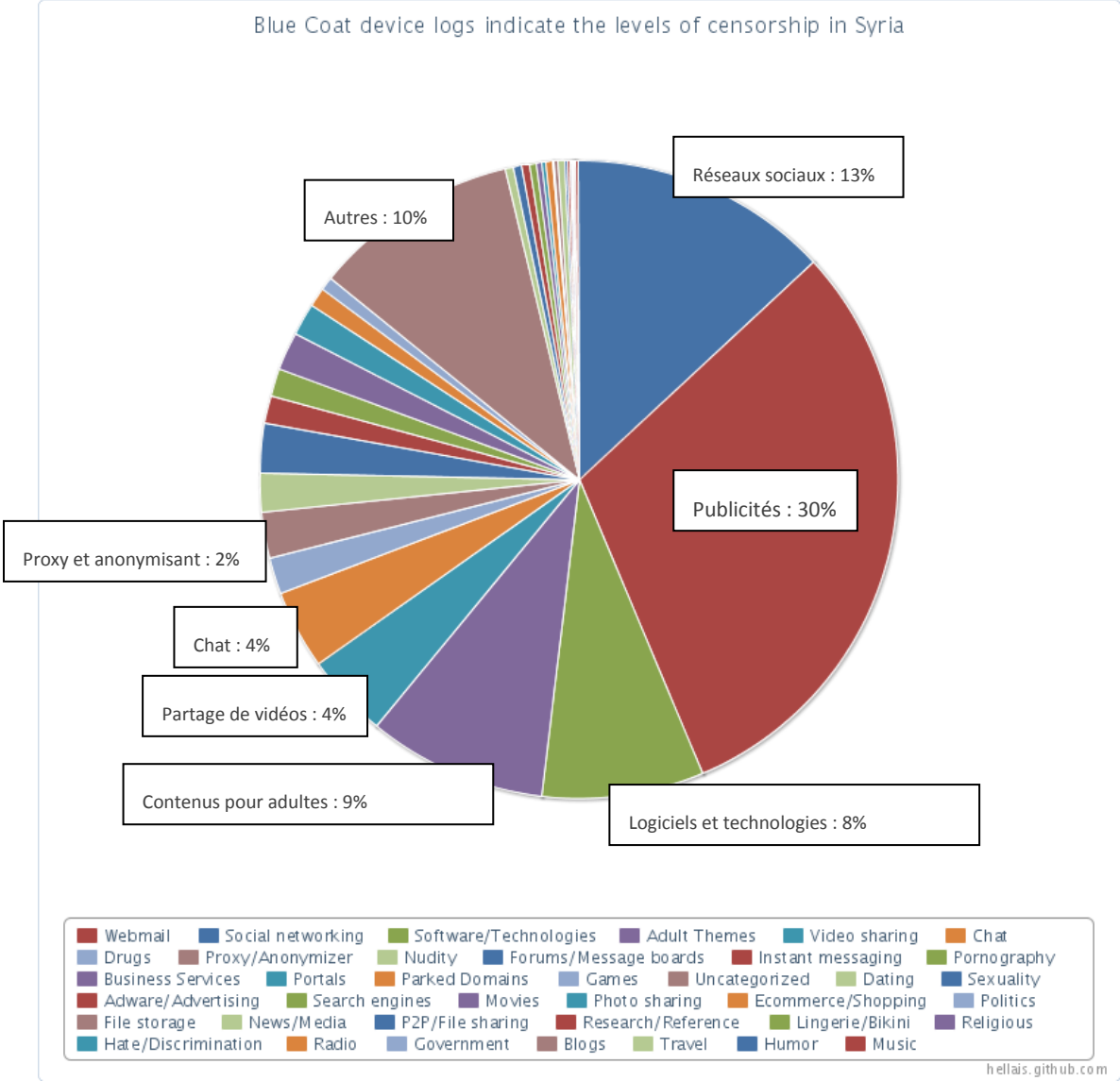


Figure 11. Analyse des contenus censurés par le matériel Blue Coat en Syrie[83]

La nouvelle a traversé l'Atlantique[84] [85] et Blue Coat a vivement démenti avoir vendu du matériel à la Syrie, ajoutant que ses produits n'étaient pas conçus pour surveiller les populations, mais pour filtrer certains contenus. La société n'a cependant pas exclu la possibilité que le régime se soit procuré du matériel via un tiers. En effet, les entreprises américaines n'ont pas le droit de vendre leurs produits à la Syrie depuis 2004, sauf autorisation spéciale de la part du *Commerce Department*. Les autorités américaines, et plus particulièrement le *Bureau of Industry and Security (BIS),* ont lancé une enquête afin de déterminer les raisons expliquant la présence de ces équipements en Syrie. D'après certains éléments, le matériel aurait d'abord transité par les Emirats Arabes Unis avant d'être expédié en

[83] Source : http://hellais.github.com/syria-censorship/

[84] Source : http://www.washingtonpost.com/world/national-security/syria-using-american-software-to-censor-internet-experts-say/2011/10/22/gIQA5mPr7L_story.html

[85] Source : http://www.washingtonpost.com/world/national-security/us-probes-use-of-surveillance-technology-in-syria/2011/11/17/gIQAS1iEVN_story.html

Syrie[86]. Le mal est fait pour les insurgés et les équipements de Blue Coat ont, selon le Wall Street Journal[87], filtré 750 millions de requêtes entre le 22 juillet et 6 août 2011 et bloqué 6% des connexions. Plus de 26 700 tentatives de connexion sur des sites de l'opposition ont été enregistrées par les forces de sécurité sur la même période.

1.3.2.3.2 D'autres sociétés sont également présentes

Le même scénario s'est reproduit avec les sociétés HP[88] et NetApp[89]. Plusieurs médias américains se sont fait l'écho de la présence de matériel fabriqué par les deux sociétés dans le dispositif de surveillance syrien, ce que les entreprises concernées se sont empressées de dénoncer. Il apparaît que les différents équipements ont transité via une société italienne, Area SpA, qui s'est chargée de l'installation du dispositif en envoyant des techniciens sur place. Du matériel de surveillance vendu par la société française Qosmos, ainsi que des produits d'Utimaco Safeware en provenance d'Allemagne auraient également été intégrés au système d'interception et de surveillance électronique. Intitulé « Asfador »[90], l'ensemble du projet est évalué à presque 18 millions de dollars selon certaines sources. Une enquête a été ouverte par le BIS sur le rôle de NetApp dans la constitution de ce système. Aucune autre indication n'est publiquement disponible, si ce n'est que l'entreprise a vanté sa coopération avec les autorités[91]. La société Qosmos a, de son côté, publié un communiqué dans lequel elle précise que son rôle s'est limité à fournir une *« brique technologique »* à la société italienne, ajoutant qu'elle n'a pas fourni les « *moyens techniques nécessaires à son fonctionnement* »[92].

Plusieurs autres systèmes de filtrage sont également évoqués çà et là, mais sans plus de détails : logiciel *Thundercache*[93] [94], matériel de la société allemande Fortinet[95], de la société suédoise Ericsson[96] ou de son voisin finlandais Nokia[97], voire *« d'entreprises irlandaises »*[98].

1.3.3 Le développement de capacités offensives

La constitution d'une force organisée est le trait principal différenciant la Syrie des régimes égyptien, libyen ou tunisien. La Tunisie était un pays avec un taux de pénétration d'Internet élevé et le régime n'a pas pu endiguer la contestation en ligne malgré ses efforts. En Egypte et en Libye, les populations étaient espionnées, mais il n'y avait pas de véritable contre-attaque étatique dans le cyberespace. Le pouvoir cherchait à déconnecter les insurgés et à les empêcher de communiquer et de s'organiser. La

---

[86] Source : http://www.bis.doc.gov/federal_register/rules/2011/76fr78146.pdf
[87] Source : http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html
[88] Source : http://www.bloomberg.com/news/2011-11-18/hewlett-packard-computers-underpin-syria-electonic-surveillance-project.html
[89] Source : http://www.sfgate.com/business/article/U-S-probes-NetApp-role-in-Syrian-surveillance-3588858.php
[90] Source : http://intelnews.org/2011/11/07/01-860/#more-7503
[91] Source : http://www.bloomberg.com/news/2012-06-20/netapp-reports-giving-u-s-information-in-syria-spy-gear-probe.html
[92] Source : http://www.qosmos.com/news-events/position-de-qosmos-sur-la-syrie-suite-aux-articles-de-presse-parus-r%C3%A9cemment
[93] Source : http://owni.fr/2011/06/07/la-syrie-coupure-net/
[94] Source : http://www.maxisciences.com/internet/qui-coupe-le-flux_art22073.html
[95] Source : http://www.itnews.com.au/News/277928,us-investigates-blue-coat-over-syria-filter-claims.aspx
[96] Source : http://www.lefigaro.fr/flash-actu/2012/06/25/97001-20120625FILWWW00491-syrie-fabius-veut-plus-de-sanctions.php
[97] Source : http://www.scancomark.se/05-08-2010-How-Nokia-technology-helps-syria-clamp-down-on-dissidents.html
[98] Source : http://www.francetv.fr/info/telecomix-des-hactivistes-au-secours-du-peuple-syrien_62941.html/

Syrie va plus loin et contrecarre les insurgés (et de leurs soutiens) en retournant leurs méthodes contre eux : hacking, attaques DDoS, etc.

Cet aspect offensif se retrouve dans la guerre de l'information que se livrent les deux camps. Par exemple, le régime encourage la création de pages Facebook d'informations qui relayent pratiquement les dépêches de l'agence SANA[99] : l'intox et la désinformation sont un moyen efficace de brouiller le discours des opposants[100]. Le régime envoie également ses supporters sur les divers réseaux sociaux et autres blogs noyer les commentaires négatifs sur le régime parmi un océan de commentaires positifs.

Les outils d'interception achetés à l'étranger sont utilisés dans le cadre d'une démarche active de recherche d'informations : le pouvoir ne se contente pas d'écouter en attendant qu'une information intéressante soit interceptée, mais pousse les dissidents à la faute et agit comme si le cyberespace était un terrain d'affrontement supplémentaire dans lequel il faudrait ramener l'ordre. Ces efforts se sont particulièrement accentués depuis le début de l'année 2012. Un grand nombre d'actions a été recensé depuis, et s'il est difficile d'en faire un inventaire exhaustif, voici un large panel des méthodes employées.

1.3.3.1 Méthodes et outils

1.3.3.1.1 Usage stratégique du blocage d'accès à certains sites

Comme dit précédemment, en février 2011, l'accès à Facebook et YouTube a été de nouveau autorisé, après plus de trois ans de blocage. Certains Syriens s'étaient alors réjouis de la nouvelle sur les réseaux sociaux[101]. Intervenant quelques semaines après les évènements en Egypte et en Tunisie, ce geste a été salué par le gouvernement américain[102] comme une *« décision positive »* dans la crise actuelle. Personne n'avait alors idée de l'ampleur du système de surveillance mis en place par Damas pour espionner les réseaux télécoms : l'ouverture contrôlée du web syrien est assurément une stratégie mûrement réfléchie par les autorités. Certains insurgés, prudents, ont continué à utiliser leurs logiciels de chiffrement, même après *« l'ouverture »* du Web syrien.

1.3.3.1.2 Attaques DDOS

Les attaques par déni de service distribué (DDOS) sont une méthode simple pour perturber le fonctionnement d'un site : on bombarde le serveur hébergeant ce dernier d'un très grand nombre de requêtes afin que celui-ci ne soit plus capable d'y répondre. Cette technique a été largement utilisée en Syrie, notamment par la Syrian Electronic Army, afin de faire pression sur certains sites prorévolutionnaires notamment.

---

[99] Agence de presse arabe syrienne - http://www.sana.sy/index_fra.html

[100] Source : http://syrie.blog.lemonde.fr/2011/08/10/qui-tue-qui-aujourdhui-en-syrie/

[101] Source : http://globalvoicesonline.org/2011/02/08/syria-facebook-and-youtube-unblocked-among-others/

[102] Source : http://abonnes.lemonde.fr/technologies/article/2011/02/09/les-syriens-reconnectes-a-facebook-et-youtube_1477641_651865.html

1.3.3.1.3 Trojans

Les trojans (ou chevaux de Troie) ont été très utilisés par les forces syriennes[103], afin de récupérer autant d'informations que possible sur les insurgés : mots de passe, documents, courriers électroniques, etc. Le logiciel Skype a été particulièrement utilisé comme vecteur pour disséminer des trojans[104]. Les victimes recevaient par exemple un message prétendument destiné à organiser la résistance dans la ville d'Alep, mais le fichier joint était malicieux[105]. D'autres témoignages rapportent l'existence de liens vers des *« logiciels anti-virus gratuits »,* qui mènent en réalité à des spywares[106]. Une attaque similaire a été recensée avec un faux outil de chiffrement de Skype[107]. Dans la majorité des cas, les logiciels malveillants envoient les données dérobées vers un nombre limité d'adresses IP, la plupart appartenant au gouvernement ou à la compagnie publique de télécommunications (EST).

1.3.3.1.4 Attaques Man-in-the-Middle

Facebook a également été la cible de nombreuses convoitises. Le réseau est international, son interface est simple et permet de partager facilement et rapidement des contenus. Son rôle, ainsi que celui d'autres réseaux sociaux comme Twitter, a sans doute été surestimé par certains observateurs, mais reste néanmoins indiscutable. Les internautes syriens ont été victimes d'attaques de niveaux variables : certaines étaient assez élémentaires, comme l'attaque *« man-in-the-middle »* [108]. Un pirate s'immisce dans la communication entre l'internaute et les serveurs de Facebook, afin d'intercepter les échanges de données. Mais ce détournement est facilement identifiable par les navigateurs Internet, qui émettent en général un message d'alerte.

1.3.3.1.5 Phishing

Les tentatives de phishing sont nombreuses : de fausses pages Facebook[109] ou Youtube[110] pullulent sur Internet, réclamant de manière irrégulière identifiant et mot de passe aux utilisateurs, et proposant parfois de fausses mise à jour d'Adobe Flash Player afin d'infecter leurs terminaux[111]. Ces attaques peuvent paraitre banales, mais pouvaient piéger un utilisateur trop peu vigilant. Les insurgés ont néanmoins été depuis très sensibilisés aux problématiques de sécurité et sont particulièrement méfiants.

1.3.3.1.6 Blocage de connexions

---

[103] Source : https://www.eff.org/deeplinks/2012/04/campaign-targeting-syrian-activists-escalates-with-new-surveillance-malware
[104] Source : http://blog.trendmicro.com/fake-skype-encryption-software-cloaks-darkcomet-trojan/
[105] Source : https://www.eff.org/deeplinks/2012/05/trojan-hidden-fake-revolutionary-documents-targets-syrian-activists
[106] Source : http://edition.cnn.com/2012/02/17/tech/web/computer-virus-syria/index.html
[107] Source : https://www.eff.org/deeplinks/2012/05/fake-skype-encryption-tool-targeted-syrian-activists-promises-security-delivers
[108] Source : http://blogs.voanews.com/digital-frontiers/2011/05/12/syrias-internet-hijack/
[109] Source : https://www.eff.org/deeplinks/2012/03/pro-syrian-government-hackers-target-syrian-activists-facebook-phishing-attack
[110] Source : http://www.guardian.co.uk/technology/2012/mar/20/syrian-activists-fake-youtube?newsfeed=true
[111] Source : https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware

Les forces de sécurité bloquent également les accès sécurisés à certains sites (voir le schéma ci-dessous publié sur le site Reflets.info[112]), forçant des connexions « classiques », non sécurisées et donc vulnérables à des interceptions.

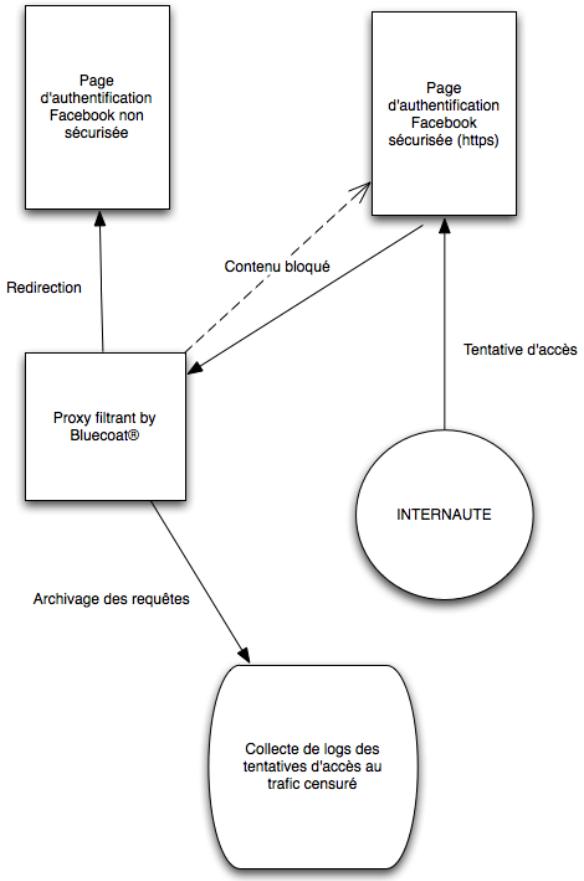


Figure 12. Schéma de blocage de l'accès aux pages web sécurisées

L'activiste Dlshad Othman rapporte des blocages du réseau TOR, ainsi que le blocage ponctuel des connexions SSL[113]. Les réseaux privés virtuels (VPN) ont également été ciblés. Certains soupçons, plus inquiétants, concernaient l'éventualité d'une surveillance des flux chiffrés en SSL par le matériel de Blue Coat : *« début août 2011, les BlueCoat syriens semblaient être en mesure de faire de l'interception sur les flux SSL »*[114]. Mais cette hypothèse soulève un problème de taille : « *pour être en mesure de décrypter le trafic SSL, les machines Bluecoat doivent être en possession de certificats SSL valides* ». Et les rédacteurs de Reflets d'élaborer l'hypothèse de l'utilisation de certificats compromis.

1.3.3.2 La Syrian Electronix Army

1.3.3.2.1 Rôle

[112] Source : http://reflets.info/opsyria-la-censure-du-net-syrien-en-pratique/
[113] Source : http://www.slideshare.net/DavidVyorst/the-internet-in-syria
[114] Source : http://reflets.info/opsyria-bluecoat-au-coeur-dattaque-mitm-de-grand-envergure/

Constituée autour du Syrian computer club[115], groupe présidé autrefois par Bachar Al-Assad lui-même, cette unité est apparue pour la première fois en avril 2011. Elle a été officiellement reconnue par le président Al-Assad comme une *« armée réelle dans une réalité virtuelle »*[116], même si la SEA nie tout lien direct avec une quelconque entité gouvernementale. Selon les informations disponibles, elle réunit des profils hétéroclites[117], du professionnel aguerri au conscrit doué en informatique, en passant par l'élève en école d'ingénieur. Il est pourtant difficile de savoir s'il s'agit d'une réelle unité organisée comme tel, ou une forme de groupe éphémère lançant des attaques coordonnées, à la manière des Anonymous. Un internaute, se présentant comme un des leaders de la SEA, et revendiquant le piratage d'Al-Arabiya, a répondu aux questions de Faisal J. Abbas, journaliste au Huffington Post. Il prétend dans cet entretien que *« l'armée électronique »* est composée de plusieurs milliers de personnes[118], même s'il y a de fortes probabilités pour que ce chiffre soit exagéré.

La SEA participe à la guerre d'informations en répandant la propagande pro-Assad sur le Web, y compris sur des pages Facebook occidentales (cf. la capture du site fhimt.com), ou en noyant Twitter sous un flot de contenus pro-gouvernementaux ou sans intérêt grâce à des bots[119]. Certaines pages proposent des phrases toutes faites en anglais, accusant par exemple les insurgés d'être des terroristes, prêtes à être postées sur des sites occidentaux[120].

[115] Source : http://edition.cnn.com/2011/11/22/world/meast/syria-cyberwar/index.html
[116] Source : http://www.sana.sy/eng/337/2011/06/21/353686.htm
[117] Source : http://blog.thepro.sy/
[118] Source : http://www.huffingtonpost.co.uk/faisal-abbas/exclusive-syrian-electron_b_1452425.html
[119] Source : http://www.guardian.co.uk/commentisfree/2011/apr/21/syria-twitter-spambots-pro-revolution
[120] Source : http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/

Figure 13. Capture d'écran de la page Facebook de Barack Obama[121]

[121] Source : http://www.fhimt.com/wp-content/uploads/2011/08/syrianelectronicarmy-obama.jpg

Figure 14. Capture d'écran de la page Facebook de Nicolas Sarkozy[122]

[122] Source : http://opennet.net/sites/opennet.net/files/SEArmy-Figure-11.png

Figure 15. Capture d'écran de la page Facebook d'ABC News[123]

La Free syrian Army mène également des opérations qui pourraient s'apparenter à une « guérilla » numérique : défacement de pages Web[124], infections d'ordinateurs d'opposants[125], piratage de compte Twitter (par exemple celui d'Al-Arabiya[126]), etc.

[123] Source : http://opennet.net/sites/opennet.net/files/SEArmy-Figure-14.png
[124] Source : http://www.infowar-monitor.net/2011/06/syrian-electronic-army-defaces-41-web-sites-one-uk-government-web-site/
[125] Source : http://threatpost.com/en_us/blogs/syrian-dissidents-hit-another-wave-targeted-attacks-062012
[126] Source : http://www.huffingtonpost.co.uk/faisal-abbas/syrian-electronic-army-de_b_1448517.html

1.3.3.2.2 Affrontements virtuels

Figure 16. Image issue du défaçage de 41 sites britanniques[127]

La SEA a ainsi eu maille à partir avec des hackers se revendiquant des Anonymous. Ces derniers s'en étaient pris au site du ministère de la Défense syrien, et l'armée électronique s'est alors vengée en défaçant un réseau social dédié aux Anonymous, « AnonPlus »[128] (voir image ci-dessous).

Figure 17. Image issue du défaçage du réseau « AnonPlus »

Des « escarmouches » ont également eu lieu sur des sites russes : la SEA ripostant à l'initiative des insurgés de commenter le soutien du Kremlin à Bachar Al-Assad[129].

---

[127] Source : http://www.infowar-monitor.net/wp-content/uploads/2011/06/3SEA1.png

[128] Source : https://www.computerworld.com/s/article/9218981/Syrian_hackers_retaliate_deface_Anonymous_social_network?taxonomyId=17

[129] Source : http://www.themoscowtimes.com/news/article/syria-cyber-war-opens-new-front-in-russia/452200.html

1.3.3.2.3 La diffusion d'outils de piratage « grand public » et la mobilisation de sympathisants

La SEA met à disposition des outils de piratage à destination de ses sympathisants ainsi que les modes d'emploi pour pirater un ordinateur[130] ou défacer un site[131]. Cette vidéo, disponible en arabe et en anglais, explique comment utiliser Shell, un script destiné à pénétrer des sites.

Figure 18. Tutoriel vidéo en arabe pour utiliser l'outil de piratage « Shell »[132]

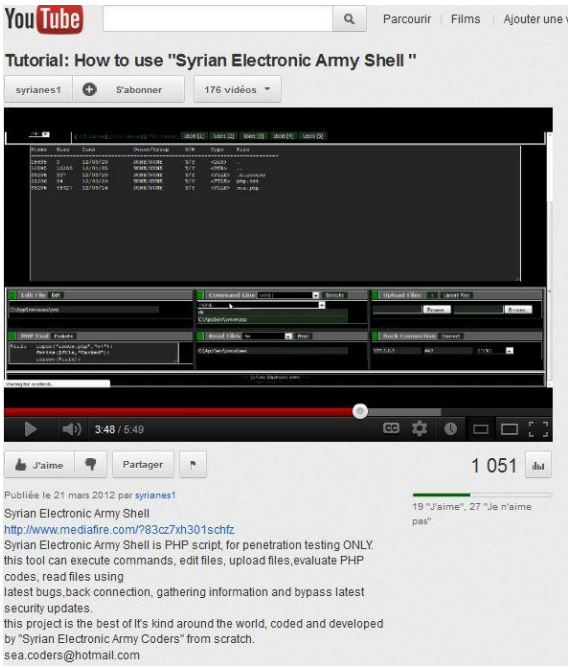


Figure 19. Tutoriel vidéo en anglais pour utiliser l'outil de piratage « Shell »[133]

Développée par « Syrian Electronic Army Coders », mais existant selon certaines sources depuis 2004[134], cet exemple est révélateur d'un mimétisme intéressant avec les pratiques des Anonymous :

---

[130] Source : http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/

[131] Source : http://www.youtube.com/watch?v=foD56TQbMEo&feature=relmfu

[132] Source : http://www.youtube.com/watch?v=foD56TQbMEo&feature=relmfu

[133] Source : http://www.youtube.com/watch?v=O8rnZo8oFaw&feature=relmfu

en effet, ces derniers s'étaient distingués lors de leurs dernières opérations en mettant à dispositions des non-initiés qui souhaitaient les soutenir un outil spécifique, le *Low Orbit Ion Cannon* ou *LOIC*. Celui-ci permet de mettre la machine sur lequel il était installé à disposition des Anonymous pour lancer des DDoS. L'utilisateur transformait en quelque sorte volontairement sa machine en « machine-zombie ». Le niveau d'automatisme n'est pas du tout équivalent, mais on retrouve la même intention de rendre possible pour un non-initié la participation à une activité de piratage à but politique.

Il est d'ailleurs question d'une « Syrian Hackers School » sur Internet[135]. Cette dernière vise à recruter des hackers et à les former à certaines attaques élémentaires, afin de maintenir une pression constante sur les ennemis de la Syrie. Là encore, des outils de DDoS sont mis à disposition, ces mêmes outils étant parfois détournés au profit de causes anti-gouvernementales (voir ci-dessous).

Figure 20. Outil de DDoS à destination des internautes pro-gouvernementaux[136]

Figure 21. Outil de DDoS à destination des internautes insurgés[137]

---

[134] Source : http://www.infowar-monitor.net/2011/06/syrian-electronic-army-defaces-41-web-sites-one-uk-government-web-site/

[135] Source : http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/

[136] Source : http://opennet.net/sites/opennet.net/files/SEADisruptiveAttacksFigure-11.png

1.3.4 Perspectives.

Le site Infowar-monitor.net a effectué une étude approfondie des attaques revendiquées par la SEA, l'année dernière, et en a tiré plusieurs conclusions[138]. Tout d'abord, le groupe semble privilégier la visibilité au détriment de l'efficacité. Certains des sites visés ne traitaient pas nécessairement de politique syrienne et il semble que les pirates aient exploité des failles qu'ils avaient à disposition plutôt que de chercher de nouvelles failles. Cela témoigne-t-il d'un choix stratégique ou d'un niveau technique insuffisant ? De plus, de nombreuses correspondances ont été observées entre des sites piratés par un groupe intitulé « Iranian Hackers » et ceux défacés quelques semaines plus tard, entre mai et juin 2011, par la SEA. Cela semble indiquer l'existence d'une collaboration entre certains groupes de hackers pro-syriens et pro-iraniens.

Cette « armée électronique » n'est pas pour autant à l'abri des défections. « Aleppo News Network », groupe réputé appartenir à la SEA, a annoncé en mars 2012 son soutien aux insurgés suite aux massacres ayant eu lieu dans la ville de Homs : « *nous apportons tout notre soutien aux personnes tentant de conserver leur dignité* »[139]. Cette annonce avait alors déclenché une avalanche de réactions sur les réseaux sociaux, même s'il était *in fine* impossible d'être sûr que cette désertion virtuelle n'était pas le fait d'un piratage de la part des opposants.

Si le cyberespace offre un moyen d'existence à la contestation syrienne, en lui permettant de contourner le rideau de fer électronique imposé par le pouvoir en place, il peut également être un piège. Le régime syrien a depuis longtemps saisit les enjeux du cyberespace, et les opposants doivent être particulièrement vigilants pour ne pas être identifiés en ligne. Même si les insurgés ont réussi quelques coups d'éclats, comme la diffusion de mails appartenant à la famille du président Al-Assad, la différence de moyens humains et techniques entre les camps se fait toujours sentir et le gouvernement ne reste pas passif face aux cyberdissidents.

1.4 Conclusion

1.4.1 Constat : l'Internet syrien, théâtre d'affrontement idéologique à l'échelle internationale

Les différents acteurs de la communauté internationale se positionnent et font de l'Internet syrien le théâtre d'une opposition idéologique, les partisans de la libre circulation des communications affrontant ceux du contrôle et de la maîtrise des informations.

---

[137] Source : http://opennet.net/sites/opennet.net/files/SEADisruptiveAttacksFigure-12.png

[138] Source : http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/

[139] Source : http://english.alarabiya.net/articles/2012/03/14/200652.html

1.4.1.1 L'encadrement de la vente de matériel de cybersurveillance.

Si c'est bien avec des équipements de Bluecoat que les dissidents syriens sont surveillés et contrôlés au quotidien, la firme américaine a toutefois souligné[140] qu'elle n'avait en aucun cas fournit ces produits à la Syrie. Le pays fait en effet l'objet d'un embargo[141] de la part des Etats-Unis. Si l'on associe à cet embargo les ambitions de *« diplomatie numérique »* des américains ou le programme *« No disconnect »* européen, il est fort probable que le marché de la cybersurveillance se retrouve, en partie au moins, délaissé par les entreprises occidentales.

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. Nous avons vu plus haut que les Etats-Unis ont annoncé l'adoption de mesures similaires. Une telle décision peut-elle constituer un frein au développement du marché de la cybersurveillance ?

Pas si sûr et, ce, pour de nombreuses raisons :

- Il est primordial pour les Etats occidentaux de rester leader dans ces technologies ;
- Les dictatures ne sont pas seules clientes de ce type de produit (comme en témoigne l'Ethiopie qui s'est récemment équipé d'un système DPI[142]) ;
- Les marchés intérieurs de la surveillance électronique, notamment américains, sont conséquents et vont sans doute soutenir le développement de ce type de produits ;
- Ces technologies sont, comme pour certaines armes, à « double-usage ». Les finalités de la technologie *Deep Packet Inspection* (DPI) sont variées : elle peut autant servir à espionner des dissidents qu'à proposer de la publicité comportementale sur le Web ou à empêcher le téléchargement de contenus illicites. Les débouchés pour ces technologies sont donc vastes, et ne se limitent pas à la surveillance pure et dure. Cela permettra de soutenir la croissance du secteur mais compliquera en revanche le contrôle de l'exportation, car il sera difficile de garantir le respect de la finalité initiale d'une technologie DPI « civile » une fois qu'elle aura quitté le territoire.

De ce fait, c'est un véritable marché « non-éthique » des technologies de cybersurveillance qui risque de se développer et sur lequel de nombreuses sociétés non soumises aux contraintes américaines et européennes, pourront se positionner. Les offres issues de pays du Sud et pays émergents sont en effet en plein essor. En décembre 2010, la Chine aurait, via la firme ZTE Corp. fourni au leader des télécommunications iranien TCI (Telecommunication Co. of Iran), un système de surveillance capable de filtrer et d'enregistrer les télécommunications de tout le pays[143]. Semptian, société fondée par des ex-responsables du géant Huawei, a également commencé par développer des solutions

[140] Source : http://www.zdnet.co.uk/blogs/security-bullet-in-10000166/blue-coat-web-filtering-technology-used-by-syria-10024276/
[141] Source : http://www.bis.doc.gov/licensing/exportingbasics.htm
[142] Source : https://blog.torproject.org/blog/ethiopia-introduces-deep-packet-inspection
[143] Source : http://articles.chicagotribune.com/2012-04-23/news/sns-rt-us-usa-technology-rightsbre83m05z-20120422_1_iran-and-syria-monitoring-landline-islamic-revolutionary-guard-corps

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[144].

Ainsi, force est de constater que l'interdiction en Europe et aux Etats-Unis de vendre des outils de surveillance de masse n'empêchera pas les Etats clients de s'équiper auprès de leurs alliés. De nombreux exemples sont, à cet égard, particulièrement explicites : citons le fait que ZTE Corp. fournisse du matériel à l'Iran, allié de la Syrie ou encore que l'Iran ait vraisemblablement formé le régime syrien aux techniques de cybersurveillance[145].

1.4.1.2 La transposition de la logique de soutien aux dissidents dans le cyberespace :

Les Etats partisans de la libre circulation des communications envisagent ensuite de s'investir plus directement dans le conflit **en équipant et en entrainant** les dissidents. Bachar Al-Assad va jusqu'à parler de *« complot occidental »*[146] contre l'Etat syrien, accusant certains pays occidentaux et arabes d'apporter *« en sous-main »*, leur soutien à la rébellion syrienne. Mais ces programmes de soutien permettent en fait de rééquilibrer les forces et les compétences en présence.

La Turquie, l'Arabie Saoudite et le Qatar ont par exemple été accusés de fournir un soutien logistique (connexion à Internet) et armé aux dissidents[147]. De leur côté, à l'aide de leur concept de *« diplomatie numérique »*, les Etats-Unis ont par exemple 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[148], *« la défense de la liberté d'Internet est* [déjà] *un dossier prioritaire de [la politique étrangère américaine] »*[149]. Comme vu précédemment, l'administration Obama soutient déjà activement ces technologies via des projets de téléphonie mobile[150] et d'Internet fantôme[151].

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 »*[152]. 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 ».* Les *« kits de survie sur*

---

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

[145] Source : http://www.mediapolicy.org/wp-content/uploads/Syria-Cyber-Wars-06-01-2012-proof2.pdf p.20

[146] Source : http://lci.tf1.fr/monde/moyen-orient/syrie-a-la-television-assad-se-pose-en-victime-du-complot-occidental-7392996.html

[147] Source : http://www.presse-dz.com/info-algerie/23215-apres-le-qatar-ryadh-pret-a-armer-l-opposition-syrienne.html

[148] Source : http://www.scribd.com/doc/48895078/Hillary-Rodham-Clinton-Feb-15-2011

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

[150] Source : http://www.lemonde.fr/international/article/2012/04/21/le-logiciel-de-telephonie-mobile-qui-defie-le-controle-des-etats_1688852_3210.html

[151] Source : https://code.commotionwireless.net/projects/commotion

[152] « 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

Internet » évoqués par Neelie Kroes ne sont donc pas sans rappeler les fameuses valises[153] *« Internet fantôme »* imaginées par les Etats-Unis.

1.4.1.3 La mise en œuvre de sanctions

Ces sanctions visent la dimension informatique du conflit, preuve qu'Internet est une des composantes principales du conflit syrien.

> *« These technologies should be in place to empower citizens, not to repress them »* (Barack Obama, discours au Musée mémorial de l'Holocauste, à Washington, avril 2012).

Dans un discours prononcé en avril dernier, à l'United States Holocaust Memorial, Obama a annoncé[154] la prise de sanctions contre ceux ayant aidé directement ou par fourniture de moyens la Syrie (et l'Iran) à traquer les dissidents. Selon le président américain, tout acteur leur fournissant une aide quelconque à cette fin pourrait être tenu coresponsable des violations aux droits de l'Homme qui en ont résulté.

Les mesures consisteront dans le gel des avoirs et la restriction de délivrance de visas et concerneront les individus, les sociétés ou les agences de sécurité aidant la Syrie (ou l'Iran) à surveiller l'ensemble des communications transitant par satellite, ordinateur ou téléphonie mobile. Sont pour l'instant visés par cette mesure[155] le Syrian General Intelligence Directorate, Syriatel, le Ministère iranien de l'intelligence et de la sécurité, le corps des Gardiens de la révolution islamique iranien, l'Iran's Law Enforcement Forces, ainsi que de nombreuses personnes physiques. Cette approche a toutefois été accueillie avec scepticisme[156], considérée comme trop souple à l'égard de la Syrie.

De son côté, la Russie a suspendu ses contrats avec la Syrie[157], précisant qu'il ne s'agirait là que d'un acte de prudence motivé par des raisons purement économiques, *« jusqu'à la normalisation de la situation dans ce pays »*[158]. Le pays qui se dit toutefois *« prêt à lâcher Bachar Al-Assad »*[159] en raison de la teneur des violences perpétrées, ne se positionne pas sur le plan numérique.

---

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

[154] Source : http://articles.chicagotribune.com/2012-04-23/news/sns-rt-us-usa-technology-rightsbre83m05z-20120422_1_iran-and-syria-monitoring-landline-islamic-revolutionary-guard-corps

[155] Executive order : « BLOCKING THE PROPERTY AND SUSPENDING ENTRY INTO THE UNITED STATES OF CERTAIN PERSONS WITH RESPECT TO GRAVE HUMAN RIGHTS ABUSES BY THE GOVERNMENTS OF IRAN AND SYRIA VIA INFORMATION TECHNOLOGY »
http://www.whitehouse.gov/the-press-office/2012/04/23/executive-order-blocking-property-and-suspending-entry-united-states-cer

[156] Source : http://articles.chicagotribune.com/2012-04-23/news/sns-rt-us-usa-technology-rightsbre83m05z-20120422_1_iran-and-syria-monitoring-landline-islamic-revolutionary-guard-corps

[157] Source : http://french.news.cn/dossiers/2012-03/03/c_131443895.htm

[158] Source : http://french.news.cn/dossiers/2012-03/03/c_131443895.htm

[159] Source : http://www.lefigaro.fr/international/2012/06/05/01003-20120605ARTFIG00665-la-russie-se-dit-prete-a-lacher-bachar-el-assad.php

1.4.2 Perspectives : une issue à géométrie variable

Si la supériorité technologique du gouvernement syrien est incontestable sur le terrain, force est de constater qu'à l'échelle internationale, Bachar Al-Assad a déjà perdu la « *guerre de communication* ». Mais les investissements massifs dans la maîtrise accrue de ses réseaux de télécommunication permettront tout de même à l'Etat syrien de renforcer ses capacités numériques jusque-là peu développées.

1.4.2.1 Le régime syrien perdrait la guerre de la communication, malgré sa supériorité technologique.

« *Le régime syrien va perdre (…) une bonne partie de la guerre de communication* » pouvait-on lire dans un article de la revue Moyen-Orient (n°12, octobre-décembre 2011). Un tel constat contraste avec l'ampleur des moyens mis en œuvre par le régime de Bachar Al-Assad pour contenir l'information et empêcher sa diffusion au reste du monde. Comme a pu le rappeler le blogueur Shakeeb al-Jabri, « *on ne gagne pas de guerre sans d'abord gagner la guerre des médias* ». Or, malgré la volonté affirmée de Bachar Al-Assad de tenir les médias internationaux à l'écart du pays et d'empêcher la diffusion de l'information, la communauté internationale est bel et bien mise au fait de ce qui se déroule actuellement. Et ce, malgré les importantes campagnes de désinformation engagées.

1.4.2.2 La Syrie prête à exister sur le plan numérique à l'échelle internationale ?

L'investissement massif dans des technologies confère à l'Etat syrien une maîtrise accrue de son réseau de télécommunications. Cet attrait pour les nouvelles technologies de l'information et de la communication est susceptible de s'élargir à la volonté de disposer de réelles capacités de lutte informatique défensive et offensive. D'autant plus que le conflit syrien a mis en lumière et fédéré nombre de partisans et sympathisants de Bachar Al-Assad ; ce qui, en cas de conflit à l'échelle internationale, pourrait constituer un vivier de « hackers patriotes » mobilisables sur simple demande.

Le taux de pénétration faible, qui constitue à première vue un handicap, pourrait être exploité comme avantage : un pays faiblement connecté étant moins vulnérable aux attaques qu'un pays qui, comme l'Estonie, s'appuie sur Internet pour la plupart de ses infrastructures.

La Syrie bénéficiera enfin de ses alliances déjà bien établies avec des puissances numériques plus ou moins importantes. Et si elle entame enfin un processus de développement de ses capacités « cyber », il sera sous l'influence d'Etats tels que l'Iran, la Chine ou la Russie, participant ainsi à l'affirmation d'une polarisation du cyberespace opposant d'une part, partisans de la libre circulation des communications et d'autre part, partisans d'un Internet maîtrisé, contrôlé.

2 Cyber-dissuasion ou dissuasion à l'ère du cyberespace ?

2.1 Introduction

Le débat sur la dissuasion dans le cyberespace soulève plusieurs questions :

- Une stratégie de dissuasion est-elle possible dans le cyberespace ? Ou plus précisément, peut-on empêcher un acteur d'utiliser des moyens informatiques offensifs en le persuadant que le bénéfice de son attaque sera inférieur au coût de celle-ci ? Au plan théorique, il n'y a pas de raison *a priori* pour que le cyberespace, environnement créé par l'Homme et à ce titre, théâtre d'affrontement et enjeu de puissance, à la fois reflet des tensions existant dans la vie réelle et objet de tensions à part entière, échappe à une telle posture. La dissuasion, rappelons-le, n'est pas née avec le nucléaire même si elle a pris une nouvelle dimension avec la crainte de l'holocauste atomique.

- Qu'entend-on alors par cyber dissuasion ? Comme souvent lorsque l'on évoque le cyberespace, deux réalités s'entremêlent : on confond l'environnement que constitue le cyberespace et les capacités qui permettent d'y agir, lesquelles peuvent être cybernétiques, c'est-à-dire propres au cyberespace, ou physiques. A partir de cette distinction, la cyber-dissuasion recouvre donc deux aspects :

    - Le fait de se prémunir contre les attaques informatiques, visant à la fois le cyberespace, mais également les environnements physiques, le cyberespace étant un environnement transverse susceptible de permettre l'accès aux environnements physiques ;

    - Le fait de se prémunir contre des attaques conventionnelles par la maîtrise que l'on pourrait avoir du cyberespace en tant qu'environnement, les capacités cybernétiques constituant à la fois un instrument de puissance à part entière et un multiplicateur de force applicable aux capacités matérielles.

Dans la pratique, comment mettre en œuvre ces deux facettes de la cyber-dissuasion ? Quelles en sont les limites ? Peut-on se contenter de transposer au cyberespace le concept de dissuasion hérité de l'ère nucléaire ? Faut-il réinventer un nouveau concept de dissuasion ?

2.2 De nombreux obstacles

Les caractéristiques propres du cyberespace, tant en termes d'environnement que de capacités d'action, génèrent en première analyse de nombreux obstacles à la mise en œuvre efficace d'une

stratégie de dissuasion, surtout si l'on se réfère à la dissuasion la plus efficace jamais observée, la dissuasion nucléaire.

2.2.1 Pas de destruction mutuelle assurée

La dissuasion repose notamment sur la certitude de dommages irréparables et irréversibles. Cette certitude est a priori difficile à obtenir dans le cyber. D'une part, les effets d'une attaque sont peu prévisibles. D'autre part, les effets n'ont clairement pas le caractère effrayant d'une attaque nucléaire. On peut également observer que des représailles informatiques ne permettent pas systématiquement de détruire la menace comme une attaque matérielle. Il s'agit en effet de suspendre les effets de l'attaque, à l'exception de certaines attaques sophistiquées atteignant le niveau physique (exemple : Stuxnet ou les attaques visant des systèmes SCADA). A défaut de « destruction massives », peut-on alors voir dans l'attaque informatique un risque de « perturbations massives » ? De nombreux experts considèrent que « la stabilité macroscopique *actuelle du réseau et des systèmes informatiques ne semble pas devoir être remise en cause »*[160]. Il est ainsi peu probable qu'une attaque puisse à elle seule provoquer l'effondrement d'internet, en raison de son maillage et de la redondance des équipements. En revanche, une attaque ciblant spécifiquement 5 % des nœuds à haute connectivité pourrait provoquer un effondrement de l'Internet en une série d'îlots, chacun interconnectant un maximum d'une centaine de calculateurs entre eux.[161]

2.2.2 Pas de réelle démonstration

Le « Pearl Harbor » informatique souvent annoncé n'a pas eu lieu. La cyber-dissuasion souffre donc d'une absence de démonstration, là où le nucléaire a connu Hiroshima et Nagasaki.

2.2.3 Des effets imprévisibles

Le cyberespace est une construction humaine. En conséquence, les lois de la physique ne s'y appliquent que partiellement (le rayon d'effet d'un virus est impossible à définir). Les effets sont donc largement imprévisibles. Si l'attaquant n'est pas certain de pouvoir atteindre ses objectifs, ni même de pouvoir sélectionner un type d'effet (« scalabilité » des effets), le défenseur aura également du mal à maîtriser les effets de sa riposte. A l'image des attaques chimiques, les risques d'effet boomerang sont en effet nombreux en raison du caractère maillé du cyberespace et de l'interdépendance des réseaux.

2.2.4 Une attribution complexe

L'attribution est généralement perçue comme l'obstacle majeur dans l'application d'une stratégie de dissuasion au cyberespace. Difficile, en effet, de dissuader un attaquant qui ne craint pas de riposte

---

[160] Source : Cyberdissuasion, Fondation pour la recherche stratégique, 2012.
http://www.frstrategie.org/barreFRS/publications/rd/2012/RD_201203.pdf

[161] Source : Future Global Shocks, OECD Review of Risk Management Policies, OECD, 2011.
http://www.oecd.org/dataoecd/24/36/48256382.pdf

puisqu'il est anonyme, ou plus exactement utilise une série de relais pour masquer son identité et origine réelles.

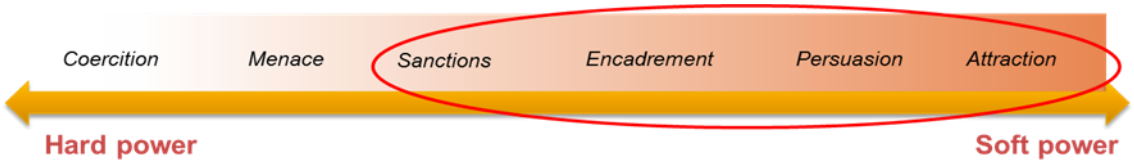
2.2.5 Comment dissuader un adversaire ne disposant pas des mêmes vulnérabilités ?

Contrairement à l'intimidation, une stratégie de dissuasion est généralement omnidirectionnelle. Or dans le cas du cyberespace, dont l'émergence a largement contribué à faire apparaître de nouveaux acteurs et à diluer partiellement la souveraineté étatique, la dissuasion apparait relativement inefficace à l'égard d'acteurs non étatiques ou d'Etats peu développés, aujourd'hui peu connectés et donc peu vulnérables. La cyber dissuasion sera donc plus efficace dans un contexte symétrique.

Par ailleurs, le cyberespace est par essence partagé entre une multiplicité d'acteurs, gouvernement, ONG, entreprises et particuliers (certains analystes parlent « d'empowerment » pour souligner le fait que des individus sont maintenant susceptibles de disposer de capacités identiques à celles des Etats), ce qui complexifie les choses.

2.2.6 Un faible degré de coercition

Pour qu'une dissuasion soit efficace, il faut que l'on puisse répéter la réponse en permanence. Ce n'est pas le cas pour la lutte informatique dans laquelle l'arme est souvent basée (à l'exception du déni de service) sur des vulnérabilités et est donc à usage unique. La cible peut rapidement corriger ses vulnérabilités, rendant la capacité inefficiente. Sans même se poser la question de savoir si les capacités d'attaques informatiques sont juridiquement assimilables à des armes, ne serait-ce que « par destination », on mesure que l'arme informatique est totalement incapable d'exercer une pression suffisante et répétée pour faire plier un adversaire résolu et le degré de coercition nécessaire, comme pourrait le faire un bombardement stratégique. Lorsqu'il est utilisé de façon autonome, le cyber est d'abord un instrument de « soft power ».



Echelle de la puissance[162]

2.2.7 Une transparence impossible

La dissuasion, telle qu'héritée de l'ère nucléaire, suppose une transparence complète sur les moyens offensifs développés et la chaîne de commandement. Or dans le cyberespace, le simple fait que les armes soit à usage unique, rend cette transparence impossible. Cette absence de communication constitue en première analyse un obstacle important car pour être dissuadé, l'attaquant potentiel

[162] Cyber Power, Joseph Nye. Source : http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf

doit non seulement savoir qu'il peut faire l'objet d'une riposte mais s'apercevoir rapidement qu'il a fait l'objet d'une attaque. La manœuvre de dissuasion exige par essence transparence et maîtrise de la communication.

2.2.8 Absence de seuil

Cette transparence doit notamment concerner des seuils au-delà desquels l'adversaire sait qu'il s'expose à une menace de riposte. Il ne peut y avoir de dissuasion sans seuil et sans échelle, qu'il s'agisse d'une échelle d'effets, de moyens utilisés ou d'adversaire.

Or dans le cyberespace, ces seuils apparaissent aujourd'hui inexistants et se révèlent techniquement et juridiquement difficiles à mettre en œuvre :

- D'un point de vue juridique et politique, il n'existe encore pas de normes communes définissant des règles de conduite ou des cibles légitimes et non légitimes. Un traité international qui régulerait le cyberespace au même titre que les autres « global commons » apparait même fortement hypothétique pour l'instant ;

- D'un point de vue technique, des seuils apparaissent compliqués à établir compte tenu de l'imprévisibilité des effets et de la nature même des cyber-armes qui sont à usage dual. « *Il manque une catégorisation de la puissance des armes numériques pour que la dialectique soit pleinement efficace. Dans ce cas, il est probable que les plus puissantes devraient être qualifiées de non emploi, si l'on est cohérent avec la logique de dissuasion…* »[163].

2.2.9 Une temporalité différente

Les attaques informatiques peuvent se dérouler sur plusieurs mois, voire plusieurs années. Dans ces conditions, planifier une riposte informatique est complexe. Alors qu'une attaque conventionnelle laisse en général la possibilité à la cible de détecter avec un préavis minimal l'attaque, l'attaque informatique est en outre à première vue nettement plus difficile à anticiper. Même si une attaque est précédée d'activités de reconnaissance, cela ne donne pas forcément beaucoup de précisions utiles.

2.2.10 Un dialogue dissuasif impossible

« *L'invisibilité des agents (et de leurs effets dans de nombreux cas) rend peu crédible l'idée d'une escalade maîtrisée dans laquelle les intentions des protagonistes sont clairement compréhensibles* »[164]. En l'absence de « téléphone rouge » entre les parties, le dialogue dissuasif est donc complexe, voire impossible.

---

[163] Source : http://alliancegeostrategique.org/2011/12/27/cyberdissuasion-ou-cyber-dans-la-dissuasion/

[164] Source : Cyberdissuasion, Fondation pour la recherche stratégique, 2012.
http://www.frstrategie.org/barreFRS/publications/rd/2012/RD_201203.pdf

2.2.11 « On ne lance pas une pierre quand on est dans une maison de verre »

« *On ne lance pas une pierre quand on est dans une maison* de verre », affirme un proverbe chinois. La question est en effet de savoir si des pays disposant des capacités cybernétiques nécessaires seraient prêts à « ouvrir la boîte de pandore » et à s'exposer alors mêmes qu'ils apparaissent comme les plus vulnérables à des attaques informatiques ?

Au-delà des vulnérabilités techniques, les pays occidentaux auraient également sans doute quelques difficultés politiques et juridiques à s'engager dans une attaque informatique. On observe d'ailleurs que les Etats-Unis auraient à plusieurs reprises préparé des attaques informatiques en support d'opérations militaires conventionnelles (Irak en 2003, Libye en 2011) sans toutefois les engager, en raison de craintes d'effet boomerang mais également de craintes quant à l'acceptabilité politique de ce type d'attaque et au fait que cela aurait pu générer à terme des restrictions internes quant à la possibilité pour l'exécutif d'engager ce type d'action sans l'aval du Congrès[165].

2.3 Des obstacles sans doute surévalués

Paradoxalement, dans la pratique, un certain nombre de ces obstacles peuvent être levés ce qui fait dire à certain que « la cyber-dissuasion est plus difficile en théorie qu'en pratique »[166]. Par ailleurs, ce n'est pas parce que le modèle de dissuasion nucléaire ne peut pas être transposé au cyberespace que toute stratégie de dissuasion est vouée à l'échec dans le cyberespace ou par des moyens cybernétiques.

2.3.1 Dépasser l'attribution

Si l'anonymat régnant aujourd'hui dans le cyberespace est un obstacle important, il est souvent surévalué. Les attaques laissent finalement beaucoup de traces, celles-ci étant souvent sous-utilisées. A ce propos, l'émergence des technologies « big data » devraient jouer un rôle positif. Les technologies de traçabilité progressent. Par ailleurs, il est fort probable que sous la pression des usages, le cyberespace de demain soit en moins en partie beaucoup moins anonyme qu'aujourd'hui.

Si l'attribution de l'attaquant est difficile, compte tenu du fait qu'il peut se masquer derrière une fausse identité et qu'il peut s'agir d'un individu ou d'une organisation non structurée, le pays qui tolèrerait l'utilisation d'infrastructures basées sur son territoire pourrait voir sa responsabilité mise

---

[165] Source : http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=1

[166] Will Goodman "Cyber Deterrence: Tougher in Theory than in Practice?," 2 which appeared in the Fall 2010 issue of *Strategy Studies Quarterly. On exagère les obstacles. http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf*

en cause, qu'il s'agisse d'une complicité active ou passive. Un projet d'articles sur les actes internationaux illicites a ainsi été proposé à l'ONU en 2001.

Les attaques de grande ampleur qui dépasseraient les attaques de basse intensité connues aujourd'hui seraient revendiquées par l'attaquant. Elles surviendraient par ailleurs dans le cadre de tensions préalables qui donneraient de forts indices au pays attaqué.

L'affaire estonienne montre que « l'assignation » d'une responsabilité en raison d'indices concordants et d'un contexte de tension donné peut compenser la difficulté d'attribution formelle.

L'attaquant ne peut donc être certain de ne pas être identifié, ce qui concourt en soi à une forme de dissuasion basée sur l'ambiguïté. En revanche, il est fort probable que l'identification prenne un peu de temps et que la riposte ne puisse pas être immédiate.

2.3.2 L'incertitude sur les effets peut jouer un rôle dissuasif

En matière informatique, l'incertitude des effets peut jouer un rôle dissuasif, un acteur hésitant à s'engager dans une action offensive en l'absence de certitude que son attaque peut réussir. Cette incertitude des effets doit se doubler d'une incertitude sur les capacités de l'adversaire à riposter.

2.3.3 Des démonstrations limitées sont possibles

En l'absence de « Pearl Harbor » numérique, des démonstrations limitées de capacités offensives sont possibles, à la condition toutefois qu'elles ne révèlent pas trop d'information.

Plusieurs exemples :

- Israël a laissé à plusieurs reprises fuiter des informations sur ses capacités de guerre électronique et informatique, en particulier à la suite de l'opération Orchard contre la Syrie ;

- Même si au départ les fuites d'information ne sont pas forcément volontaires, les affaires Stuxnet et Flame révèlent les capacités développées par les Etats-Unis et Israël, ce qui contribue à la crédibilisation des capacités de ces deux pays et, dans le cas de Stuxnet, à la crédibilisation des moyens cybernétiques pour agir dans le réel. On peut d'ailleurs imaginer que les révélations récentes sur l'opération Olympic Game et le fait que Stuxnet ait été une coproduction américano-israélienne ont été *a minima* tolérées par les autorités américaines.

Les exercices d'attaque informatique ou de gestion de crise constituent enfin un moyen intéressant de démontrer ses capacités et son état de préparation.

2.3.4 Les acteurs non étatiques sont également susceptibles de faire l'objet de stratégies de dissuasion

Même s'ils sont plus difficile à atteindre, les acteurs non étatiques peuvent faire l'objet de stratégies directes et indirectes mettant en œuvre des moyens variés, pas forcément cybernétiques (influence, moyens judiciaires etc.).

2.3.5 Les contextes d'affrontement numériques seront de plus en plus symétriques

S'il est exact que la cyber-dissuasion soit plus efficace à l'égard d'acteurs disposant de vulnérabilités similaires, on observe que de plus en plus de pays sont aujourd'hui « connectés » et donc vulnérables à terme compte tenu du très rapide développement du cyberespace et de son changement total de centre de gravité[167]. La Chine compte aujourd'hui le double d'internautes que les Etats-Unis (500 contre 250 millions) avec un taux de pénétration de 40 %. Autre exemple : seuls 13 % de la population africaine est connectée mais ce retard se comble rapidement. La connectivité a ainsi progressé de 300 % depuis 2009. La forte asymétrie dont bénéficiait certains pays, et notamment la Chine ou la Russie, face aux Etats-Unis a donc diminué, rendant ces pays plus vulnérables à des attaques informatiques.

2.4 Une dissuasion *sui generis*

A la lumière des éléments précédents, on mesure que la démarche dissuasive dans le cyberespace, si elle est possible, ne peut se construire uniquement *sui generis*, par référence à des démarches existantes. Si le principe de dissuasion est susceptible de s'appliquer partiellement au cyberespace, l'émergence du cyberespace est également susceptible d'avoir un impact sur le concept de dissuasion. Celui-ci, qui a été au cœur des relations internationales pendant la guerre froide, doit donc évoluer, puisqu'il reste une composante essentielle d'une stratégie de puissance, laquelle englobe nécessairement le cyberespace.

2.4.1 Une dissuasion ambigüe

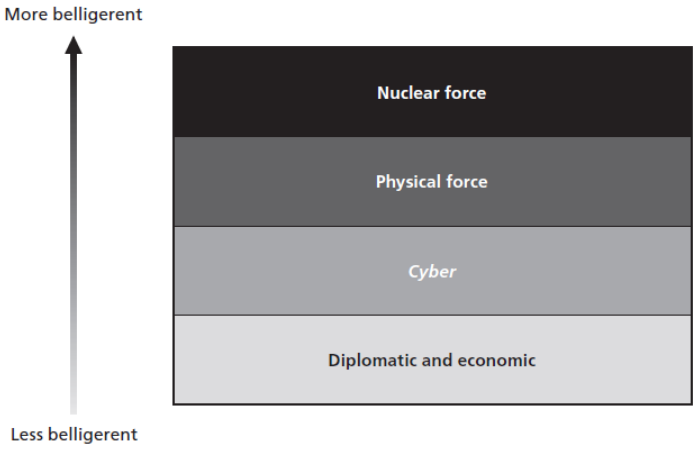
Alors que la transparence était de mise à l'ère nucléaire, l'opacité et l'ambiguïté doivent être privilégiées dans le cyberespace. On peut ainsi parler de dissuasion « floue ». Par ailleurs, la perception tend à l'emporter sur la réalité. Au-delà des capacités mises en place et de la volonté politique de les utiliser, c'est avant tout la perception qu'en ont les adversaires qui est importante.

2.4.2 Une dissuasion transverse à l'ensemble des domaines

La riposte ne doit pas nécessairement avoir lieu dans le même domaine et peut donc utiliser des moyens divers. Plus le contexte sera asymétrique (un Etat contre une nébuleuse hacker par exemple), plus la riposte devra être asymétrique pour être efficace. De la même façon que les conflits sont globaux et qu'un conflit majeur strictement limité au cyberespace apparait improbable,

[167] Ce changement de centre de gravité est facilement perceptible en regardant cette animation : *http://www.conceptualdevices.com/ENG/Human%20World/Internet_Users_Animation.html*

la dissuasion doit s'appréhender dans la globalité. La doctrine américaine a construit pour ce faire l'acronyme DIME (Diplomatie, Information, Militaire, Economique) devenu plus tard DIMEFIL (Finance, *Intelligence, Law Enforcement*).



Types de capacité[168]

Pour être efficace, la dissuasion doit également mettre en œuvre à la fois stratégies directes et indirectes ainsi que des outils de « hard power » et de « soft power ». Alors que le nucléaire était à la fois une arme de destruction massive et une arme psychologique, le cyber est en effet essentiellement une arme psychologique et une arme de perturbation à utiliser en combinaison avec des capacités conventionnelles. D'où l'émergence du concept de *smart power* américain qui combine à la fois « hard power » et « soft power ». Cette dissuasion globale doit enfin être accompagnée de l'élaboration d'une norme commune fixant une échelle pour maîtriser tout risque d'escalade.

2.4.3 Une dissuasion à la fois défensive et offensive

Toute dissuasion repose sur deux facteurs : la peur que l'attaque que l'on envisage ne soit pas efficace et que le ratio coût/efficacité ne soit pas au rendez-vous (dissuasion défensive), la peur que cette attaque donne lieu à des représailles qui viendraient anéantir le bénéfice attendu de l'attaque.

La dissuasion dans le cyberespace est d'abord défensive. Elle consiste à faire savoir à l'adversaire que l'on dispose de moyens de défense passifs et actifs permettant l'adaptation en temps réel des réseaux à la menace (détournement de flux, analyse forensique…) de nature à l'empêcher d'atteindre ses objectifs. La résilience des réseaux, grâce notamment à la redondance de certains équipements stratégiques et à leur diversité génétique, est également un élément dissuasif important.

[168]Cyberdeterrence and cyberwar, Martin Libicki, Rand Corporation, 2008. Source : http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf

Il semble que cette dissuasion défensive joue un rôle plus important dans le cyberesapce que dans le nucléaire où les défenses sont vues comme des éléments de déstabilisation potentielle et sont même limités par traités (dissuasion par empêchement). En l'absence de textes sur le contrôle des armements cyber (demandés par la Russie dès 1998 avec la résolution 53/70), la course technologique est au cœur de la dissuasion défensive. Pour les Etats-Unis, le maintien d'un gap technologique est ainsi capital.

La dissuasion offensive est également essentielle dans le cyberespace. Comme dans le nucléaire, la riposte doit être techniquement faisable et crédible, ce qui suppose *a minima* des démonstrations, même limitées, dans le cadre d'une stratégie de communication par l'ambiguïté.

2.4.4 Un cadre juridique à construire

A l'image du cadre juridique qui s'est rapidement mis en place dans le nucléaire, une dissuasion efficace dans le cyberespace passe obligatoirement à terme par l'établissement d'un traité international régissant le cyberespace comme un « global common ». L'approche technique et technologique ne suffit pas. Comme l'indiquait Bruce Held du Département américain de l'Energie, New York n'a pas été sauvée des bombardements soviétiques par des abris antiatomiques mais par l'outil diplomatique au service de la dissuasion[169]… Cette norme commune décrirait les comportements légitimes et illégitimes, fixerait une typologie d'attaques (en fonction de leurs effets plus des moyens mis en œuvre) permettant de disposer d'une échelle et préciserait ce qui relève de la souveraineté des Etats et ce qui appartient à tous (système DNS par exemple).

Si un tel texte apparait souhaitable pour améliorer la stabilité du cyberespace, il semble fortement hypothétique aujourd'hui compte tenu de l'opposition des Etats-Unis. La puissance dominante dans le cyberespace entend en effet d'abord mettre en place des capacités, asseoir sa domination et forger une norme qui lui soit favorable. Le pays plaide donc d'abord pour une approche « law enforcement » et un renforcement de la coopération internationale en matière de lutte contre la cybercriminalité.

Une riposte asymétrique, c'est-à-dire dans un autre environnement et/ou avec d'autres types de capacités, à l'image de la récente prise de position américaine selon laquelle le pays serait susceptible d'utiliser son arsenal nucléaire face à une attaque informatique visant ses infrastructures critiques, apparait en effet complexe à la lumière du droit international actuel. Pour qu'une telle asymétrie soit possible, il faudrait :

- Soit baisser de quelques crans le niveau d'intensité requis pour l'exercice de la légitime défense en droit des conflits. Une telle diminution apparait peu souhaitable : cela risquerait d'augmenter le risque d'escalade, tout en supprimant pour les Etats un espace

[169] Source : http://www.wired.com/dangerroom/2010/07/how-to-stop-cyberattacks-diplomacy-well-maybe/

d'affrontement de basse intensité agissant comme une sorte de soupape de sécurité dans les relations internationales

- Soit créer une nouvelle forme d'agression. Cela sous-entend du même coup qu'il y a un vide juridique dans le cyberespace, ce qui n'est pas vrai. Il s'agit plus de clarifier les règles et de rassembler des éléments épars.

Une autre évolution juridique serait intéressante : la possibilité de mettre en cause la responsabilité d'un Etat qui aurait non seulement organisé, sponsorisé ou facilité une attaque informatique, mais également toléré une telle attaque depuis son territoire. Un projet d'article sur les actes internationaux illicites a été présenté en ce sens à l'ONU en 2001. Un tel texte serait assez dissuasif face à des paradis numériques et réglerait le problème de l'attribution en privilégiant un mécanisme d'assignation.

2.5 L'exemple de la doctrine américaine

Avec l'émergence de nouveaux acteurs nucléaires, les Etats-Unis reconnaissent que la modèle de dissuasion héritée de la guerre froide n'est plus totalement adaptée. « *Nous faisons face à des formes émergentes de combat – terrorisme transnational, guerre informatique, combat spatial, pour lesquelles nous n'avons que peu d'expérience de la dissuasion. Nous avons besoins de réfléchir attentivement à comment la dissuasion s'applique ou pas à ces menaces. Nous avons besoin de modeler notre stratégie de dissuasion et les capacités associées en fonction. Je crois que la dissuasion joue un rôle critique dans ces menaces* » (Vice Amiral Carl V. Mauney, commandant adjoint, US Stratcom).

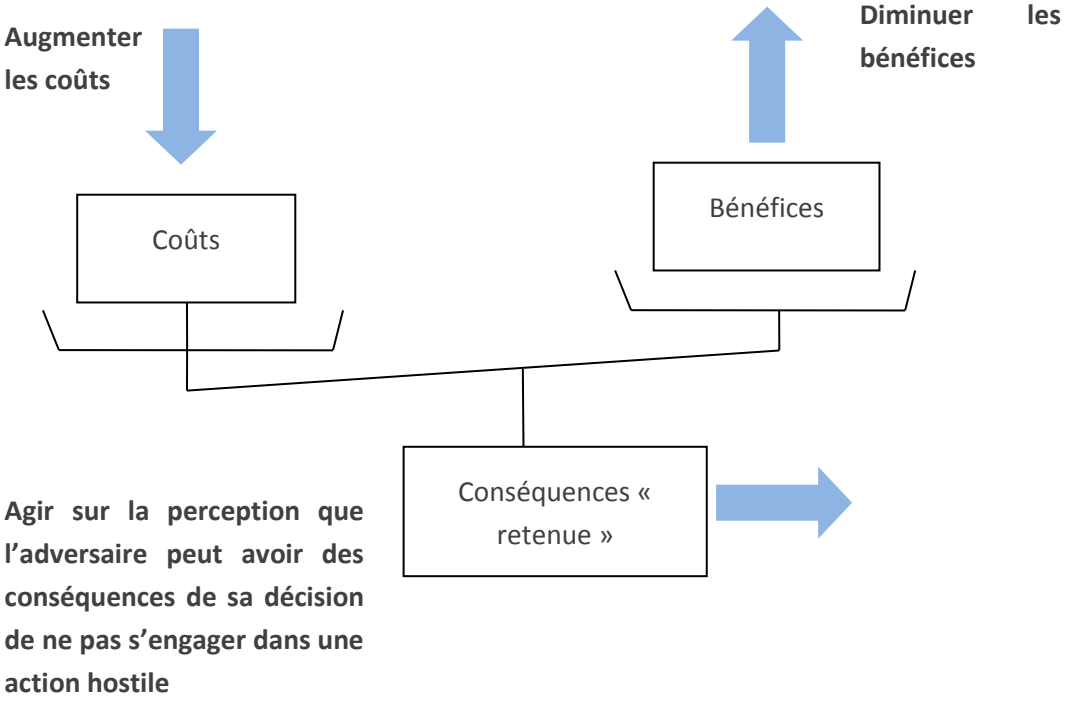
2.5.1 Le cyber au service de la dissuasion globale

Dès 2006, la doctrine de dissuasion américaine[170] intègre les capacités cybernétiques comme un outil au service d'une capacité de dissuasion plus globale, tout en reconnaissant que certains acteurs seront plus difficiles à dissuader que d'autres. Priorité est donnée aux acteurs rationnels et à une dissuasion défensive basée sur le doute de l'adversaire quant à l'efficacité de son attaque et de ses bénéfices. Le document admet toutefois la possibilité de *« conduire des opérations de combat dans le cyberespace comme le sabotage (par exemple la manipulation de données financières) de systèmes associés avec les activités d'acquisition d'armes de destruction massive et empêcher leur utilisation des tierces parties ».*

De façon générale, selon la doctrine américaine, les opérations militaires combinées contribuent à l'objectif de dissuasion en affectant le processus de décision de l'adversaire sur 3 variables :

[170] Deterrence Operation Joint Operating Concept 2.0 de 2006.

- Les coûts,
- Les bénéfices,
- L'analyse que l'on fait de la balance entre les 2.



Dans une étude très détaillée, le major Kevin R. Beeker de l'US Air Force[171], explique comment une dissuasion équilibrée est possible dans le cyberespace en agissant sur ces trois variables pour faire en sorte que les coûts soient nettement supérieurs aux bénéfices. La dimension psychologique qui consiste à agir sur la perception que l'adversaire a de ces propres intérêts apparait très importante. Cette capacité de dissuasion est donc globale, tant dans les effets recherchés, que dans les moyens mis en œuvre.

Objectif	Effets	Moyens
Imposer des coûts	Escalade dans la réponse à une attaque	Posture déclaratoire : le cyberespace fait partie des infrastructures sensibles et on se réserve le droit de répondre à une attaque informatique par des

[171] Strategic Deterrence in cyberspace : practical application, Kevin R. Beeker, USAF, Air University, juin 2009. Source : http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA502250

		moyens cyber et non cyber
	Maintenir l'infrastructure ennemie en risque	Entretenir ses compétences et la connaissance du réseau adverse, s'entrainer à la réalisation d'une attaque (exercices). Lui interdire des « ports » de repli.
	Développer une coalition internationale	Renforcer les normes internationales, condamner les comportements non voulus, « ostraciser » les adversaires.
Empêcher les bénéfices	Détection et préemption dès la phase de préparation d'une attaque	Efficacité relative dans le cas d'une attaque informatique émanant d'un Etat nation.
	L'attaque ne procurera pas un avantage suffisant pour défaire les forces américaines	Capacité à intervenir dans un environnement contesté (cf. capacité à intervenir dans un environnement chimique)
	Défense active perçue comme très efficace	Infrastructures robustes, techniques d'obfuscation, possibilité de riposte
	Réseaux d'information perçus comme très robustes	Entraînement, sécurité des systèmes d'information, Identity Access management
Encourager la retenue	Certaines cibles ne peuvent pas être attaquées	Consensus international sur les cibles légitimes dans le cyberespace
	Incitation	Déconnecter les utilisateurs abusant de la confiance
	Aider l'adversaire en matière de « situational awareness »	« Situational Awareness » partagé. Définition de ce qui est acceptable en termes de Computer Network Exploitation (espionnage)
	Les Etats-Unis sont considérés comme un	Influencer l'adversaire dans sa planification militaire. Agir sur ses

	objectif limité	capacités

2.5.2 Une dissuasion collective…

A l'image du modèle de défense collective hérité de la guerre froide, les Etats-Unis ne conçoivent cette nouvelle dissuasion globale intégrant le cyberespace que dans une optique collective. L'objectif est de construire une sorte de parapluie cybernétique permettant d'une part de disposer d'un système d'alerte avancée et d'autre part de façonner la vision que le reste du monde a du cyberespace grâce à des normes de conduite basées sur la vision américaine.

Pour parvenir à cet objectif, de nombreux programmes de « diplomatie numérique » ont été mis en place par le Département d'Etat, dans la lignée des discours d'Hillary Clinton sur la liberté numérique. On peut notamment citer : le programme Commotion Wireless visant à développer une solution technique permettant de se connecter depuis un pays coupé du monde (montant de la subvention : 2 millions de $) ou le programme baptisé « TechWomen » visant à organiser, en partenariat avec la Silicon Valley, la formation de spécialistes du numérique issus notamment des pays du Moyen-Orient et d'Afrique. Au total, ce serait 150 millions de $ qui auraient été consacrés à ces initiatives de diplomatie numérique ces deux dernières années.

Cette posture collective apparait clairement dans deux documents stratégiques récents :

- La stratégie internationale de la Maison Blanche pour le cyberespace (International Strategy for Cyberspace) publiée en 2011[172]. Extraits : « *La réduction des risques sur une échelle globale suppose une capacité d'application de la loi, des normes internationales communes de comportement, des mesures qui créent la confiance et renforcent l'autonomie, une diplomatie active et informé et une dissuasion appropriée. (…) Les Etats Unis s'assureront que les risques associés avec les attaques informatiques ou l'exploitation de nos réseaux dépasseront largement les bénéfices potentiels. Nous reconnaissons pleinement que les activités dans le cyberespace peuvent avoir des effets dépassant les réseaux. De tels événements nécessitent des réponses en termes de légitime défense. De la même façon que les réseaux interconnectés rendent les Nations interdépendantes, ainsi une attaque contre le réseau d'une nation peut avoir un impact largement au-delà de ses frontières.* »

- La stratégie du DoD dans le cyberespace (DoD strategy for operating in cyberspace[173]) publiée en juillet 2011. Extrait : « *le développement de capacités internationales d'alerte et de situational awareness permettra une légitime défense collective et une dissuasion collective. En partageant des indicateurs pertinents sur les événements cyber, les signatures de code malicieux et des informations sur les acteurs et menaces émergents, les alliés et les*

[172]Source : http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

[173]Source : http://www.defense.gov/news/d20110714cyber.pdf

partenaires internationaux peuvent développer une cyberdéfense collective. Le cyberespace est un réseau de réseaux qui inclut des milliers de fournisseurs d'accès dans le monde. Aucun Etat ou organisation peut seul maintenir une cyber défense efficace ».

2.5.3 …Soutenue par une vision bien comprise de leurs intérêts

Au-delà des considérations idéologiques, les Etats-Unis voient évidemment un triple intérêt à promouvoir internet dans le monde entier :

- Les vulnérabilités des challengers (Chine et, dans une moindre mesure, Russie) progressent, ainsi que celles des pays émergents, ce qui a pour effet de rendre ces pays accessibles pour les capacités numériques ;

- Le développement du cyberespace et la globalisation qu'il génère et soutient tout à la fois, rendent les économies interdépendantes, ce qui crée une forme d'auto-dissuasion. Pourquoi la Chine[174] irait-elle attaquer les Etats-Unis si elle possède une large part de la dette américaine ? C'est la théorie du « too big to fail » ;

- En amenant leurs adversaires sur ce terrain, ils peuvent exploiter le gap technologique qui les sépare de leurs adversaires, à la condition toutefois de maintenir et de développer leur suprématie (d'où la nouvelle Initiative de Défense Stratégique) qui est engagée avec le cyber.

2.6 Conclusion

Plus que de cyber-dissuasion, il faut parler d'une « dissuasion à l'ère cyber » ou d'une contribution du « cyber » à une posture de dissuasion globale. Au plan stratégique, le cyberespace ne peut définitivement pas être appréhendé de façon autonome. Il est de plus imbriqué dans le réel et devient indissociable des environnements physiques dans lesquels il se fond. Il faut donc réinventer une doctrine de dissuasion, qui, compte tenu de la dimension transverse et globalisante du cyberespace, englobe l'ensemble des domaines ainsi que des moyens « soft » et « hard » dans une stratégie de « smart power ». L'objectif est de « combiner les outils de l'intimidation et les outils de l'inspiration », affirmait John Hamre, ancien secrétaire adjoint à la défense.

Cette nouvelle dissuasion nécessitera cependant un traité international. Comme le soulignaient Stéphane Dossé et Olivier Hubac[175] : « *deux stratégies globales sont envisageables : un traité mondial*

[174] Cette stratégie de dissuasion se heurte au scepticisme chinois. C'est ce que révèle un article du China Defense Dail (source : http://www.chinanews.com/gj/2012/01-09/3590771.shtml). Malgré tous les avantages que ces experts reconnaissent aux Etats-Unis (maîtrise de 10 des 13 serveurs racine, suprématie technologique…), non sans une certaine exagération, le pays est perçu comme incapable de sécuriser ses réseaux, impuissant à mettre en œuvre des capacités de détection précoce.

[175] Source : http://www.cesat.terre.defense.gouv.fr/IMG/pdf/Cahiers_25.pdf

de désarmement prônant le principe de neutralité et d'inviolabilité de certaines parties du cyberespace, définissant ce qui est de l'ordre de la souveraineté des États ou non, ou la mise en place de doctrines de cyberdissuasion conjointement à une adaptation du droit de la guerre. Comme dans le domaine nucléaire, la seconde permettrait d'assurer un équilibre stratégique dans le cyberespace, en attendant que la première puisse être un jour effective. Ceci reprend le principe décrit dans Le Prince de Machiavel: là où il n'y a point de bonnes armes, il ne peut y avoir de bonnes lois, […] au contraire il y a de bonnes lois là où il y a de bonnes armes ».