



CEIS

« NOUVELLES GUERRES DE L'INFORMATION » : LE CAS DE LA SYRIE

Céline Pigot

et

Alexandre Durand

Consultants

Les notes  stratégiques

Novembre 2012

Les notes stratégiques



Les notes stratégiques
Policy Papers – Research Papers

« NOUVELLES GUERRES DE L'INFORMATION » : LE CAS DE LA SYRIE

Par
Céline Pigot
et **Alexandre Durand**,
consultants

Avec la contribution de :

Charles Ibrahim
Robin Beaumont,
analystes

Sous la direction de :
Barbara Louis-Sidney
blouis@ceis.eu



CEIS est une société de conseil en stratégie et en management des risques, structurée autour de quatre pôles de compétences. Notre vocation est d'assister nos clients dans leur développement en France et à l'international et de contribuer à la protection de leurs intérêts. Pour cela, nous associons systématiquement vision prospective et approche opérationnelle, maîtrise des informations utiles à la décision et accompagnement dans l'action. Riches d'expertises variées, nos 80 consultants interviennent dans les secteurs de l'énergie, de la défense et sécurité, du transport et de la logistique, des industries de transformation, de l'agro-alimentaire, de la finance et des services, en France et à l'étranger.

Veille, études, conseils, accompagnement stratégique : retrouvez nos offres et nos compétences sur

www.ceis.eu

Les idées et opinions exprimées dans ce document n'engagent que les auteurs et ne reflètent pas nécessairement la position de la Société CEIS.

SOMMAIRE DE LA NOTE

I. Une forte asymétrie dans les forces en présence.....	6
A. Internet, fenêtre sur le monde pour les dissidents	6
o <i>Une utilisation atypique des réseaux sociaux.....</i>	6
o <i>Témoigner à tout prix : une logique de diffusion de l'information.....</i>	7
B. Les capacités accrues de l'Etat syrien dans la guerre de l'information	10
o <i>Le contrôle des infrastructures.....</i>	10
o <i>Le contrôle de l'information et des images.....</i>	12
o <i>Le développement de capacités offensives.....</i>	14
II. Le rôle des intervenants extérieurs au cœur du conflit syrien - vers un rééquilibrage des forces en présence ?	19
A. L'intervention des acteurs extérieurs au conflit comme contrepoids face aux capacités de l'Etat syrien.....	20
o <i>L'apport de la diaspora syrienne.....</i>	20
o <i>Des hackers engagés aux côtés des dissidents.....</i>	21
o <i>L'intervention accrue de certains Etats.....</i>	22
B. Des soutiens extérieurs pourtant controversés.....	27
o <i>Un soutien étatique occidental jusque-là cantonné au cyberspace.....</i>	27
o <i>La remise en cause de la légitimité et de l'efficacité des soutiens étatiques occidentaux.</i>	28
Conclusion : guerre de l'information syrienne, quelle issue ?.....	31

Nouvelles guerres de l'information: le cas de la Syrie

Le conflit syrien, qui dure à présent 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 el-Assad, et d'un autre côté Bachar el-Assad lui-même qui, refusant de quitter son poste, met tout en œuvre pour enrayer et écraser la rébellion.

Dans cet affrontement, dissidents et autorités syriennes se sont emparés d'Internet à des fins radicalement opposées : alors que les premiers cherchent à alerter et mobiliser l'opinion publique internationale, les seconds tentent de museler l'opposition tant dans la rue que sur la Toile.

Toutefois, les deux forces en présence ne s'affrontent pas à armes égales. Le gouvernement syrien, fort des leçons tirées du Printemps arabe, dispose d'outils de cybersurveillance importants, d'une force de coercition et d'une maîtrise accrue de ses réseaux. En face, les dissidents tentent, parfois en amateurs, de déjouer ce système afin d'atteindre leurs objectifs. Se dessine alors une véritable guerre contre, pour et par l'information, de nature incontestablement asymétrique¹.

Mais c'est sans compter sur les intervenants extérieurs qui, en se positionnant comme soutiens aux forces en présence, pèsent de tout leur poids sur l'équilibre de l'affrontement. Le conflit syrien est, à cet égard, symptomatique d'une intervention accrue d'acteurs divers et variés, désirant aider et soutenir des parties prenantes à un conflit, principalement dans le cyberspace.

► Quelles sont les capacités et rôles des acteurs du conflit syrien en matière de guerre de l'information ? Comment se traduisent les interventions d'acteurs extérieurs ? Ces interventions sont-elles susceptibles de rééquilibrer les capacités des forces en présence ? Quelle est l'étendue de leur efficacité et de leur légitimité auprès des cyberactivistes syriens eux-mêmes ? Comment mesurer l'importance d'Internet et de la guerre de l'information, dans un conflit connaissant une telle escalade de violence ?

¹ Déjà en 2003 en effet, Sophia Clément-Noguier qualifiait cette « guerre de l'information » comme menace par nature asymétrique (cf. « SÉCURITÉ DU FORT CONTRE ASYMÉTRIE DU FAIBLE », Armand Colin, Revue internationale et stratégique.)

I. Une forte asymétrie dans les forces en présence

« On ne gagne pas de guerre sans d'abord gagner la guerre des médias »²

A. Internet, fenêtre sur le monde pour les dissidents

Comme le montre le nombre d'arrestations de blogueurs et cyberactivistes, les liens entre le cyberspace 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. 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, les opposants au régime n'ont cependant pas eu tout à fait le même usage des réseaux sociaux que leurs voisins. Se distinguent en effet deux temps dans la crise syrienne. Le premier, « le temps de la manifestation »³, s'est caractérisé par des soulèvements révolutionnaires et des manifestations plus ou moins pacifiques. Internet a été un instrument d'organisation, il a permis le mimétisme entre manifestants. Le second temps, celui de l'insurrection armée et militarisée, a vu le rôle d'Internet évoluer et s'amoindrir sur le terrain. Dans cette phase de répression sanglante, Internet a joué un rôle majeur au sein d'une véritable guerre de l'information entre dissidents et gouvernement syriens.

o Une utilisation atypique des réseaux sociaux

Selon le blogueur syrien Shakeeb Al-Jabri, la Syrie serait « *complètement dépendante des médias sociaux* »⁴. 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 dissidents⁵, les réseaux sociaux n'ont pas été utilisés comme en Egypte ou en

² Shakeeb al-Jabri (blogueur syrien exilé à Beyrouth, Liban), au Figaro - <http://www.lefigaro.fr/international/2012/06/18/01003-20120618ARTFIG00820-en-syrie-la-guerre-passe-aussi-par-les-images.php>

³ Entretien accordé à CEIS par Jean-Baptiste Beauchard, le 30 août 2012.

⁴ Source : <http://www.courrierinternational.com/article/2012/01/25/sans-internet-la-revolution-aurait-ete-immediatement-ecrasee>

⁵ Voir infra

Tunisie. Après trois années de censure, la Syrie n'a par exemple autorisé l'accès à Facebook qu'en février 2011. Alors que certains dissidents, ainsi que la communauté internationale⁶, avaient salué cette ouverture qui intervenait peu de temps après le début des manifestations égyptiennes⁷, il est de plus apparu très vite que le gouvernement syrien avait mis en place un important système de surveillance du réseau social. Les appels au rassemblement rapidement diffusés sur Facebook n'ont, de ce fait, pas reçu l'écho escompté en Syrie. Ce sont la Commission Générale de la Révolution Syrienne (CGRS) ainsi que les Comités Locaux de Coordination (CLC) qui ont joué le rôle de fédérateurs et d'organiseurs de manifestations⁸.

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 événements et de leur répression.

- *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 (...)* »⁹. C'est pourquoi le faible taux de pénétration syrien n'est pas un obstacle à cette démarche. Les syriens ne sont pas les seuls 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 el-Assad* »¹⁰. Pour ce faire, les opposants au régime se sont emparés du

⁶ Voir infra

⁷ Source : <http://globalvoicesonline.org/2011/02/08/syria-facebook-and-youtube-unblocked-among-others/>

⁸ Source : http://www.letemps.ch/Page/Uuid/71333062-a5db-11e1-9fa9-143c3f93e20d/Divis%C3%A9e_lopposition_syrienne_cherche_sa_strat%C3%A9gie ;

http://www.lemonde.fr/idees/article/2012/08/08/comment-s-organise-l-opposition-interieure-en-syrie_1743592_3232.html

⁹ Source : <http://obsession.nouvelobs.com/high-tech/20120312.OBS3577/jasmine-cyber-dissidente-syrienne-et-prix-rsf-sans-internet-nous-mourrions-en-silence.html>

¹⁰ Source : <http://obsession.nouvelobs.com/high-tech/20120312.OBS3577/jasmine-cyber-dissidente-syrienne-et-prix-rsf-sans-internet-nous-mourrions-en-silence.html>

Web : depuis les blogs^{11 12}, Twitter¹³, Youtube¹⁴ ou encore Facebook^{15 16 17 18 19}, 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.

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 coordination²⁰, chacun pourvu d'un Centre des médias. Ces Centres des médias fonctionnent comme une agence de presse proposant à ses visiteurs un flux RSS, compilant témoignages, images et vidéos. Dotés d'ordinateurs portables, de clés 3G, de clés USB ou encore de smartphones²¹, les contributeurs de ces cellules rassemblent 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.

De la même manière, d'autres formations reprennent et diffusent sur les réseaux sociaux des vidéos des manifestations et des exactions commises par le régime. A l'instar de la Commission générale de la révolution syrienne (CGRS), mouvance majoritaire en Syrie avec 150 coordinations locales, ou encore des Frères musulmans²², ces organisations possèdent des bureaux médiatiques, en charge de l'information des médias internationaux sur la situation dans le pays.

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 communiquer entre eux²³, tandis que d'autres, situés aux frontières du pays, utilisent des serveurs libanais ou turques.

¹¹ Source : <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.

¹² Source : <http://7urreya.wordpress.com/tag/english-post/>

¹³ Source : <http://twitter.com/#!/RevolutionSyria>

¹⁴ Source : <http://www.youtube.com/watch?v=SPd3yCclE1U>

¹⁵ Source : <http://ar-ar.facebook.com/ShaaamNews>

¹⁶ Source : <http://ar-ar.facebook.com/UgaritNEWS>

¹⁷ Source : <http://ar-ar.facebook.com/syria.news.F.N.N>

¹⁸ Source : <http://www.facebook.com/pages/Syrian-Revolution-News-Round-ups/108855819196476>

¹⁹ Source : <https://www.facebook.com/SuriyeDevrimi?ref=ts>

²⁰ Local Coordination Committees of Syria, LCCSyria, <http://www.lccsyria.org/>

²¹ Source : <http://owni.fr/2012/03/08/syrie-liberation-freedom-4566-turquie/>

²² Source : http://www.lemonde.fr/idees/article/2012/08/08/comment-s-organise-l-opposition-interieure-en-syrie_1743592_3232.html

²³ Source : <http://www.france24.com/fr/20120215-syrie-internet-homs-pigeons-voyageurs>

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.

En mars 2012, plus de 3 000 mails²⁴ échangés entre Bachar el-Assad et sa femme ont été interceptés par des dissidents syriens qui avaient mis sous surveillance leurs boîtes 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 internationale²⁵.

Mais ce sont les procédés techniques utilisés par les dissidents syriens qu'il faut ici retenir. En effet, les mails n'ont pas été obtenus pas un piratage « *hautement élaboré* »²⁶, mais parce que les dissidents étaient en possession des adresses et mots de passes divulgués par un sympathisant travaillant au ministère de l'Intérieur syrien. Quelques mois plus tard, en juillet 2012, le site Wikileaks publie à son tour près de 2,5 millions de mails « *en provenance de personnalités politiques syriennes, de ministères et d'entreprises* »²⁷. Ces fuites remettent à nouveau en cause les autorités syriennes mais aussi les liens qu'elles entretiennent avec certaines compagnies étrangères, notamment accusées de fournir des logiciels de surveillance.

Aussi cette affaire souligne-t-elle l'un des aspects essentiels des capacités des cyberdissidents syriens : ils ne disposent que de très peu de marge de manœuvre sur Internet ; et sont très peu familiers de l'informatique et, plus particulièrement des techniques permettant de se protéger et de contourner efficacement les mesures de censure sur le réseau.

Dès lors, pour communiquer, les dissidents s'appuient sur des soutiens extérieurs, souvent mieux formés et disposant d'une plus grande marge de manœuvre sur Internet. Objectif : faire face aux importants moyens engagés par l'Etat syrien sur le champ numérique.

²⁴ Source : <http://www.arte.tv/fr/6536018,CmC=6536372.html>

²⁵ Source : <http://www.guardian.co.uk/world/middle-east-live/2012/mar/15/syria-assad-emails-aftermath-live#block-18>

²⁶ 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

²⁷ Source : http://www.liberation.fr/monde/2012/07/05/wikileaks-devoile-des-millions-de-mails-sur-la-syrie_831427

B. Les capacités accrues de l'Etat syrien dans la guerre de l'information

« Le fort imite les techniques du faible. Mais le fort reste le fort. »²⁸

Le développement d'internet et des réseaux sociaux a profondément modifié le rapport des gouvernements, notamment dans les régimes autoritaires, avec les forces d'opposition. Dans le Printemps arabe, ces régimes se sont révélés incapables de comprendre le phénomène et ont été rapidement débordés par le passage du virtuel au réel qui s'est opéré dans les communautés. Malgré la censure, la surveillance ou la propagande, les gouvernements n'ont pas pu empêcher des « communautés à lien faible », qui se retrouvent autour de sujets initialement apolitiques, de devenir des communautés militantes²⁹.

Avec le conflit syrien, la donne a changé. Les dictateurs ont probablement tiré des leçons des déboires de leurs homologues, renversés lors du Printemps arabe. Le régime syrien a ainsi développé une riposte s'articulant autour de trois piliers imbriqués :

- La maîtrise du « contenant », c'est-à-dire les infrastructures ;
- La maîtrise du « contenu » (informations et images) ;
- L'animation d'un vivier de partisans pouvant déployer des capacités offensives dans le cyberspace.

○ *Le contrôle des infrastructures*

Le secteur des télécommunications en Syrie est l'un des plus réglementés et des moins développés de tout le Moyen-Orient³⁰. Le gouvernement syrien possède cependant un atout majeur : le contrôle des infrastructures du réseau. Le principal opérateur mobile et fournisseur d'accès à 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 Syrie³¹. Le second opérateur majeur, Syriatel, est dirigé par le cousin du président Bachar el-Assad. Les autres opérateurs

²⁸ François-Bernard Huygue, docteur d'État en Sciences Politiques et chercheur à l'IRIS.

²⁹ Entretien accordé à CEIS par François-Bernard Huygue, docteur d'État en Sciences Politiques et chercheur à l'IRIS, le 04 septembre 2012.

³⁰ Source : <http://www.budde.com.au/Research/Syria-Telecoms-Mobile-Broadband-and-Forecasts.html>

³¹ Rapport Open Net Initiative Syria, 2009

comme MTN ou Aya, d'une taille plus modeste, sont plus ou moins directement sous contrôle du pouvoir central.

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 s'atténuer³². Parmi les divers incidents relevés, citons : une interruption d'Internet 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 Alep³³, afin d'empêcher les manifestant de s'organiser³⁴ une fois sur place.

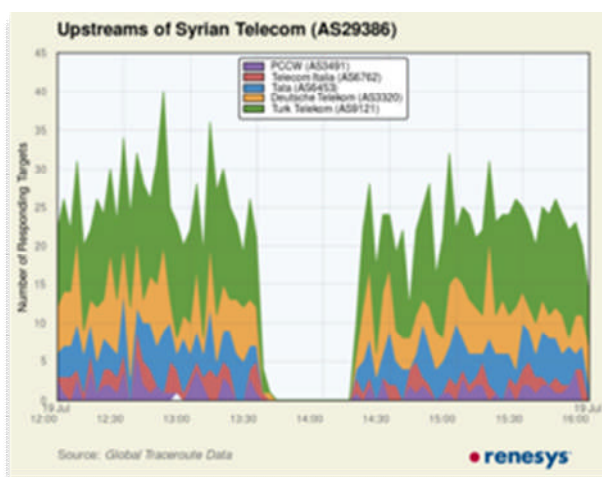


Figure 1. Une coupure de réseau en Syrie, le 19 juillet 2012

Le contrôle des réseaux est également facilité par le faible nombre des routes de télécommunication vers l'extérieur du pays.

³² Source : <http://owni.fr/2011/06/07/la-syrie-coupe-net/>

³³ Source : <http://www.relaystationmedia.com/2012/06/social-media-and-the-arab-summer/>

³⁴ Les manifestations ont en effet lieu le vendredi.

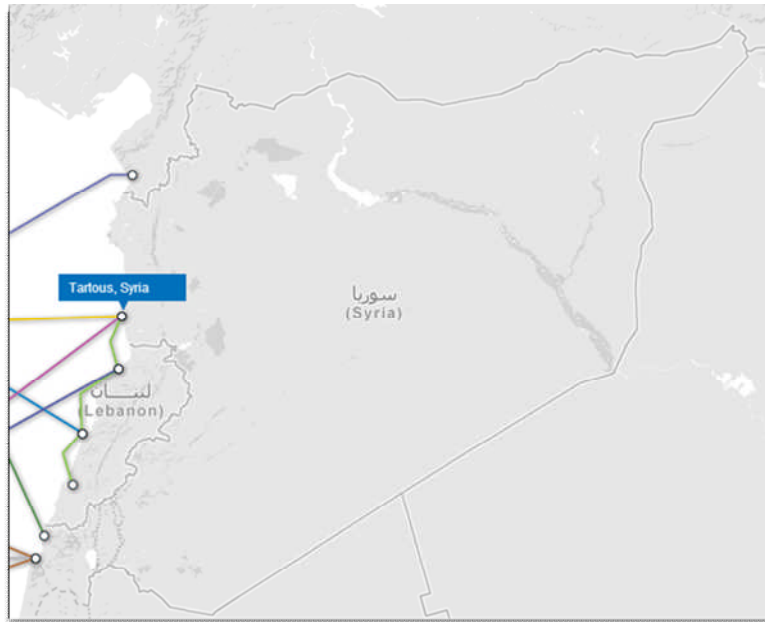


Figure 2. Il n'y a qu'un seul câble sous-marin reliant la Syrie à Internet³⁵

○ *Le contrôle de l'information et des images*

Ce contrôle est d'abord assuré par une censure que l'on peut qualifier de généralisée et de masse, grâce à l'investissement dans d'importants outils de cybersurveillance. La Syrie possède à cet égard une solide expérience : dès 2006, elle est classée parmi les 13 pays ennemis de l'Internet par Reporter sans frontières (RSF) qui la qualifie de plus « *grande prison du Moyen-Orient pour les cyberdissidents* ». Dans le rapport 2011/2012 de l'ONG, la Syrie est située au 176^{ème} rang sur 179 pays classés : « *censure absolue, surveillance généralisée, violences aveugles et manipulations du régime ont rendu impossible le travail des journalistes* ». Bachar el-Assad semble en outre avoir tiré les leçons des précédentes révolutions qui ont secoué 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* »³⁶.

Le régime baasiste ne se contente cependant pas de l'aspect technique : il s'est en effet assuré de disposer des outils juridiques nécessaire à la légalisation de ce contrôle, et à la répression des opposants.

³⁵ <http://www.submarinecablemap.com/>

³⁶ Source : <http://syrie.blog.lemonde.fr/2011/08/10/qui-tue-qui-aujourd'hui-en-syrie/>

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 Syriens³⁷ et de mettre en place un contrôle renforcé de la population. L'atteinte à « *l'unité nationale* », ou à la « *sécurité nationale* »³⁸, est également sanctionnée et la presse s'est vue imposer 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 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 blog³⁹ que « *le régime détient un monopole sur l'information intérieure (...) dont le contrôle est assuré par les services de renseignements* », les *Moukhabarat*.

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. 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)⁴⁰, celles-là même qui avaient défrayé la chronique avec le matériel d'Amesys, filiale de Bull, en Libye.

Les membres de Telecomix se sont, les premiers, penchés sur le dispositif de surveillance syrien et ont diffusé 54 Go de données⁴¹ prouvant la surveillance des communications électroniques syriennes par du matériel de la société américaine Blue Coat. La nouvelle a traversé l'Atlantique⁴² ⁴³ et Blue Coat a vivement démenti avoir vendu du matériel à la Syrie. La société n'a cependant pas exclu la possibilité

³⁷ Source : <http://www.state.gov/r/pa/ei/bgn/3580.htm>

³⁸ Source : <http://www.freedomhouse.org/report/freedom-press/2007/syria>

³⁹ Source : <http://syrie.blog.lemonde.fr/2011/08/10/qui-tue-qui-aujourd'hui-en-syrie/>

⁴⁰ Source : <http://www.monde-diplomatique.fr/2012/01/CHAMPAGNE/47183>

⁴¹ Source : <http://reflets.info/opsyria-syrian-censoship-log/>

⁴² Source : http://www.washingtonpost.com/world/national-security/syria-using-american-software-to-censor-internet-experts-say/2011/10/22/gIQA5mPr7L_story.html

⁴³ Source : http://www.washingtonpost.com/world/national-security/us-probes-use-of-surveillance-technology-in-syria/2011/11/17/gIQA51iEVN_story.html

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. En réalité, le matériel aurait d'abord transité par les Emirats Arabes Unis avant d'être expédié en Syrie⁴⁴. Le mal est fait pour les insurgés et les équipements de Blue Coat ont, selon le Wall Street Journal⁴⁵, 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.

Le même scénario s'est reproduit avec les sociétés HP⁴⁶ et NetApp⁴⁷. 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 »⁴⁸, l'ensemble du projet serait évalué à presque 18 millions de dollars. Plusieurs autres systèmes de filtrage sont également évoqués çà et là, mais sans plus de détails : logiciel *Thundercache*^{49 50}, matériel de la société allemande Fortinet⁵¹, de la société suédoise Ericsson⁵² ou de son voisin finlandais Nokia⁵³, voire « *d'entreprises irlandaises* »⁵⁴.

- *Le développement de capacités offensives*

La constitution d'une force étatique 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 cyberspace. Le

⁴⁴ Source : http://www.bis.doc.gov/federal_register/rules/2011/76fr78146.pdf

⁴⁵ Source : <http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html>

⁴⁶ Source : <http://www.bloomberg.com/news/2011-11-18/hewlett-packard-computers-underpin-syria-electronic-surveillance-project.html>

⁴⁷ Source : <http://www.sfgate.com/business/article/U-S-probes-NetApp-role-in-Syrian-surveillance-3588858.php>

⁴⁸ Source : <http://intelnews.org/2011/11/07/01-860/#more-7503>

⁴⁹ Source : <http://owni.fr/2011/06/07/la-syrie-coupure-net/>

⁵⁰ Source : http://www.maxisciences.com/internet/qui-coupe-le-flux_art22073.html

⁵¹ Source : <http://www.itnews.com.au/News/277928,us-investigates-blue-coat-over-syria-filter-claims.aspx>

⁵² Source : <http://www.lefigaro.fr/flash-actu/2012/06/25/97001-20120625FILWWW00491-syrie-fabius-veut-plus-de-sanctions.php>

⁵³ Source : <http://www.scancomark.se/05-08-2010-How-Nokia-technology-helps-syria-clamp-down-on-dissidents.html>

⁵⁴ Source : http://www.francetv.fr/info/telecomix-des-hactivistes-au-secours-du-peuple-syrien_62941.html/

pouvoir cherchait à déconnecter les insurgés et à les empêcher de communiquer et de s'organiser. La Syrie va plus loin : le régime n'est plus seulement censeur et émetteur d'information. Il combat les médias sociaux par les médias sociaux et contrecarre les insurgés (et leurs soutiens) en retournant leurs méthodes contre eux : hacking, attaques DDoS, etc. Cette stratégie n'est cependant possible que parce que le régime conserve de nombreux partisans qui se sont fortement impliqués dans les affrontements numériques.

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 SANA⁵⁵ : l'intox et la désinformation sont un moyen efficace de brouiller le discours des opposants⁵⁶. Le régime envoie également ses supporters sur les divers réseaux sociaux et autres blogs noyer les commentaires négatifs sur le régime par un océan de commentaires positifs.

Les outils d'interception achetés à l'étranger sont, quant à eux, 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 cyberspace 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 rapide inventaire des méthodes employées.

Ces moyens sont variés ; Ils allient d'anciennes méthodes adaptées à de nouvelles techniques propres au réseau (coupures stratégiques du réseau, surveillance et monitoring à grande échelle, hacking⁵⁷).

Usage stratégique du blocage d'accès à certains sites : en février 2011, l'accès à Facebook et YouTube a été de nouveau autorisé, après plus de trois ans de blocage.

⁵⁵ Agence de presse arabe syrienne - http://www.sana.sy/index_fra.html

⁵⁶ Source : <http://syrie.blog.lemonde.fr/2011/08/10/qui-tue-qui-aujourd'hui-en-syrie/>

⁵⁷ Source : <http://www.atlantico.fr/decryptage/crise-syrienne-guerre-etend-desormais-aussi-reseaux-sociaux-francois-bernard-huyghe-455988.html>

Certains Syriens s'étaient alors réjouis de la nouvelle sur les réseaux sociaux⁵⁸. Intervenant quelques semaines après les événements en Egypte et en Tunisie, ce geste a été salué par le gouvernement américain⁵⁹ 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 cependant continué à utiliser leurs logiciels de chiffrement, même après cette « *ouverture* ».

Attaques DDOS : Méthode simple de perturbation d'un site, cette technique a été largement utilisée en Syrie, notamment par la Syrian Electronic Army à l'encontre de certains sites prorévolutionnaires.

La Syrian Electronic Army

Constituée autour du Syrian computer club⁶⁰, groupe présidé autrefois par Bachar el-Assad lui-même, cette unité est apparue pour la première fois en avril 2011 et compterait, selon l'un de ses membres, plusieurs milliers de personnes. Elle a été officiellement reconnue par le président el-Assad comme une « *armée réelle dans une réalité virtuelle* »⁶¹, même si la SEA nie tout lien direct avec une quelconque entité gouvernementale. Selon les informations disponibles, elle réunit des profils hétéroclites⁶², du professionnel aguerri au conscrit doué en informatique, en passant par l'élève-ingénieur. Il est pourtant difficile de savoir s'il s'agit d'une réelle unité organisée comme telle, ou une forme de groupe éphémère lançant des attaques coordonnées, à la manière des Anonymous.

Trojans : Les trojans (ou chevaux de Troie) ont été très prisés par les forces syriennes⁶³ afin de récupérer autant d'informations que possible sur les insurgés : mots de passe, documents, courriers électroniques, faux antivirus⁶⁴, etc. Le logiciel Skype a notamment été utilisé comme vecteur de diffusion de ces trojans^{65 66}. Dans la majorité des cas, les logiciels malveillants envoient les données dérobées vers un

⁵⁸ Source : <http://globalvoicesonline.org/2011/02/08/syria-facebook-and-youtube-unblocked-among-others/>

⁵⁹ Source : http://abonnes.lemonde.fr/technologies/article/2011/02/09/les-syriens-reconnectes-a-facebook-et-youtube_1477641_651865.html

⁶⁰ Source : <http://edition.cnn.com/2011/11/22/world/meast/syria-cyberwar/index.html>

⁶¹ Source : <http://www.sana.sy/eng/337/2011/06/21/353686.htm>

⁶² Source : <http://blog.thepro.sy/>

⁶³ Source : <https://www.eff.org/deeplinks/2012/04/campaign-targeting-syrian-activists-escalates-with-new-surveillance-malware>

⁶⁴ Source : <http://edition.cnn.com/2012/02/17/tech/web/computer-virus-syria/index.html>

⁶⁵ Source : <http://blog.trendmicro.com/fake-skype-encryption-software-cloaks-darkcomet-trojan/>

⁶⁶ Source : <https://www.eff.org/deeplinks/2012/05/fake-skype-encryption-tool-targeted-syrian-activists-promises-security-delivers>

nombre limité d'adresses IP appartenant, pour la plupart, au gouvernement ou à la compagnie publique de télécommunications (EST).

Attaques Man-in-the-Middle : Facebook a été la cible de nombreuses convoitises. Les internautes syriens ont ainsi été victimes d'attaques de type « *man-in-the-middle* »⁶⁷ : un pirate s'immisce dans la communication entre l'internaute et les serveurs de Facebook afin d'intercepter les échanges de données.

Phishing : Les tentatives de phishing sont nombreuses : de fausses pages Facebook⁶⁸ ou Youtube⁶⁹ pullulent sur Internet, réclamant de manière irrégulière identifiant et mot de passe aux utilisateurs, et proposant parfois de fausses mises à jour d'Adobe Flash Player afin d'infecter leurs terminaux⁷⁰.

Blocage de connexions : Les forces de sécurité bloquent également les accès sécurisés à certains sites, forçant des connexions « classiques », non sécurisées et donc vulnérables à des interceptions. L'activiste Dlashad Othman rapporte des blocages du réseau TOR, ainsi que le blocage ponctuel des connexions SSL⁷¹. 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 Coat⁷².

Propagande et guérilla numérique : La SEA participe à la guerre d'informations en répandant la propagande pro-Assad sur le Web, y compris sur des pages Facebook occidentales, ou en noyant Twitter sous un flot de contenus pro-gouvernementaux ou sans intérêt grâce à des bots⁷³. Certains messages de propagande sont diffusés, pré-rédigés et prêts à être réutilisés par les partisans⁷⁴. La Free Syrian Army mène également des opérations qui pourraient s'apparenter à une « guérilla » numérique :

⁶⁷ Source : <http://blogs.voanews.com/digital-frontiers/2011/05/12/syrias-internet-hijack/>

⁶⁸ Source : <https://www.eff.org/deeplinks/2012/03/pro-syrian-government-hackers-target-syrian-activists-facebook-phishing-attack>

⁶⁹ Source : <http://www.guardian.co.uk/technology/2012/mar/20/syrian-activists-fake-youtube?newsfeed=true>

⁷⁰ Source : <https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware>

⁷¹ Source : <http://www.slideshare.net/DavidVvorst/the-internet-in-syria>

⁷² Source : <http://reflets.info/opsyria-bluecoat-au-coeur-dattaque-mitm-de-grand-evergure/>

⁷³ Source : <http://www.guardian.co.uk/commentisfree/2011/apr/21/syria-twitter-spambots-pro-revolution>

⁷⁴ Source : <http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/>

défacement de pages Web⁷⁵, infections d'ordinateurs d'opposants⁷⁶, piratage de comptes Twitter (par exemple celui d'Al-Arabiya⁷⁷), etc.

La diffusion d'outils de piratage « grand public » et la mobilisation de sympathisants : La SEA met à disposition des outils de hacking à destination de ses sympathisants ainsi que les modes d'emploi pour pirater un ordinateur⁷⁸ ou défacier un site⁷⁹. Des vidéos, disponibles en arabe et en anglais, expliquent comment utiliser Shell, un script destiné à pénétrer des sites^{80 81}. Développé par les « Syrian Electronic Army Coders », mais existant selon certaines sources depuis 2004⁸², cet exemple est révélateur d'un mimétisme intéressant avec les pratiques des Anonymous : ces derniers avaient mis à disposition de leurs sympathisants un outil permettant de transformer volontairement leur ordinateur en « machine-zombie » pour effectuer des attaques par DDoS. On retrouve ici 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 Internet⁸³. 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^{84 85}.

Dès lors, si le cyberspace 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 saisi les enjeux du cyberspace 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.

⁷⁵ Source : <http://www.infowar-monitor.net/2011/06/syrian-electronic-army-defaces-41-web-sites-one-uk-government-web-site/>

⁷⁶ Source : http://threatpost.com/en_us/blogs/syrian-dissidents-hit-another-wave-targeted-attacks-062012

⁷⁷ Source : http://www.huffingtonpost.co.uk/faisal-abbas/syrian-electronic-army-de_b_1448517.html

⁷⁸ Source : <http://www.theatlantic.com/international/archive/2011/08/syrias-digital-counter-revolutionaries/244382/>

⁷⁹ Source : <http://www.youtube.com/watch?v=foD56TQbMEo&feature=relmfu>

⁸⁰ Source : <http://www.youtube.com/watch?v=foD56TQbMEo&feature=relmfu>

⁸¹ Source : <http://www.youtube.com/watch?v=O8rnZo8oFaw&feature=relmfu>

⁸² Source : <http://www.infowar-monitor.net/2011/06/syrian-electronic-army-defaces-41-web-sites-one-uk-government-web-site/>

⁸³ Source : <http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/>

⁸⁴ Source : <http://opennet.net/sites/opennet.net/files/SEADisruptiveAttacksFigure-11.png>

⁸⁵ Source : <http://opennet.net/sites/opennet.net/files/SEADisruptiveAttacksFigure-12.png>

Il faut donc souligner le déséquilibre caractérisant l'affrontement entre gouvernement syrien et opposants. Ces derniers partent désavantagés, devant composer avec un système verrouillé d'entrée de jeu par le gouvernement qui maîtrise son réseau. « *Les opposants désarmés mènent une guerre psychologique et virtuelle, avec les moyens du bord* »⁸⁶. Toutefois, des facteurs extérieurs sont venus tempérer cette affirmation.

II. Le rôle des intervenants extérieurs au cœur du conflit syrien - vers un rééquilibrage des forces en présence ?

Dans cet affrontement déséquilibré, Internet constitue un premier facteur égalisateur, un terrain favorable au développement, avec de faibles moyens, d'outils de contournement de la censure relativement efficaces. Ainsi, pour contourner la supériorité technologique de l'Etat syrien, les dissidents vont utiliser des « *moyens et solutions alternatifs* »⁸⁷ avec pour objectif de gagner cette guerre de l'information en diffusant et en informant le plus possible la communauté internationale.

Mais les dissidents sont également largement soutenus par des acteurs extérieurs au conflit. Membres de la diaspora syrienne, hackers et Etats mettent à leur disposition des moyens importants, des compétences, de la créativité et du temps afin de permettre aux dissidents de retrouver l'accès aux moyens de communication. Leur objectif : « *rétablir un équilibre entre un régime qui déploie [d'importants] moyens pour surveiller Internet, et des internautes qui souhaitent accéder à l'information que le régime leur refuse* »⁸⁸. Et pour cause, l'intervention de ces acteurs étrangers a pour effet direct de procurer aux dissidents des moyens et des outils dont ils ne disposeraient pas autrement.

Ces soutiens extérieurs ont un impact considérable sur le conflit, comme le souligne François-Bernard Huyghe : « *source importante de motivation pour les manifestants et cyberdissidents, ils contribuent à une plus forte mobilisation de l'opinion internationale. Si on a du mal à mesurer l'impact réel du phénomène, il suffit*

⁸⁶ Source : <http://mediarabe.info/spip.php?article2060>

⁸⁷ Sophia Clément-Noguier, « SÉCURITÉ DU FORT CONTRE ASYMÉTRIE DU FAIBLE », Armand Colin, Revue internationale et stratégique.

⁸⁸ Source : <http://reflets.info/syrie-qui-est-defavorise-sur-le-terrain-de-la-communication/>

d'observer, a contrario, un pays où la guerre de l'information n'a pas été remportée par les dissidents vite écrasés : le Bahreïn. La TV ne parle pas de la répression perpétrée dans ce pays, la communauté internationale n'est que peu sensibilisée. »⁸⁹

Si l'impact de ces interventions est a priori positif, il est en réalité loin de faire l'unanimité : tant son efficacité que sa légitimité sont source de polémiques. Ce qui nécessite un retour sur les tenants et aboutissants de cette intervention extérieure.

A. L'intervention des acteurs extérieurs au conflit comme contrepoids face aux capacités de l'Etat syrien

Diaspora syrienne, hackers et Etats s'investissent de façon originale et créative afin de fournir aux dissidents les moyens nécessaires au contournement de la censure et de la répression de Damas. Cette aide est loin d'être superflue car seuls, les dissidents ne disposent que de peu de moyens pour rivaliser avec stratégie mise en œuvre par le régime de Bachar el-Assad.

o L'apport de la diaspora syrienne

Crowdmapping et géolocalisation : Le 25 mars 2012 a été mise en ligne la crowdmap⁹⁰ Syria Tracker⁹¹, qui permet de recueillir des chiffres directement auprès de la population syrienne, via Internet et les téléphones portables, afin de cartographier et réaliser 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.

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. 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

⁹⁰ Source : Crowdsourcing : méthode collaborative permettant de fédérer les informations issues d'un grand nombre de personnes afin d'alimenter un projet.

⁹¹ Source : <https://syriatracker.crowdmap.com/>

Aïd »⁹². Sur Facebook et sur Twitter, la campagne a reçu un vaste écho. 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 »⁹³.

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.

- *Des hackers engagés aux côtés des dissidents*

Plusieurs groupes de hackers politiques, des hacktivistes, se sont organisés pour apporter leur expertise et leur savoir-faire aux opposants syriens.

#OpSyria : Telecomix, un cluster de hacktivistes, est parvenu à détourner dans la nuit du 4 au 5 septembre 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 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 publié⁹⁴, accompagné de la plateforme Syrian Stories⁹⁵ qui éditorialise le contenu du premier site.

La créativité technologique mise au service des dissidents : Telecomix travaillerait 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 dissidents⁹⁶. 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

⁹² Source : <http://globalvoicesonline.org/2011/11/09/global-campaigns-in-solidarity-with-syria-keep-growing/>

⁹³ Source : <http://www.syriansitin.com/>

⁹⁴ Source : <http://broadcast.telecomix.org/syria/>

⁹⁵ Source : <http://syrianstories.org/>

⁹⁶ Source : <http://owni.fr/2012/06/03/telecomix-syrie-ong-drone/>

partager de la musique, Telecomix souhaiterait que la Pirate Box, alimentée par panneaux solaires, serve à « *communiquer dans un périmètre critique* »⁹⁷, grâce notamment à un module de *chat* anonymisé.

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 opposants⁹⁸ ou encore en piratant les mails de plusieurs collaborateurs du chef de l'État syrien⁹⁹.

L'Electronic Frontier Foundation : Enfin, l'Electronic Frontier Foundation¹⁰⁰ 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 Skype¹⁰¹ (en réalité un programme malveillant d'espionnage), de la mise en ligne d'un faux Youtube¹⁰² ou encore de la multiplication de tentatives de phishing sur Facebook¹⁰³.

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 el-Assad : certains États s'emploient également à soutenir le soulèvement pro-démocratique.

- *L'intervention accrue de certains Etats*

Si le cyberspace est un terrain d'affrontements entre l'Etat syrien et les insurgés, c'est également un excellent moyen pour les acteurs internationaux d'intervenir plus ou moins discrètement afin de soutenir les différentes parties au conflit. Les Etats-

⁹⁷ Source : <http://owni.fr/2012/06/03/telecomix-syrie-ong-drone/>

⁹⁸ Source : http://www.huffingtonpost.com/2011/08/08/syria-ministry-of-defense-hacked-anonymous_n_920733.html

⁹⁹ Source : <http://www.lefigaro.fr/international/2012/02/12/01003-20120212ARTFIG00187-des-hackers-devoilent-les-mails-secrets-entre-damas-et-teheran.php>

¹⁰⁰ Source : <https://www.eff.org/>

¹⁰¹ 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

¹⁰² Source : http://www.lemonde.fr/technologies/article/2012/03/15/un-faux-youtube-pour-pieger-les-activistes-syriens_1669410_651865.html

¹⁰³ Source : http://www.lemonde.fr/technologies/article/2012/03/30/les-opposants-syriens-vises-par-du-phishing-sur-les-reseaux-sociaux_1678017_651865.html

Unis, qui ont une vision stratégique de l'usage d'Internet et soutiennent les rebelles, sont bien entendu omniprésents.

Cet engagement contribue sans aucun doute à rééquilibrer ou, du moins, à changer la donne dans l'équilibre du conflit opposant dissidents et pro-Assad. L'intervention de la puissance américaine est en effet souvent considérée par certains analystes comme un facteur favorisant une situation de dissymétrie, en raison de la supériorité des moyens généralement engagés par les Etats-Unis¹⁰⁴.

Comme le relatent le Time Magazine¹⁰⁵ et Al Monitor¹⁰⁶, 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 House¹⁰⁷. Certains dissidents se sont donc 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.

La Syrie n'a pas été le premier théâtre d'opération de la stratégie numérique américaine. L'ensemble de ces technologies et de ces programmes de formations s'inscrit dans le cadre¹⁰⁸ 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. Le projet s'est ensuite élargi, puisque suite aux manifestations iraniennes de 2009 et aux événements 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.

¹⁰⁴ Dissymétrie : « stratégie étatique visant à recourir sur la durée à la supériorité qualitative et quantitative des moyens techniques ». La revue internationale et stratégique, n°51, automne 2003

¹⁰⁵ Source : <http://world.time.com/2012/06/13/hillarys-little-startup-how-the-u-s-is-using-technology-to-aid-syrias-rebels/>

¹⁰⁶ Source : <http://www.al-monitor.com/pulse/security/01/06/americas-electronic-war-on-syria.html>

¹⁰⁷ Source : <http://www.al-monitor.com/pulse/security/01/06/americas-electronic-war-on-syria.html>

¹⁰⁸ L'intervention américaine, sous forme d'aide gouvernementale, a, elle, des racines profondes. Ses méthodes, favoriser ou fournir de médias à la dissidence, remontent à la Guerre froide (à l'époque, l'Amérique finançait des radios anticommunistes qui émettaient à direction de l'est, collées au rideau de fer). Mais elles se sont modernisées, et les États-Unis ont affiché un soutien à toutes les cyberdissidences (stages, formations, fourniture de technologies...). » Entretien accordé à CEIS par François-Bernard Huyghe, docteur d'État en Sciences Politiques et chercheur à l'IRIS, le 04 septembre 2012.

Sur le terrain, l'objectif de la stratégie américaine consiste à donner aux insurgés la possibilité de communiquer sur leur lutte, ce qui passe par plusieurs étapes :

- assurer une **capacité de connexion** en toutes circonstances, ce qui implique la possibilité de se connecter même lorsque les infrastructures télécoms sont désactivées ou endommagées ;
- fournir un **équipement**, même rudimentaire, permettant de témoigner et de documenter la lutte (ordinateur portable, caméra, ...) ainsi que permettre le fonctionnement de ce matériel (alimentation électrique, consommables, etc.) ;
- permettre le **contournement des moyens de censure étatiques**, afin que les informations d'un cyberdissident puissent être librement accessibles sur Internet par un autre dissident, ou par la scène internationale ;
- **former les utilisateurs** à l'utilisation des outils numériques en toute sécurité. Il s'agit d'initier les utilisateurs aux méthodes de cryptographie et d'anonymisation des connexions, ainsi qu'aux techniques permettant de déjouer la surveillance des Etats.

L'exemple de Psiphon.

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 ». 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, le programme de recherche sur le cyberspace et les droits humains de l'Université de Toronto (Canada), a bénéficié de fonds en provenance du gouvernement américain.

Si les Etats-Unis et le Canada semblent afficher clairement leurs intentions de soutien à la Syrie, il n'en va pas de même pour l'Europe qui se positionne timidement à l'aide de sa stratégie baptisée « No disconnect ».

Côté européen, la stratégie de soutien se révèle en effet plus timide. En décembre 2011, soit un an après le début du « printemps arabe », la vice-présidente de la Commission européenne Neelie Kroes a prononcé un discours présentant la stratégie européenne « No Disconnect » destinée à promouvoir la liberté d'expression sur Internet¹⁰⁹. Cette stratégie s'organise autour de quatre objectifs¹¹⁰. Il s'agit tout d'abord de fournir aux populations des régimes non-démocratiques des outils technologiques « destinés à améliorer la protection de la vie privée et la sécurité ». Ensuite, il faut « éduquer et sensibiliser les militants quant aux possibilités et aux risques inhérents aux TIC » et « collecter des renseignements » permettant de « contrôler le niveau de surveillance et de censure à un moment donné et dans un lieu donné ». Enfin, il s'agit de promouvoir la coopération entre « toutes les parties concernées ». Neelie Kroes est récemment revenue sur son blog sur les avancées de cette stratégie¹¹¹. Expliquant qu'il fallait soutenir les opposants aux régimes autoritaires en leur fournissant les outils pour contourner la censure, elle a dévoilé un appel à propositions¹¹² dédié au « renforcement du respect des droits de l'homme et des libertés fondamentales là où ils sont les plus menacés et [au] soutien aux défenseurs des droits de l'homme ». Elle a également insisté sur l'importance des initiatives technologiques¹¹³, notamment de « réseaux communautaires décentralisés » (decentralised community networks)¹¹⁴. La technologie n'est pas le seul aspect envisagé par la commissaire, qui estime qu'il faut responsabiliser les industriels grâce à un projet de guide de bonne conduite¹¹⁵, avant de conclure sur l'importance d'avoir à disposition des sources d'informations fiables afin de pouvoir distinguer la censure d'une interruption accidentelle.

Comparée à la stratégie américaine, cette stratégie paraît modeste, et selon certains, tardive. Julien Nocetti, chercheur associé à l'Ifri, fustige la frilosité européenne : « occultant le potentiel du Web comme outil diplomatique, se focalisant sur la « croissance du marché européen numérique », cette stratégie traduirait surtout le

¹⁰⁹ Source :

<http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/866&format=HTML&aged=0&language=EN&guiLanguage=en>

¹¹⁰ Source : <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1525>

¹¹¹ Source : <http://blogs.ec.europa.eu/neelie-kroes/eu-fighting-cybercensorship/#more-2002>

¹¹² Source : [https://webgate.ec.europa.eu/europeaid/online-](https://webgate.ec.europa.eu/europeaid/online-services/index.cfm?ADSSChck=1337616216735&do=publi.detPUB&searchtype=AS&Pgm=7573843&zgeo=38220&aoet=36539&debpub=&orderby=upd&orderbyad=Desc&nbPubliList=15&page=1&aoref=132760)

[services/index.cfm?ADSSChck=1337616216735&do=publi.detPUB&searchtype=AS&Pgm=7573843&zgeo=38220&aoet=36539&debpub=&orderby=upd&orderbyad=Desc&nbPubliList=15&page=1&aoref=132760](https://webgate.ec.europa.eu/europeaid/online-services/index.cfm?ADSSChck=1337616216735&do=publi.detPUB&searchtype=AS&Pgm=7573843&zgeo=38220&aoet=36539&debpub=&orderby=upd&orderbyad=Desc&nbPubliList=15&page=1&aoref=132760)

¹¹³ Source : http://cordis.europa.eu/fp7/ict/fire/events/evwfsfriends_en.html

¹¹⁴ Source : <http://confine-project.eu/>

¹¹⁵ Source : http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=5752&lang=en

manque de vision politique de l'Union européenne sur les questions Internet, au risque de se voir distancée durablement par les Etats-Unis »¹¹⁶.

La France apparaît quant à elle dans la droite ligne de la stratégie européenne. Le Premier ministre Jean-Marc Ayrault a ainsi indiqué que la France envoyait des « éléments non létaux, [...] de communication et de protection »¹¹⁷.

Les soutiens numériques à l'Etat syrien.

Il est possible de recenser quelques soutiens à l'Etat syrien sur le plan numérique. Les principaux soutiens internationaux de la Syrie sont, sans surprise, l'Iran, la Russie et la Chine¹¹⁸. Les raisons de ce soutien ont déjà été largement évoquées par la presse¹¹⁹. Si certains ont ainsi évoqué la crainte que ces révoltes n'encouragent des mouvements semblables dans leurs pays, une chose est sûre : ces pays ont une importante expérience en matière de surveillance et de contrôle des réseaux. Qu'il s'agisse de l'usage des réseaux sociaux dans les soulèvements ayant secoué l'Iran en 2009 ou de la censure institutionnalisée en Chine, ces pays sont parfaitement conscients du potentiel du cyberspace d'un point de vue politique et stratégique.

Le site Infowar-monitor.net a effectué une étude approfondie des attaques revendiquées par la SEA l'année dernière, et en a tiré plusieurs conclusions¹²⁰. 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 pourrait indiquer l'existence d'une collaboration entre certains groupes de hackers pro-syriens et pro-iraniens. Des correspondances qui pourraient même témoigner d'une coopération entre Téhéran et Damas.

Cette hypothèse semble être confirmée par d'autres sources qui expliquent que « *l'Iran aurait d'ailleurs fourni des armes à son allié, ainsi que des systèmes de surveillance d'Internet et des réseaux sociaux que Téhéran a déjà testés régulièrement à l'encontre des militants et des opposants iraniens* »¹²¹. Dans le même article, l'auteur précise que « *l'Iran aide la Syrie au niveau de la cyber-guerre pour le contrôle des outils internet. Il l'aide même sur le terrain puisque ça a été reconnu dernièrement à Téhéran par des membres des "pasdaran". Ils disent qu'ils aident pour éviter que cela ne dégénère trop, comme si l'Iran était susceptible d'empêcher que le conflit en Syrie ne dégénère en guerre civile ethno-confessionnelle à grande échelle.* »¹²² Tal Be'ery, ancien expert informatique de l'armée israélienne et actuellement chercheur chez Imperva, partage cette vision¹²³. Il va même encore plus loin en expliquant que les services russes ont infiltré l'opposition avec succès grâce à des

¹¹⁶ Source : <http://www.ifri.org/downloads/pe22011articlejuliennocetti.pdf>

¹¹⁷ Source : http://www.lepoint.fr/monde/ayrault-sur-le-plan-militaire-nous-avons-repondu-a-la-demande-du-cns-22-08-2012-1498023_24.php

¹¹⁸ Source : <http://www.france24.com/fr/20120221-syrie-pourquoi-axe-teheran-moscou-pekinn-supporte-le-regime-bachar-al-assad>

¹¹⁹ Source : http://www.francetvinfo.fr/syrie-les-raisons-du-soutien-russe-et-chinois-a-bachar-al-assad_59929.html

¹²⁰ Source : <http://www.infowar-monitor.net/2011/06/syrian-electronic-army-disruptive-attacks-and-hyped-targets/>

¹²¹ Source : <http://www.rfi.fr/sites/filesrfi/Syrie%20Iran%20Plan%20Annan.doc>

¹²² Source : <http://www.rfi.fr/sites/filesrfi/Syrie%20Iran%20Plan%20Annan.doc>

¹²³ Source : http://www.huffingtonpost.com/2012/08/07/syria-cyber-war_n_1750724.html?ncid=edlinkusaolp00000003

méthodes comme les faux profils Facebook ou les certificats SSL falsifiés, des méthodes que l'on retrouve également en Syrie. Moscou ayant été très impliqué dans la mise en place du système d'interception syrien, il en conclut qu'il est parfaitement plausible que Damas ait encore accès à des ressources humaines ou matérielles russes.

B. Des soutiens extérieurs pourtant controversés

- *Un soutien étatique occidental jusque-là cantonné au cyberspace.*

« Si on avait des missiles antichars et antiaériens, on aurait déjà fini cette révolution, dit Abou Riyad. Quand j'entends dire que les Américains ou les pays du Golfe nous livrent des armes, j'ai envie de rire. On n'a jamais rien reçu. Notre principal fournisseur, c'est l'armée de Bachar. »¹²⁴

Le conflit syrien se caractérise par une aide essentiellement cantonnée au cyberspace. Ni les Etats-Unis, ni les Etats européens n'auraient fourni d'armes aux rebelles.

L'objectif est clair : éviter un soutien décrié, parfois difficile à assumer, notamment lorsque le matériel livré aux combattants est revendu, distribué et détourné de son objectif premier. Le Figaro, qui titre « *La dangereuse idée d'armer les rebelles syriens* », a pu souligner à cet égard que, « *sans la condamner ouvertement, l'Occident est mal à l'aise avec l'idée d'armer les rebelles anti-Bachar de l'ASL (Armée syrienne libre)* »¹²⁵. Selon l'auteur de ce même article, « *favoriser les droits de l'homme et la démocratie en Islam par l'usage du soft power (le pouvoir d'influence par la culture et les médias) est de loin préférable à celui du hard power (le pouvoir des armes)* ». C'est précisément le chemin emprunté par les Etats-Unis et, plus timidement, l'Europe avec sa stratégie « No Disconnect ».

Le cyberspace apparaît donc comme une aubaine : un moyen discret, détourné et non létal d'aider et de contribuer aux révolutions, un outil diplomatique sans précédent. En bref, le cyberspace devient un nouvel espace d'expression des alliances et des soutiens aux rebelles.

¹²⁴Source : Membre de l'armée syrienne libre, citée par Le Figaro - <http://www.lefigaro.fr/international/2012/07/19/01003-20120719ARTFIG00510-syrie-les-rebelles-lancent-des-raids-jusqu-au-c339ur-des-villes.php>

¹²⁵Renaud Girard, La dangereuse idée d'armer les rebelles syriens, <http://www.lefigaro.fr/international/2012/04/01/01003-20120401ARTFIG00184-la-dangereuse-idee-d-armer-les-rebelles-syriens.php>

Le sujet, « *politiquement à la mode* »¹²⁶, est par exemple aux Etats-Unis à l'origine de nombreuses conférences ciblant les cyberactivistes arabes. Les sociétés privées s'engagent (Twitter, Google...) ¹²⁷.

Cette aide par l'envoi de matériel non létal contraste également fortement avec les possibles livraisons d'armes en provenance du Qatar et d'Arabie saoudite à l'Armée Syrienne Libre¹²⁸. En se positionnant ainsi sur le terrain de la guerre de l'information, les Etats-Unis parviennent à fournir des moyens financiers, des compétences, des outils techniques, etc.

Mais cette contribution est parfois décriée, voire qualifiée par certains cyberdissidents de « *baiser de la mort* ». Quelles sont les limites de cette intervention étatique accrue ?

- *La remise en cause de la légitimité et de l'efficacité des soutiens étatiques occidentaux.*

De nombreuses voix se sont élevées contre l'intervention des Etats occidentaux dans le conflit syrien. Qualifiée d'intéressée, d'inappropriée voire de contreproductive, l'aide du gouvernement américain semble tout particulièrement cristalliser les critiques.

Dans un article intitulé « *Les cyber-activistes arabes face à la liberté sur Internet made in USA* »¹²⁹, le blogueur cyberactiviste Samir Ben Gharbia considère que ce soutien américain aux révoltes arabes ne serait qu'un moyen, pour les Etats-Unis, de favoriser leurs propres intérêts géopolitiques.

Cette aide serait « *sélective* », car ciblant principalement des pays tels que la Chine ou l'Iran, rivaux de longue date de la puissance américaine. Cette aide traduirait également une vision partielle de la réalité. C'est aussi ce qu'indique le cyberactiviste égyptien Alla Abd El Fattah ou le thaïlandais CJ Hinke : certains Etats ne présentant qu'un intérêt moindre dans l'agenda géopolitique américain seraient purement et

¹²⁶ Source : <http://nawaat.org/portail/2011/01/03/les-cyber-activistes-arabes-face-a-la-liberte-sur-internet-made-in-usa/>

¹²⁷ Voir conférence « Internet liberty 2010 ».

¹²⁸ Source : <http://globe.blogs.nouvelobs.com/archive/2012/06/19/la-syrie-theatre-d-une-nouvelle-guerre-froide.html>

¹²⁹ Source : <http://nawaat.org/portail/2011/01/03/les-cyber-activistes-arabes-face-a-la-liberte-sur-internet-made-in-usa/>

simplement oubliés. Samir Ben Gharbia relève également le double-jeu opéré par certains Etats occidentaux qui, d'un côté, financent et soutiennent certains gouvernements et qui, de l'autre, tentent de soutenir les opposants à ces mêmes gouvernements. De quoi décrédibiliser l'action des cyberactivistes. L'aide serait ainsi contreproductive, un véritable « *baiser de la mort* ». Certains Etats sont même accusés de mettre les dissidents en danger, à travers l'élaboration d'une documentation excessivement renseignée, ou l'utilisation de logiciels de communication non-sécurisés.

Sur le fond, certains se sont interrogés sur le caractère libérateur des outils numériques. Dans son article éponyme, Larry Diamond définissait les « *liberation technologies* » comme « *les technologies de l'information et de la communication qui permettent de développer la liberté politique, sociale et économique* ». Soulignant l'importance du contrôle de l'information dans le maintien des régimes autoritaires, il explique que les « *technologies libératrices* » peuvent affaiblir l'emprise des Etats sur ce contrôle, créer une sphère publique, introduire de la transparence pour finalement donner aux citoyens la possibilité de se mobiliser. Mais cette thèse ne fait pas l'unanimité. Dès 2007, Joshua Goldstein¹³⁰ s'interrogeait, à propos de la révolution Orange ukrainienne de 2004, sur un potentiel retournement des nouveaux medias contre les mouvements d'opposition : « *are these tools [communication tools] inherently conducive to the expansion of civic engagement and democratization or will authoritarian governments adapt the technology to their own advantage ?* »¹³¹.

L'action des Etats-Unis peut quant à elle apparaître comme une véritable ingérence, notamment par les alliés du gouvernement syrien. C'est le cas de Moscou qui n'a pas hésité à exprimer ses craintes quant à un éventuel effet de contagion de ce « *concept de promotion de la démocratie* » et du « *changement de pouvoir par une révolution pacifique* »¹³².

Evgeny Morozov¹³³ est le plus célèbre critique de ceux qu'il appelle les « *cyberutopistes* ». Selon lui, associer si étroitement la liberté d'Internet à la stratégie

¹³⁰ Chercheur du *Berkman Center for Internet and Society* de l'Université de Harvard.

¹³¹ Source : http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Goldstein_Ukraine_2007.pdf

¹³² <http://globe.blogs.nouvelobs.com/archive/2012/06/19/la-syrie-theatre-d-une-nouvelle-guerre-froide.html>

¹³³ Source : <http://www.foreignpolicy.com/articles/2011/01/02/freedomgov?page=full>

américaine fait de cette liberté une sorte de « *cheval de Troie de l'impérialisme américain* », ce qui desservirait le projet initial. Il explique également que la proximité affichée par le gouvernement avec les géants américains d'Internet a desservi ces derniers en les délégitimant¹³⁴. Selon Evgeny Morozov, désormais, lorsqu'une entreprise s'exprime, on ne manquerait pas d'y deviner la main de Washington. Un rapport du Congressional Research Service émet d'ailleurs des doutes sur la perception de la politique américaine à l'étranger : « *Focusing Internet freedom efforts on priority countries such as China and Iran has led some to question whether the United States considers Internet freedom a **global principle** or merely a **selective tool** of U.S. foreign policy* »¹³⁵.

L'omniprésence des acteurs américains¹³⁶ dans le secteur IT entraîne une frilosité de plus en plus grande parmi les autres Etats qui cherchent à affirmer leur indépendance. Ainsi, Google apparaît « *chez un nombre croissant de dirigeants russes comme une extension du département d'Etat américain* »¹³⁷. Cette crainte pousse un grand nombre de pays à vouloir étendre leur souveraineté sur une partie du Web. Ils tentent pour cela de fragmenter le web mondial afin d'en extraire une part nationale – si tant est que ce soit possible –, qui pourrait progressivement être isolée du reste du monde. En témoigne les exemples de projets de moteur de recherche national en Turquie, en Russie, d'Intranet national en Iran, etc.

Les cyberdissidents, enfin, souhaitent conserver leur autonomie, leur indépendance. Selon Ben Gharbia, il s'agit là d'un facteur de réussite indispensable à toute « *campagne et initiative numérique réussie* ».

Les cyberdissidents plaident donc pour le développement de capacités internes, sans pour autant s'isoler des autres initiatives. C'est pourquoi les actions de hackers détachés de tout financement gouvernemental restent privilégiées, afin que l'issue de la révolution ne soit pas confisquée par des considérations politiques. L'indépendance est cependant synonyme de développement endogène de capacités suffisantes, notamment en matière de contournement de censure. La professionnalisation de certaines tâches cyberactivistes constituerait-elle un embryon de solution ?

¹³⁴ Source : <http://www.fas.org/sgp/crs/row/R42601.pdf>

¹³⁵ Ibid

¹³⁶ Citant Steve Rubel, expert en nouveaux médias chez Edelman, Eric Scherer explique que « cinq sociétés technologiques américaines influent ensemble sur toute l'offre d'information en ligne : Twitter, Facebook, Apple, Google et Amazon ». Voir : <http://meta-media.fr/2012/08/10/cinq-societes-us-controlent-lacces-a-linfo/>

¹³⁷ Source : www.ifri.org/downloads/ifrinocettiwebroussefra30mars2011.pdf

Conclusion : guerre de l'information syrienne, quelle issue ?

► ***Un possible retournement de situation*** : Il convient de nuancer tout constat excessivement positif quant à l'issue de la guerre de l'information se déroulant actuellement en Syrie. Les régimes autoritaires s'adaptent aux NTIC¹³⁸ et ces dernières pourraient se retourner contre les pays du monde occidental, voire contre les dissidents eux-mêmes, dont les exactions pourraient être diffusées à ce même public. L'appréciation de la situation par les opinions publiques peut par ailleurs être déformée par le surcroît de visibilité et de notoriété dont bénéficient subitement quelques blogueurs ou leaders d'opinion qui ne sont pas forcément représentatifs de la population locale.

► ***Une guerre de l'information au second plan face à l'escalade de violence sur le terrain*** : S'il est vrai que les dissidents atteignent leur objectif en diffusant l'information au reste du monde, il ne s'agit là que d'un objectif secondaire face à la sanglante répression, réalité du terrain. La dimension cybernétique du conflit s'est en effet amoindrie depuis le passage à une militarisation extrême. De plus, les dictatures ont beaucoup appris des dernières révolutions et peuvent retourner ces méthodes et outils à leur avantage. D'autre part, même si la maîtrise du cyberspace est essentielle, la lutte pour la démocratie suppose un passage de relais avec le réel, soit vers des moyens pacifiques, soit par des moyens armés. Or la maîtrise du terrain suppose, tant du côté du régime en place que de la dissidence, des moyens conventionnels, le cyber ne pouvant pas générer le degré de coercition nécessaire.

¹³⁸ Thèse notamment défendue dès 2003 par S. Kalathil et T. Boas dans leur ouvrage *Open Networks, Closed Regimes : The Impact of the Internet on Authoritarian Rule*



les notes stratégiques

Déjà parus :

La sauvegarde de la BITD italienne : quel rôle pour les districts aérospatiaux ? Mai 2012

Enjeux caucasiens : quelles recompositions d'alliances ? Juin 2012

**Puissance aérienne française et format de l'armée de l'air
Le cas de l'aviation de combat.** Juin 2012

**L'assistance militaire à des armées étrangères, l'avenir de
l'action indirecte.** Juillet 2012 – english version available

Le F35/JSF : ambition américaine, mirage européen. Juillet 2012

Ariane et l'avenir des lancements spatiaux européens
Août 2012

A paraître prochainement :

Politique et numérique, la question de la légitimité.

Compagnie Européenne d'Intelligence Stratégique (CEIS)
Société Anonyme au capital de 150 510 € - SIRET : 414 881 821 0022 – APE :
741 G
280 boulevard Saint Germain – 75007 Paris - Tél. : 01 45 55 00 20 – Fax : 01
45 55 00 60
Tous droits réservés

Les notes stratégiques