LES ENNEMIS D'INTERNET

RAPPORT 2013

RAPPORT SPECIAL : SURVEILLANCE

REPORTERS SANS FRONTIERES
POUR LA LIBERTE DE L'INFORMATION

L'ÈRE DES MERCENAIRES NUMÉRIQUES

"Mon ordinateur avait été arrêté avant moi". C'est le constat lucide d'un activiste syrien arrêté et torturé par le régime de Bachar al-Assad. Pris dans les filets de la surveillance en ligne, Karim Taymour explique à un journaliste de Bloomberg[1] s'être vu présenter lors de son interrogatoire une pile de plus de 1000 pages détaillant ses conversations électroniques et ses fichiers échangés sur Skype. Ses bourreaux savaient manifestement autant de lui que s'ils s'étaient trouvés dans sa chambre, ou plutôt dans son ordinateur.

La surveillance en ligne représente un danger grandissant pour les journalistes, blogueurs, citoyens-journalistes et défenseurs des droits de l'homme. En 2011, Wikileaks rendait publics les Spyfiles, des documents qui montrent l'étendue du marché de la surveillance et le poids financier qu'il représente (plus de 5 milliards de dollars), ainsi que la sophistication des produits proposés.

La surveillance traditionnelle n'a pas du tout disparu. Des policiers continuent de rôder près des cybercafés en Erythrée, les dissidents vietnamiens sont suivis et parfois pris à partie par des policiers en civil, le cyber-dissident chinois Hu Jia et son épouse Zeng Jinyang ont dû supporter des policiers stationnés en permanence au bas de leur immeuble pendant des mois. Les mises sur écoutes téléphoniques des journalistes trop curieux ont grandement facilité le travail des services de renseignement. Mais aujourd'hui, les possibilités offertes par la surveillance en ligne élargissent le champ des possibles pour les gouvernements.

L'édition 2013 du rapport sur les Ennemis d'Internet traite de la surveillance, au sens de l'activité de veille destinée à contrôler les voix dissidentes et la diffusion d'informations sensibles, une activité instrumentalisée pour conforter les pouvoirs en place et prévenir toute déstabilisation potentielle.

Le 12 Mars, Journée mondiale contre la cybercensure, une première liste de **5 "Etats ennemis d'Internet" est rendue publique. Elle recense des Etats engagés dans une surveillance active, intrusive, des acteurs de l'information, permettant de graves violations de la liberté de l'information et des droits de l'homme.** Il s'agit de la **Syrie,** de la **Chine,** de **l'Iran,** du **Bahreïn** et du **Vietnam.**

Une liste de 5 **"Entreprises ennemies d'Internet"**, autrement dit de **"mercenaires de l'ère digitale"**, est également publiée. **Gamma, Trovicor, Hacking Team, Amesys et Blue Coat** ont été sélectionnées pour ce recensement non exhaustif, appelé à s'allonger dans les prochains mois. Leurs produits ont été ou sont utilisés par les autorités pour commettre des violations des droits de l'homme et de la liberté de l'information. A l'instant même où ces entreprises ont entrepris de commercer avec des régimes autoritaires, elles ne pouvaient ignorer que leurs produits pourraient être utilisés pour surveiller des journalistes, dissidents ou net-citoyens. Lorsque ces produits de surveillance numérique ont été vendus à un régime autoritaire par un intermédiaire sans que la société éditrice n'en soit informée, l'incapacité de celle-ci à tracer les ventes et exportations de ses propres logiciels est révélateur de l'absence de prise en compte par ces entreprises du risque d'utilisation détournée de leurs technologies et de la vulnérabilité des défenseurs des droits de l'homme.

Des enquêtes menées par Bloomberg, le Wall Street Journal et les chercheurs du Citizen Lab de l'Université de Toronto ont révélé que des technologies de surveillance utilisées contre des dissidents et militants des droits de l'homme dans des pays comme l'Egypte, le Bahreïn et la Libye provenaient d'entreprises occidentales. Deux types de produits fournis par les entreprises sont épinglées dans ce rapport : du matériel d'écoute à grande échelle pour surveiller le réseau dans son ensemble, des logiciels espions (spyware) et autres dispositifs permettant de mettre en place une surveillance ciblée.

1 Lire l'article "Hackers in Damascus"

Ces logiciels espions sont utilisés pour espionner le contenu d'autres disques durs, récupérer des mots de passe, accéder au contenu de messageries électroniques ou espionner des communication de VOIP. Ils peuvent être installés directement sur les ordinateurs ou via le réseau Internet par l'intermédiaire de fausses mises-à-jour ou de pièces jointes dans un e-mail sans que l'utilisateur ne s'en aperçoive. L'usage civil de ce genre de programme est limité. Certains fabricants fournissent directement des acteurs étatiques tels que les services secrets et les services de sécurité ; d'autres n'hésitent pas à faire publicité de leurs capacités à surveiller et traquer les opposants politiques. Dans les régimes autoritaires, ce système est utilisé pour espionner les journalistes et leurs sources afin d'éradiquer la liberté d'information.

Un double emploi peut être fait de certaines technologies ; utilisées à des fins légitimes de lutte contre le cybercrime, elles se transforment en redoutables outils de censure et de surveillance contre les défenseurs des droits de l'homme et les acteurs de l'information lorsqu'elles sont utilisées par des régimes autoritaires. Le manque d'encadrement du commerce de ces 'armes digitales' permet à des gouvernements autoritaires d'identifier des (citoyens-)journalistes pour s'en prendre à eux.

Reporters sans frontières demande la mise en place d'un contrôle de l'exportation de technologies et matériel de surveillance vers des pays qui bafouent les droits fondamentaux. Une telle démarche ne saurait être laissée au secteur privé. Le législateur doit intervenir. L'Union européenne et les Etats-Unis ont interdit l'exportation de technologies de surveillance vers l'Iran et la Syrie. Une décision louable qui ne saurait rester un acte isolé. Les gouvernements européens doivent adopter une approche harmonisée pour contrôler l'exportation des technologies de surveillance. L'administration Obama doit également adopter ce type de législation, tel le Global Online Freedom Act (GOFA).

Des négociations entre gouvernements avaient pourtant déjà eu lieu, se soldant par l'arrangement de Wassenaar conclu en juillet 1996, qui vise à promouvoir « la transparence et une plus grande responsabilité dans les transferts d'armes et de biens à double usage afin de prévenir les accumulations déstabilisantes ». Il regroupe aujourd'hui 41 pays dont la France, l'Allemagne, le Royaume Uni et les États-Unis.

Les démocraties semblent céder progressivement aux sirènes de la surveillance nécessaire et de la cybersécurité à tout prix. En témoigne la multiplication de projets et propositions de lois potentiellement liberticides, permettant la mise en place d'une surveillance généralisée. FISAA et CISPA aux Etats-Unis, British Communications Data Bill au Royaume-Uni, Wetgeving bestrijding cybercrime aux Pays-Bas, autant de textes qui sacrifient la liberté d'expression sur Internet sur l'autel de la lutte contre le cybercrime (pour plus d'informations, lire le chapitre "Tour d'horizon de la cybercensure"). L'adoption par des régimes traditionnellement respectueux des droits de l'homme de ce type de législations liberticides donnerait des arguments aux dirigeants de pays répressifs qui se dotent d'un arsenal législatif contre les voix critiques.

C'est le modèle d'Internet tel que conçu par ses fondateurs, espace d'échanges et de libertés, transcendant les frontières, qui est remis en cause par l'accélération de la cyber-censure et la banalisation de la cyber-surveillance. D'autant qu'Internet fait les frais des luttes d'influence entre Etats. La généralisation de la surveillance est l'un des enjeux majeurs des acteurs qui se battent pour contrôler la gouvernance du Net. Lors de la conférence mondiale des télécommunications de Dubaï en décembre 2012, la Chine a soutenu une proposition destinée à étendre de manière drastique le contrôle de l'ITU sur Internet. La Chine avait l'appui de la Russie, de l'Arabie Saoudite, de l'Algérie et du Soudan pour remettre en cause entre autres le rôle de l'ICANN dans l'attribution des noms de domaines et des plages d'adresse IP, la protection de "la sécurité physique et opérationnelle des réseaux", l'utilisation du DPI dans les réseaux de nouvelle génération [2].

2 Le sommet de l'UIT en décembre 2012 à Dubaï avait pour objectif d'uniformiser les normes et les standards utilisés sur le réseau Internet. L'une des normes proposée de la conférence était la généralisation de l'installation des technologies de Deep Packet Inspection. Ce type de technologie est extrêmement intrusif puisqu'il permet d'accéder au contenu d'emails échangés, d'intercepter les messages instantannés et d'accéder à l'intégralité du contenu consulté par un utilisateur sur Internet.

L'équation est compliquée pour les acteurs de l'information, pris en étau entre d'une part le besoin de protection personnelle et de sécurité de leurs sources en ligne, et d'autre part la nécessité de collecter et faire circuler l'information. La protection des sources ne relève plus seulement de l'éthique des journalistes, elle dépend de plus en plus de leur maîtrise de leur ordinateur comme le note le spécialiste en cybersécurité Chris Soghoian dans un éditorial publié dans le New York Times.

Avant de partir sur le terrain, s'il est soucieux de sa sécurité physique, le reporter de guerre se munit d'un casque et d'un gilet pare-balles. De même, tout journaliste devrait se munir d'un "kit de survie numérique" dès qu'il stocke ou échange des informations sensibles en ligne, sur son ordinateur ou sur son téléphone portable. Ce kit, développé progressivement par Reporters sans frontières sur le site WeFightCensorship, met en avant la nécessité de nettoyer ses documents des métadonnées souvent trop bavardes, explique comment utiliser le réseau Tor ou des réseaux privés virtuels (VPN) pour anonymiser les communications, dispense des conseils pour sécuriser les communications et les données sur les terminaux mobiles etc..

Journalistes et net-citoyens doivent apprendre à mieux estimer les risques potentiels de surveillance et le type de données ou de communications à protéger afin de trouver la solution adaptée à leur situation, et si possible simple d'utilisation. Face à la sophistication des moyens déployés par censeurs et services de renseignements, l'ingéniosité des acteurs de l'information et des hacktivistes qui les épaulent est mise à rude épreuve. Mais de l'issue de leur bras de fer dépend l'avenir de la liberté d'informer. Un combat sans bombes, sans barreaux de prisons, sans encarts blanchis dans les journaux, mais un combat où, si l'on n'y prend pas garde, les ennemis de la réalité et des vérités pourraient imposer une domination absolue.

Note : Le rapport 2013 sur les "Ennemis d'Internet" se distingue des précédents éditions : il ne prétend pas couvrir de manière exhaustive toutes les formes de cybercensure dans l'ensemble des pays du monde, mais se concentre sur la thématique de la surveillance en ligne. Le rapport 2013 analyse de manière approfondie les activités des cinq États et cinq entreprises „leaders" dans ce domaine, mais cette liste est loin d'être exclusive. Un État qui apparaissait dans la liste des „Ennemis d'Internet" en 2012 n'y apparait donc plus forcément en 2013, sans que cela ne signifie une amélioration quelconque de l'état de la liberté de l'information. Retrouvez les autres développements marquants intervenus depuis un an dans notre Tour d'horizon de la cybercensure.

ENTREPRISES ENNEMIES D'INTERNET

AMESYS (MAINTENANT BULL / AMESYS)

Amesys, société française de sécurité informatique, a vendu son produit phare, le système EAGLE, à la Libye de Kadhafi. Cette technologie a été utilisée pour surveiller des journalistes et des militants des droits de l'homme. L'entreprise est poursuivie devant la justice française par la Fédération Internationale des Droits de l'Homme (FIDH) pour complicité de torture. Une instruction est en cours.

Site web : http://www.amesys.fr/
Siège: France

La société

Amesys est une société française créée en 1979 sous le nom de i2e. Elle est spécialisée dans les technologies de l'information. L'entreprise a changé de nom et est devenue "Amesys" en 2004. En 2010, elle a été rachetée par la société française d'informatique, Bull. En 2011, une ONG de défense des droits de l'homme, la FIDH, dépose plainte pour complicité de torture [1]. En 2013, Amesys cède son système EAGLE à une société tierce, Nexa Technologies. EAGLE est désormais développé et commercialisé par un groupe d'anciens employés d'Amesys, sous la direction de Stéphane Salies, ancien directeur de Bull [2].

Portfolio

Le système EAGLE permet aux agences gouvernementales de surveiller le trafic Internet et de stocker des données de connexion pour les mettre ultérieurement à disposition de la police ou des agences de renseignements. D'après le manuel fourni par Amesys, *"La technologie EAGLE développée par Amesys est pensée pour aider les autorités en charge de l'application de la loi et les organismes de renseignement à réduire le niveau de criminalité, se protéger d'une menace terroriste, et identifier toute atteinte potentielle à la sécurité de leur pays."* [3]

La solution EAGLE est composée d'un analyseur réseau, de plusieurs systèmes de stockage et de centres de surveillance destinés à l'analyse des données. Le logiciel permet la création de fiches individuelles, une pour chaque cible. Des exemplaires de ce type de fichage ont été découverts lorsque les rebelles libyens ont pénétré dans les locaux de la police secrète du régime Kadhafi.

Le système EAGLE se base sur la technologie de Deep Packet Inspection (technique d'analyse en profondeur du contenu circulant sur un réseau) et peut analyser tous les types d'activités liées au web. La documentation fournie par Amesys liste les différentes sortes d'activités en ligne pouvant ainsi être inspectées, parmi lesquelles on retrouve l'email (SMTP, POP, IMAP aussi bien que webmail), les services de VoIP, différents protocoles de messageries instantanées, les requêtes envoyées aux moteurs de recherche, et plus généralement l'ensemble du trafic web-http.

Implication en Libye

Les produits Amesys ont été repérés en Libye, où la société a passé un contrat avec la police secrète de Kadhafi. Lors d'une descente dans ses bureaux, des reporters du Wall Street Journal ont trouvé des manuels d'utilisation du système EAGLE, ainsi que des fichiers individuels concernant des citoyens libyens, frappés de son logo [4] [5]. Parmi les cibles espionnées par le régime se trouvait le journaliste libyen Khaled Mehiri. Le Wall Street Journal a démontré [6] que ses emails (dont ses échanges avec la chaîne Al-Jazeera) et ses publications sur Facebook ont été surveillés pendant des mois par des outils Amesys, pour finir imprimés et stockés. En janvier 2011, alors que le Printemps arabe culminait en Tunisie et que des troubles commençaient à apparaître en Libye, Khaled Mehiri fut convoqué par des agents du renseignement. Il subit des pressions visant à le dissuader de publier des déclarations de militants anti-Kadhafi. Sa surveillance se poursuivit après ces convocations. Par peur pour la sécurité de sa famille, le journaliste a dû se cacher pendant plusieurs mois, jusqu'à la fin des affrontements.

1 http://www.fidh.org/La-FIDH-et-la-LDH-deposent-une

2 https://www.privacyinternational.org/blog/bull-quietly-offloads-controversial-surveillance-technology-after-libya-revelations et http://reflets.info/bull-vend-eagle-a-un-actionnaire-de-crescendo-qui-est-lactionnaire-principal-de-bull/

3 http://www.wikileaks.org/spyfiles/files/0/99_AMESYS-EAGLE-GLINT-Operator_Manual.pdf

4 http://www.fidh.org/Amesys-Case-The-Investigation-12752

5 http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

6 http://online.wsj.com/article/SB10001424052970203764804577056230832805896.html

Le rôle joué par Amesys en Libye fait aujourd'hui l'objet une enquête de la justice française, suite à une plainte pour complicité de torture déposée par la Fédération Internationale des Droits de l'Homme (FIDH) au nom de cinq citoyens libyens espionnés par l'intermédiaire du système EAGLE [7].

"La Chambre de l'instruction est venue confirmer qu'il y avait matière à instruire dans cette affaire, malgré les obstacles posés par le Parquet de Paris [une première plainte déposée par l'association Sherpa avait été classée sans suite], visiblement réticent à permettre une enquête impartiale et indépendante dans cette affaire", a déclaré Patrick Baudouin, avocat et président d'honneur de la FIDH.

En septembre 2011, Amesys a publié un communiqué en réaction aux informations parues dans plusieurs médias au sujet de ses activités en Libye [8].

Reporters sans frontières a contacté Amesys le 6 mars 2013, sans réponse à ce jour.

BLUE COAT

Société américaine de sécurité en ligne, Blue Coat est principalement connue pour ses équipements de surveillance du Net. Ces équipements permettent la surveillance de journalistes, de net-citoyens, ainsi que de leurs sources potentielles. Leurs outils se basent sur la technologie d'analyse du contenu des paquets réseau dénommée Deep Packet Inspection, utilisée par de nombreux fournisseurs d'accès à Internet occidentaux pour réguler leur trafic et empêcher les connections indésirables.

Site internet : www.bluecoat.com
Siège : États-Unis

La société
Blue Coat est une société spécialisée dans les technologies de l'information basée dans la Silicon Valley, en Californie. Elle est surtout connue pour avoir fourni des outils de filtrage et de censure à des pays parmi lesquels on trouve la Syrie ou la Birmanie. Mais la société propose aussi des systèmes d'analyse réseau appelés Intelligence Center (centre de renseignement), utilisés par des entreprises et des États pour assurer une veille du trafic réseau et détecter des problèmes techniques. Ils permettent également de surveiller le comportement des internautes.

Portfolio
Blue Coat propose à ses clients une solution utilisant la technologie Deep Packet Inspection (DPI), PacketShaper, qui peut être utilisée pour surveiller et censurer le contenu web. Avec le DPI, il est possible d'analyser chaque paquet IP et de lui faire subir un traitement spécifique, basé sur son contenu (censure, mots-clefs) ou son type (email, VoIP, protocole BitTorrent). Le DPI ne contrevient pas seulement au principe de neutralité du Net que défend Reporters sans frontières, il s'oppose également au principe de la protection des donnés personnelles. Il rend les internautes identifiables. Dans les pays où le respect des droits de l'homme fait défaut, il expose à des risques d'emprisonnement arbitraire, de violences, voire de tortures.

Blue Coat décrit ainsi l'un de ses produits, PacketShaper :

C'est votre réseau. Faites-en ce que vous voulez. [...] PacketShaper analyse et reconnaît le trafic généré par des centaines d'applications professionnelles et récréatives. En outre, grâce à son intégration à WebPulse, service d'intelligence Web en temps réel de Blue Coat, PacketShaper peut même contrôler le trafic d'applications par catégories de contenus Web. [...] PacketShaper facilite le contrôle groupé des applications et contenus associés, tout en mettant à votre disposition des outils précis pour un contrôle granulaire, lorsque cela s'avère nécessaire." [1]

Le DPI est potentiellement dangereux pour les journalistes, les blogueurs, les militants, ainsi que pour leurs sources, dans la mesure où son principe porte atteinte à la nature privée et anonyme de la communication en ligne. La société Blue Coat vend ses produits aussi bien aux agences gouvernementales qu'à des entreprises privées, ce qui la distingue des autres sociétés mentionnées dans ce rapport.

7 http://www.fidh.org/Amesys-Case-The-Investigation-12752

8 http://www.amesys.fr/addons/shared_addons/themes/amesys/doc/COMMUNIQUE_Amesys_01-09-11.doc.pdf

1 http://www.bluecoat.com/products/packetshaper

Implications majeures

Birmanie

La présence en Birmanie de 13 dispositifs Blue Coat a été établie en 2011 [2]. De nombreux internautes ont reçu des messages suspects sur Internet. Ainsi ont été identifiés les produits Blue Coat :

Chers clients,
Le 17 octobre 2011, en raison d'une panne du câble optique sous-marin SEA-ME-WE 3, la connexion Internet est devenue instable. Durant la période de réparation, réalisée par le personnel qualifié, la connexion Internet peut être ralentie et parfois indisponible. Nous vous tiendrons informés en fonction et nous nous excusons pour la gêne occasionnée.
Respectueusement,
Yatanarpon Teleport

Ce message s'affichait en anglais et en birman. L'URL correspondante - notify.bluecoat.com - en a montré l'origine.

Syrie

Le collectif Telecomix, un important groupe de hackers qui a aidé à maintenir une connexion internet en Egypte et dans d'autres pays du Printemps arabe, alors que les gouvernements tentaient de couper toute connexion, a publié en 2012 cinquante-quatre GB de journaux de connexion. D'après Telecomix, ces éléments prouvent que 15 serveurs Blue Coat (Blue Coat SG9000) avaient été installés en Syrie. Ces appareils ont été découverts dans le réseau du fournisseur d'accès Syrian Telecommunications Establishment (STE) [3], propriété de l'État.

Les tentatives de connexion à Youtube, Twitter et Facebook étaient répertoriées et pouvaient potentiellement faire l'objet d'une enquête. Membre de Telecomix, Stephan Urbach a déclaré qu'il existait dans ces données non seulement des historiques de connexion et des enquêtes sur ces connexions, mais également du contenu soumis par les internautes. [4]

L'analyse des journaux de connexion suggère que les proxies de Blue Coat ont été utilisés pour intercepter et analyser du trafic chiffré [5] (https). Toutes les requêtes utilisant le port 443 (dédié au protocole https) à destination des sites web les plus fréquentés de Syrie [6] contenaient plus d'informations que nécessaire. Ces informations sont normalement protégées par une couche de chiffrement censée empêcher n'importe quel proxy de les lire.

"Nous ne souhaitons pas que nos produits soient utilisés par le gouvernement syrien ou par aucun autre pays mis sous embargo par les États-Unis", a déclaré Steve Daheb, vice-président principal de Blue Coat, dans une première tentative d'explication. Selon lui, Blue Coat est "attristée par la souffrance du peuple syrien et les pertes humaines" en Syrie [7].

Dans un rapport du Wall Street Journal [8] paru le 29 octobre 2011, Blue Coat a reconnu que 13 de ses appareils, à l'origine envoyés par un distributeur dubaïote à destination du ministère de la Communication irakien, se sont retrouvés en Syrie. La société a déclaré que ces appareils n'étaient "pas en mesure d'utiliser le service WebPulse" ou "de faire fonctionner la base de données WebFilter", composants importants du dispositif de surveillance fonctionnant en "nuage". Blue Coat a aussi indiqué [7] que les appareils en question "fonctionnaient en toute indépendance" et que la société ne disposait pas d'un "bouton OFF" pour les désactiver à distance. D'après une série de tests menés en juillet 2012 par le Citizen Lab, les équipements livrés par Blue Coat aux autorités syriennes n'interagiraient plus avec les services de cloud de la société.

Autres implications

Comme il l'explique dans un rapport détaillé, le Citizen Lab de l'Université de Toronto a passé la Toile au crible pour repérer des dispositifs Blue Coat à travers le monde [8]. Le rapport montre qu'en Égypte, au Koweït, au Qatar, et en Arabie Saoudite, des systèmes Blue Coat sont utilisés, potentiellement à des fins de censure numérique. Le Citizen Lab a aussi observé que le Bahreïn, la Chine, l'Inde, l'Indonésie, l'Irak, le Kenya, le Koweït, le Liban, la Malaisie, le Nigéria, le Qatar, la Russie, l'Arabie Saoudite, la Corée du Sud, Singa-

2 https://citizenlab.org/wp-content/uploads/2012/07/02-2011-behindbluecoatupdatefromburma.pdf

3 http://reflets.info/opsyria-bluecoat-au-coeur-dattaque-mitm-de-grand-envergure/

4 Liste des sites web ciblés : www.microsoft.com, imo.im, urs.microsoft.com, plusone.google.com, login.live.com, s-static.ak.facebook.com, www.facebook.com, secure.wlxrs.com, apis.google.com, by6.omega.contacts.msn.com, ssl.gstatic.com, www.google.com, mail.google.com, fbcdn-profile-a.akamaihd.net, login.yahoo.com

5 http://siliconangle.com/blog/2011/11/08/when-governments-curtail-freedom-a-tale-of-censorship-huawei-and-blue-coat/

6 http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

7 http://www.bluecoat.com/update-blue-coat-devices-syria

8 https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

pour, la Thaïlande, la Turquie, et le Venezuela ont utilisé des équipements pouvant être exploités pour mettre en place une surveillance et un fichage des internautes [9].

Reporters sans frontières a contacté la société Blue Coat le 7 mars 2013. Dans une réponse datée du 12 mars, la société dit s'assurer que ses produits sont vendus dans le respect des lois encadrant l'export de leurs technologies. L'ensemble des ventes des produits Blue Coat est assuré par des revendeurs lesquels doivent adhérer aux mêmes standards éthiques que Blue Coat. Blue Coat a affirmé que le détournement des technologies au détriment de la liberté d'expression est un problème très sérieux qu'une société ne peut résoudre seule. Au cours de l'année 2013, Blue Coat dit vouloir discuter avec ses actionnaires et avec les sociétés de la même branche afin de trouver des moyens supplémentaires permettant de limiter le détournement de leurs technologies.

GAMMA INTERNATIONAL

Gamma International propose des logiciels espions extrêmement élaborés. Ses logiciels ont été retrouvés notamment au Bahreïn et aux Émirats arabes unis, des pays connus pour malmener les producteurs de l'information. La technologie FinFisher vendue par la société est capable de lire des fichiers encryptés, des emails, et d'enregistrer des appels passés en VoIP. Parmi les cibles de cette surveillance, Ala'a Shehabi, journaliste bahreïnie et maître de conférence à l'université, qui a dû fuir son pays et vit désormais au Royaume-Uni.

Sites : www.finfisher.com,
https://www.gammagroup.com/
Pays d'origine : Royaume-Uni/Allemagne

La société
Gamma International est une filière de Gamma Group, basé au Royaume-Uni. Elle a des bureaux et des filiales au Royaume-Uni - incluant Jersey et Guernesey -, en Allemagne mais aussi en Asie du Sud-Est et au Moyen-Orient [1]. Elle est spécialisée dans la surveillance en ligne comme hors-ligne et propose des formations à la sécurité informatique.

„*Le groupe Gamma, créé en 1990, offre des techniques avancées de surveillance, des solutions de contrôle des communications et des formations aux gouvernements, et propose aussi des conseils aux agences de renseignements gouvernementales et aux forces de l'ordre.*" [2]

Gamma International appartient à Louthean John Alexander Nelson, fils du fondateur du groupe, William Louthean Nelson, et Martin Johannes Münch (à travers Mu Shun Gmbs), plus connu par ses initiales MJM [3]. Gamma International entretient des liens de proximité avec la compagnie allemande Elaman. Ils partagent même une adresse et un numéro de téléphone. Gamma International a confirmé à RSF que Elaman sert de revendeur à la société.

9 http://www.nytimes.com/2013/01/16/business/rights-group-reports-on-abuses-of-surveillance-and-censorship-technology.html?_r=1&

1 https://www.gammagroup.com/default.aspx] http://www.guardian.co.uk/uk/2012/nov/28/offshore-company-directors-military-intelligence

2 https://www.gammagroup.com/companyprofile.aspx

3 http://www.mushun.de/imprint.html, http://buggedplanet.info/index.php?title=NELSON,_LOUTHEAN_JOHN_ALEXANDER http://s3.amazonaws.com/files.posterous.com/temp-2011-03-07/DBEJyIrixEbjnCeshsGDGlGeycClnodEbqkAHAIldczzIJpEpntFGxoxyEGF/Gamma_International_Gesellschafter.png.scaled1000.png?AWSAccessKeyId=AKIAJFZAE65UYRT34AOQ&Expires=1360660710&Signature=5cn38R5mReoxez%2FbneKlJnlI9Bk%3D

Portfolio

Gamma International vend son matériel d'interception exclusivement aux gouvernements et aux services chargés d'appliquer la loi. Son produit FinFisher, livré avec un service d'assistance technique, utilise des logiciels malveillants capables d'infecter des ordinateurs, des téléphones portables, des serveurs, et est considéré comme l'un des plus avancés du marché à ce jour. Un ordinateur ou un smartphone peuvent être infectés à distance par un cheval de Troie, lui-même téléguidé par des agences gouvernementales par l'intermédiaire de serveurs de contrôle. Un ordinateur peut être contaminé via de fausses mises à jour et notifications de logiciels, par des emails corrompus, ou par un accès physique direct. FinFisher offre aussi une technologie qui permet d'infecter tout le parc d'un cybercafé pour en surveiller les usagers. Une fois installé, le cheval de Troie est pratiquement indélogeable. Il n'existe aucun moyen sûr de se prémunir de Finfisher sur une machine infectée.

Les logiciels malveillants de FinFisher sont réputés pour être indétectables par les antivirus standards. Ils permettent d'écouter les conversations sur Skype, lire les chats et les emails chiffrés et même allumer à distance le microphone ou la webcam d'un ordinateur. Avec la technologie FinFisher, il est possible d'avoir accès à des dossiers chiffrés présents sur un disque dur. Gamma fait la publicité de l'étendue des capacités de ses logiciels dans plusieurs vidéos commerciales. [4]

Implication au Bahrein

En juillet 2012, des informations ont couru sur une possible implication de la technologie FinFisher au Bahrein, où la situation est particulèrement difficile pour les acteurs de l'information. Beaucoup ont été arrêtés, emprisonnés et torturés, sur fond de manifestation populaire, qui secouent le pays (Lire la fiche Bahreïn). La dissidente Ala'a Shebabi, actuellement résidante à Londres, a reçu un email infecté. Le trouvant suspect, elle l'a transféré à des experts pour analyse, ce qui a permis la détection de signatures du logiciel FinFisher de Gamma [5].

Reporters sans frontières, leEuropean Centre for Constitutional and Human Rights,Privacy International, leBahrain Centre for Human Rights etBahrain Watch ont saisi l'OCDE, demandant au point de contact national de l'OCDE au Royaume-Uni d'approfondir l'enquête sur l'implication possible au Bahreïn de Gamma. La plainte est toujours en cours.

Martin Münch, responsable du développement chez Gamma, affirme que le Bahreïn a volé une version de démonstration du logiciel, l'a modifié et l'utilise actuellement pour espionner des journalistes et des dissidents. Directeur de recherche chez Privacy International, Eric King commente : *"Intégrer FinFisher dans le réseau d'un pays n'est pas chose facile. Cela requiert un planning et une analyse précis. De ce fait il est fort improbable qu'un pays puisse reconfigurer une version de démonstration FinFisher de son propre chef."* Bahrain Watch a obtenu des preuves que les serveurs de FinFisher basés au Bahreïn reçoivent des mise à jour régulières. Ce qui semble absolument incompatible avec l'hypothèse du vol du logiciel.

Offre au gouvernement égyptien

Durant une fouille effectuée au sein du bureau d'une agence égyptienne de renseignements en 2011, des militants des droits de l'homme ont découvert une proposition de contract assortie d'une offre commerciale de Gamma International pour fournir FinFisher à l'Egypte. L'entreprise a déclaré qu'aucun accord n'avait été conclu.

Autres exemples de pays concernés

Une récente étude de Rapid 7, entreprise de sécurité informatique, a identifié FinSpy, le logiciel serveur assurant le contrôle du programme FinFisher comme étant actif en Australie, en République Tchèque, en Estonie, en Éthiopie, en Indonésie, en Lettonie, en Mongolie, au Qatar, aux Emirats Arabes Unis et aux États-Unis. "Nous avons identifié plusieurs autres pays dans lesquels des serveurs de contrôle-commande géré par FinSpy opéraient," a déclaré le Citizen Lab, l'institut de l'université de Toronto spécialisé dans les problèmes numériques. "Nous avons découvert deux serveurs à Brunei, un au ministère turkmène de la Communication, deux à Singapour, un au Pays-Bas, un nouveau serveur en Indonésie et un au Bahreïn." Toujours selon le Citizen Lab [6], certains de ces serveurs paraissent avoir été mis hors-ligne après que leur existence a été révélée.

Reporters sans frontières a contacté Gamma International en février 2013.

4 http://tinyurl.com/werbungueberwachungI

5 http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html

6 http://www.informationweek.com/security/vulnerabilities/finfisher-mobile-spyware-tracking-politi/240006620

HACKING TEAM

L'entreprise italienne Hacking Team décrit elle même ses technologies comme étant "offensives". La société a été mise en cause pour des ventes au Maroc et aux Émirats arabes unis. Selon la société Hacking Team, le "Remote Control System" qu'elle a développé, dénommé avec modestie DaVinci, est capable de casser le chiffrement utilisé pour les emails, les fichiers et les protocoles VoIP.

Filiales : États-Unis, Singapour
Employés : environ 40
Site web : http://www.hackingteam.it
Siège : Milan, Italie

La société

Basée à Milan, la société Hacking Team propose aux forces de l'ordre des solutions de défense "proactives" sur les six continents. La société emploie environ 40 personnes en Italie et dispose de bureaux à Annapolis (États-Unis) et à Singapour. La société se définit ainsi : *"Chez Hacking Team, nous pensons que combattre le crime doit être facile : nous fournissons dans le monde entier une technologie offensive, efficace et simple d'utilisation, à destination des organismes chargés d'appliquer la loi et des services de renseignements. La technologie doit vous rendre plus fort, pas vous entraver."* [1]

Portfolio

"Le "Remote Control System" est un dispositif furtif d'investigation destiné aux agences gouvernementales en charge de l'application de la loi. (C'est une technologie de sécurité agressive, un logiciel espion, un cheval de Troie ou un bug. C'est un outil de surveillance, un outil d'attaque, un outil de contrôle des terminaux. En d'autres termes, c'est un outil de contrôle des ordinateurs)." [2]

Le "Remote Control System" de Hacking Team, commercialisé sous le nom de "DaVinci", est capable, d'après la société, de casser le chiffrement et de permettre à la police et aux autres services chargés de faire respecter la loi „de surveiller les fichiers et les emails (même ceux utilisant la technologie PGP), les conversations Skype et tous les autres protocoles de VoIP, ainsi que les échanges par messageries instantanées (chats). Ce système rendrait possible la localisation des cibles et l'identification de leurs contacts. Il permettrait également d'activer à distance des caméras et des micros partout dans le monde. Hacking Team prétend que son logiciel est capable de surveiller simultanément des centaines de milliers d'ordinateurs dans un même pays. Ses chevaux de Troie peuvent infecter Windows, Mac, Linux, iOS, Android, Symbian et Blackberry. [3]

"Dans le cadre des communications digitales modernes, le chiffrement est largement utilisé pour protéger les utilisateurs d'une mise sur écoute. ***Malheureusement, le chiffrement empêche aussi les agences gouvernementales et les services de renseignement*** *de contrôler et d'empêcher les attaques et les menaces contre la sécurité de leur pays. Le* ***"Remote Control System"*** *(RCS) permet de* ***contourner ce chiffrement*** *par le biais d'un agent de surveillance installé directement sur le matériel de la cible. Le recueil de preuves sur les machines surveillées est silencieux et la transmission des données collectées vers le serveur du RCS est chiffrée et intraçable. Conçu UNIQUEMENT pour les agences gouvernementales et les services chargés de faire respecter la loi. [Extraits choisis par Reporters sans frontières]"* [4]

Le porte-parole de Hacking Team a indiqué, sans rentrer dans les détails, que la société était en mesure de surveiller la manière dont son logiciel était utilisé par ses clients. [5]

1 http://www.hackingteam.it/index.php/about-us

2 Extrait de la présentation officielle de Hacking Team

3 http://www.hackingteam.it/media/video/HT-DarkSecrets.flv http://www.hackingteam.it/images/stories/RCS2012.pdf

4 http://www.hackingteam.it/index.php/remote-control-system

5 http://www.spiegel.de/netzwelt/netzpolitik/eric-rabe-vom-hacking-team-trifft-auf-den-aktivisten-jacob-appelbaum-a-886744.html

Implications dans des pays sensibles

Hacking Team prétend ne pas vendre ses logiciels aux pays qui violent les droits de l'homme. La société annonce par ailleurs que ses produits sont utilisés dans environ 30 pays sur cinq continents.

"Les logiciels développés par Hacking Team sont vendus uniquement aux agences gouvernementales, et jamais dans des pays inscrits sur listes noires par les États-Unis et les organisations internationales dont l'Union européenne et l'OTAN. Un comité indépendant composé d'experts juridiques analyse chaque opportunité de vente pour s'assurer de leur compatibilité avec notre politique. Les contrats passés avec les acheteurs gouvernementaux définissent des limites d'utilisation de nos logiciels. Nous surveillons l'actualité et les communications publiques comme les blogs et les commentaires Internet pouvant rapporter des abus, et nous enquêtons si c'est nécessaire."

Malgré ces garanties, de nombreux médias et des experts en sécurité informatique ont trouvé des traces de logiciel Hacking Team dans des pays peu respectueux de la démocratie et des droits de l'homme, comme le prouvent les quelques exemples suivants.

Implication au Maroc

Le logiciel de Hacking Team a été identifié sur les ordinateurs des bureaux du site d'information marocain Mamfakinch, quelques jours après que ce média a reçu le Breaking Borders Award 2012 par Global Voices et Google. Un logiciel malveillant y avait été déployé via un document Word, qui prétendait contenir des informations confidentielles importantes.

Contacté par Reporters sans frontières pour commenter la mise en cause de ses logiciels au Maroc, le porte-parole de la société n'a pas nié leur déploiement dans le pays : *"Nous prenons des précautions pour nous assurer que nos logiciels ne sont pas détournés et, le cas échéant, nous menons des enquêtes. Quoiqu'il en soit, nous ne révélons pas les identités de nos clients ou leur localisation." (réponse envoyée par email à Reporters sans frontières).*

Implication aux Émirats arabes unis

Un expert en sécurité, Morgan Marquis-Boire, a examiné des pièces jointes attachées à un email envoyé à Ahmed Mansoor, un blogueur émirati. Elles étaient contaminées. Il y a trouvé de fortes indications suggérant que la source du cheval de Troie provenait de Hacking Team. Ses résultats ont été publiés par le Citizen Lab, un institut de l'Université de Toronto spécialisé dans les questions numériques [6].

6 http://munkschool.utoronto.ca/canadacentre/research/backdoors-are-forever/

TROVICOR

Trovicor est l'un des plus gros fournisseur de solutions légales d'interception dans le monde et prétend équiper plus de 100 pays. La société a été interrogée, notamment lors d'une audience au Parlement européen en 2010, sur son implication en Iran, au Bahreïn ou en Syrie notamment, où des journalistes et des net-citoyens sont régulièrement emprisonnés et torturés grâce à l'utilisation de technologies vendues par des sociétés occidentales.

Anciennement connue sous le nom de "Nokia Siemens Networks" (NSN, jusqu'en 2009) et "Division for Voice and Data Recording" au sein de Siemens AG. Détenue par Johann Preinsberger par l'intermédiaire de la société Ickehorn Asset Management.

Siège : Allemagne, Munich
Filiales connues : Suisse, Dubaï, Islamabad, Kuala Lumpur, Prague
Employés : environ 170
Site web : www.trovicor.com
Portfolio: Monitoring Centre, Lifecycle Management, Intelligence Platform

La société

Créée en 1993 sous le nom de Department for Voice and Data Recording, Trovicor est l'un des premiers fournisseurs au monde d'équipements de surveillance. Cette ancienne division opérationnelle de l'entreprise de technologie allemande Siemens fournit les autorités de plus d'une centaine de pays en centres de surveillance et en matériels d'interception. La société est rattachée en 2007 à une autre structure, Nokia Siemens Networks. En 2009, elle est cédée à une société de gestion [1]. Dénommée Trovicor, la nouvelle entité s'engage à reprendre les contrats de maintenance de Nokia Siemens Network. Elle est le sponsor principal du plus grand salon d'exposition au monde en matière d'équipements de surveillance et de censure, l'ISS World MEA 2013 (Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering) [2]. Dans une audition au Parlement européen, Barry French, un représentant de Nokia Siemens Networks, expliquait [3] que : *"les centres de*

1 http://www.nokiasiemensnetworks.com/news-events/press-room/statements/telecoms-and-human-rights
http://www.nokiasiemensnetworks.com/news-events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights

2 http://www.issworldtraining.com/iss_mea/sponsors2.html http://www.nokiasiemensnetworks.com/news-events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights

3 http://www.nokiasiemensnetworks.com/news-events/press-room/statement-to-the-public-hearing-on-new-information-technologies-and-human-rights

surveillance sont, de notre point de vue, plus inquiétants [que les équipements d'interception légale] et soulèvent des problèmes liés aux droits de l'homme que nous ne sommes pas en mesure de traiter. Notre compétence première n'est pas de travailler avec les organismes d'application de la loi, qui ne sont pas nos clients habituels. Ces organismes pourraient avoir des intérêts à étendre les fonctions des centres de surveillance au-delà des standards de l'interception légale."

De nombreux éléments soutiennent la thèse d'une collaboration entre Trovicor et d'autres sociétés spécialisées dans les technologies de surveillance, qui fourniraient des solutions tels que des chevaux de Troie.
Les solutions clefs en main [de Trovicor] sont basées sur les systèmes innovants développés par la société et sont pensées pour intégrer les solutions tierces les plus performantes, fournissant ainsi une plate-forme flexible pour appréhender les criminels. [4]

Portfolio
Les centres de surveillance de Trovicor sont capables d'intercepter toutes les communications respectant les standards de l'European Telecommunications Standards Institute (ETSI), c'est-à-dire les appels téléphoniques, les envois de messages textuels, les appels en VoIP (comme Skype) ainsi que le trafic internet. L'espionnage de données stockées sur des disques durs n'est en revanche pas possible. Trovicor propose des solutions de traitement massif de grosses quantités de données grâce à une autre solution, Intelligent Platforms. La société met aussi à disposition un programme d'évaluation du réseau et de la structure Internet d'un pays, pour fournir des solutions de surveillance sur mesure ainsi que des formations adaptées aux autorités concernées (LifeCycle Management). Elle assure le cas échéant la maintenance du système et le développement d'options sur le matériel installé [5].

Implication au Bahreïn
Des médias [6] et des organisations de défense des droits de l'homme (lire la fiche pays Bahreïn) rapportent que des centres de surveillance ont été livrés au Bahreïn et ont conduit à l'emprisonnement et à la torture de journalistes et d'activistes. Des sources anonymes chez Trovicor (qui travaillaient précédemment pour Siemens) ont confirmé que des équipements y ont été livrés en 2006 par Siemens. La maintenance a été assurée par NSN puis par Trovicor.

Lors de séances de torture, des communications privées (SMS, e-mails, conversations téléphoniques) ont été présentées à des prisonniers tels qu'Abd al Ghani Khanjhar. Ces éléments ont manifestement été obtenus par le programme d'interception du pays.

Avec le European Centre for Constitutional and Human Rights, Privacy International, le Bahrain Centre for Human Rights et Bahrain Watch, Reporters sans frontières poursuit Trovicor auprès des instances allemandes de l'OCDE, pour qu'une enquête soit menée sur son rôle au Bahreïn.

Implication en Iran
En 2009, Nokia Siemens Network a livré des équipements d'interception de télécommunications aux autorités iraniennes. Lorsque la société a suspendu la vente de ses centres de surveillance, Trovicor a continué d'assurer la maintenance de ceux déjà implantés [7].

Nokia Siemens Network est toujours présente en Iran, où elle fournit une assistance aux réseaux de téléphonie mobile. La société a annoncé fin 2011 qu'elle mettait fin à ses activités sur le territoire de la République islamique [8].

Autres terrains d'implication
Des rapports fournis par des médias ont dénoncé la livraison, en 2000 et en 2008 [9], par Trovicor, de centres de surveillance à destination de la Syrie.
Le Yémen est soupçonné d'avoir acheté des centres de surveillance à Trovicor. En 2010, la société a demandé une protection de sa marque dans le pays, ce qui montre que Trovicor a bien des inérêts au Yémen [10].

Trovicor a une filiale officielle à Kuala Lumpur, en Malaisie. En 2009, la société a demandé une protection de sa marque au sein de l'espace économique malaisien [11].
En Allemagne, Trovicor a fourni des équipements d'interception légale pour la police en Bavière [12].
Reporters sans frontières a contacté la société Trovicor le 8 janvier 2013, sans réponse à ce jour.

4 http://www.issworldtraining.com/iss_mea/sponsors2.html
5 http://trovicor.com/en/communication-monitoring-en.htmlhttp://trovicor.de/en/our-offerings-en/lifecycle-management-en.html http://trovicor.de/images/pdf/release_t01_2013.pdf
6 http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html
7 http://www.belgeler.com/blg/2ztn/nokia-siemens-monitoring-system-used-by-the-iranian-regimehttp://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html
8 http://www.itworld.com/networking/233025/nokia-siemens-scales-down-presence-iran
9 http://www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html
10 http://www.abendblatt.de/politik/deutschland/article2003016/Folterer-in-Bahrain-profitieren-von-deutscher-Ueberwachungstechnik.html (allemand)
11 http://www.intellect-worldwide.com/welcome/documents/egazette/MY_eJournal/2010/25Nov2010-%28Jil.54No.24TMA-No.35%29.pdf
12 http://ted.europa.eu/udl?uri=TED:NOTICE:382568-2010:TEXT:EN:HTML&src=0&tabId=1

ETAT ENNEMI D'INTERNET

BAHREÏN

Internet au Bahreïn

- Population : 1 250 000
- Nombre d'utilisateurs d'internet : 960 000
- Taux de pénétration d'internet : 77%
- Nombre de journalistes emprisonnés : 2
- Nombre de net-citoyens emprisonnés : 1

Le Bahreïn est l'un des pays du Moyen-Orient possédant l'une des meilleures couvertures Internet [1] de la région. Le taux de pénétration d'Internet atteint 77 % de la population. La vitesse de connexion est relativement élevée (entre 512 Ko et plus de 20 Go selon les régions) et le nombre de fournisseurs d'accès à Internet (FAI) - 23 - est très développé [2] au regard de la population (1,25 million d'habitants). Batelco, dirigé par la famille royale, reste de loin le plus important [3].
Depuis le début des révoltes populaires en 2011, Internet s'est révélé un outil remarquable de communication et d'information au Bahreïn. Les activistes bahreinis disposent d'une qualité de réseau pour partager idées et documents, par le biais de médias en ligne, des blogs ou des réseaux sociaux [4]. Selon la dernière étude du Social Media Club, le second semestre de l'année 2012 a vu le nombre d'inscrits sur Twitter progresser de 40%.

Dispositif de surveillance

Si le réseau bahreini est l'un des mieux connectés du Golfe, il est également l'un des plus filtrés et espionnés au monde. La famille royale est représentée dans toutes les administrations du réseau, et dispose d'outils de pointe pour surveiller ses concitoyens. En 2012, le Bahreïn faisait son entrée dans la liste des pays "Ennemis d'Internet" établie par Reporters sans frontières. La situation de la liberté de l'information ne s'est guère améliorée alors que le pays est agité depuis le 14 février 2011 par des contestations populaires qui font écho aux soulèvements en Tunisie et en Egypte.

Une communauté d'activistes organisée mais surveillée

Avec un Internet filtré, nombre de contenus sont en théorie inaccessibles au grand public. Les contenus jugés "pornographiques" sont évidemment dans la ligne de mire mais aussi et surtout les opinions politiques et religieuses qui contreviennent aux vues du régime. S'il existe des moyens de contourner le filtrage, les communications concernant la famille royale, le pouvoir en place ou les minorités chiites sont sévèrement encadrées.

Les activités en ligne des dissidents et acteurs de l'information sont épiées de près et la surveillance se renforce. Selon Reda Al-Fardan, membre de l'ONG BahrainWatch, la communauté d'activistes bahreinis est organisée et très dynamique en ligne, notamment sur les réseaux sociaux, mais également très exposée : "le nombre d'attaques ou de mails contenants des malwares n'a cessé d'augmenter depuis mars 2012".

Des cyberattaques de deux types ont été identifiées :
- l'installation de logiciels malveillants sous forme de pièces jointes aux emails
- l'obtention des adresses IP

Hameçonnage

La propagation de ces logiciels malveillants devient de plus en plus pernicieuse. Selon Reda Al-Fardan : *"les responsables de ces attaques sont de plus en plus intelligents et se servent des arguments tels que les droits de l'homme ou la liberté de la presse"*. Le centre de recherche CitizenLab, relié à l'Université de Toronto, a intercepté

1 http://www.internetworldstats.com/stats5.htm
2 http://www-public.int-evry.fr/~maigron/RIR_Stats/RIPE_Allocations/IPv4/ByNb/BH.html
3 Viva, concurrent principal de Batelco, appartient à la famille royale saoudienne.
4 Voir le dernier rapport de RSF : http://12mars.rsf.org/i/Rapport_Ennemis_Internet_2012.pdf

quelques-uns de ces logiciels et révélé leur nature dans un rapport sur le Bahreïn [5] publié en juillet 2012. Ce rapport montre un exemple de tentative de hameçonnage répandue :

----- Forwarded Message -----
From: Melissa Chan <melissa.aljazeera@gmail.com>
To:
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab

Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.

Please check the attached detailed report along with torture images.

Dans ce cas précis, l'expéditeur semble être Melissa Chan, journaliste d'Al-Jazeera. L'objet du mail fait référence aux mauvais traitements infligés à Nabeel Rajab, actuel directeur du Centre du Bahreïn pour les droits de l'homme incarcéré au Bahreïn. Le rapport du CitizenLab évoque également un logiciel malveillant envoyé pour analyse par l'activiste, journaliste et écrivain bahreinie, Ala'a Shehabi, à Vernon Silver, journaliste de Bloomberg. Il est avéré que l'adresse IP de l'expéditeur de ce logiciel malveillant correspond au siège de Batelco, principal fournisseur d'accès à Internet du pays et propriété de la famille royale.

Piratage de l'adresse IP

Les piratages de comptes Twitter ou Facebook sont monnaie courante au Bahreïn, selon un modus operandi "classique" : des faux comptes sont créés, imitant presque parfaitement les comptes de dissidents. Ces faux comptes diffusent des liens contenant des logiciels malveillants. Si un dissident a la mauvaise idée de cliquer sur ce lien, le logiciel malveillant enregistre l'adresse IP et capture toutes les informations relatives au compte. D'après l'organisation BahrainWatch, l'obtention de l'adresse IP permet par exemple aux autorités de démasquer le dépositaire d'un compte anonyme, car les activistes tweetent très souvent depuis leur téléphone portable sans VPN, ni Tor, ni aucun autre outil d'anonymisation. Une fois l'adresse IP obtenue, il suffit donc de fouiller les fichiers des entreprises de téléphonie mobile. Pour chaque client, elles connaissent l'adresse IP utilisée pour la connexion itinérante. Le réseau de cette personne reçoit à son tour des liens frelatés et ainsi de suite. Selon nos sources, certaines des attaques proviennent directement du gouvernement. Certains dissidents ont été interpellés par le ministère de l'Intérieur juste après avoir cliqué sur ces liens.

5 https://citizenlab.org/wp-content/uploads/2012/08/09-2012-frombahrainwithlove.pdf

Mots de passe requis lors des interrogatoires

Par ailleurs, si nombre de dissidents sont arrêtés au motif qu'ils manifestaient et non en raison de leurs opinions en tant que telles, le rapport de la Bahrain Independent Commission of Inquiry indique que lors des arrestations, il leur a été demandé d'identifier leurs contacts sur Facebook ou Twitter, d'expliquer pourquoi ils adhèrent à de tels groupes, les raisons de tels "like" [6], etc. Preuve d'une surveillance de très près des activités des citoyens sur Internet. Les opposants politiques ne sont d'ailleurs pas les seuls à être épiés sur la toile. Selon BahrainWatch, les loyalistes sont également étroitement surveillés.

Une famille royale omniprésente

Au Bahreïn, la famille royale contrôle toutes les institutions de diffusion, de contrôle et de régulation de l'information sur Internet. Outre le principal fournisseur d'accès à Internet Batelco, les membres de la famille royale sont également à la tête des influentes institutions suivantes :

Information Affairs Authority (IAA) : nom d'usage du ministère de l'Information. Dirigée par le ministre d'État et membre de la famille royale Fawaz bin Mohammed Al Khalifa, l'IAA est régulièrement accusée de censurer la presse au Bahreïn, notamment depuis les manifestations de février 2011 [7]. L'IAA contrôle la Bahrain News Agency et la Bahrain Radio and Television Corporation, organes officiels du gouvernement bahreini, et surveille le seul journal indépendant du pays, Al-Wasat [8], et les journalistes étrangers résidant dans le pays, ou souhaitant s'y rendre en reportage.

Central of Informatics and Communication Organization (CIO) : Dirigé par un membre de la famille royale, Sheikh Salman Mohammed Al-Khalifa, le CIO gère le réseau Internet bahreini, les systèmes et leurs données. Créé à l'origine pour être une base de données personnelles des citoyens, le CIO a été doté de pouvoirs nettement plus étendus par décret du roi [9]. Il a désormais toute autorité sur les FAI, y compris celle de supprimer leur licence à tout moment. Il peut également accéder et contrôler l'ensemble de leur trafic. Le CIO peut croiser les données d'identification et de navigation des citoyens, sans aucun

6 http://files.bici.org.bh/BICIreportEN.pdf p.358
7 http://uncut.indexoncensorship.org/2012/01/bahrains-information-affairs-authority-censorshi/
8 http://www.bna.bh/portal/en/news/536417
9 http://www.bna.bh/portal/en/news/494535?date=2012-03-2

contrôle d'une autorité indépendante. Au CIO se situe la base de la surveillance du réseau. Selon CitizenLab, les locaux du CIO renferment un dispositif DPI (voir plus bas) offrant la possibilité d'intercepter les communications de tous les citoyens. Depuis 2012, le CIO est sous l'autorité du ministère de l'Intérieur, dirigé par un membre de la famille royale, Rashid bin Abdulla.

Ministère de l'Intérieur (MOI) : En plus du contrôle direct qu'il exerce sur le CIO, le MOI a créé une autre entité de lutte contre le cybercrime : la Direction de la lutte contre la corruption et de la sécurité électronique et économique). Créée en septembre 2012, cette unité appelle les citoyens à la dénonciation de toute "campagne de diffamation en ligne ternissant la réputation des symboles nationaux et des personnalités publiques de premier plan". Souhaitant lutter contre le "crime de diffamation", particulièrement sur les réseaux sociaux, cette initiative a conduit à l'arrestation, moins d'un mois après sa création, de quatre personnes au motif de "mauvais usage des réseaux sociaux [10] ".

Telecommunications Regulatory Authority (TRA) : dirigée par Mohamed Ahmed Al-Amer et le Sheikh Hamed bin Mohamed bin Hamed Al-Khalifa, la TRA est à l'origine de la fermeture en 2010 et 2011 des sites de VoIP comme NonoTalk et Seefcall, jugés illégaux [11] au Bahreïn. La TRA s'assure que les fournisseurs d'accès à Internet du pays actualisent leurs listes noires sur ordre du CIO.

National Security Apparatus : la NSA, agence de renseignements dirigée par Adel bin Khalifa bin Hamad Al-Fadhel, surveille activement les dissidents et les opposants politiques, notamment par le biais de leurs profils sur les réseaux sociaux. Depuis 2010, la NSA a été dotée de pouvoirs plus importants [12] et est impliquée dans de nombreuses affaires de tortures [13], notamment celles de Karim Fakhrawi12, fondateur et membre du directoire d'Al-Wasat et du blogueur Zakariya Rashid Hassan [14].

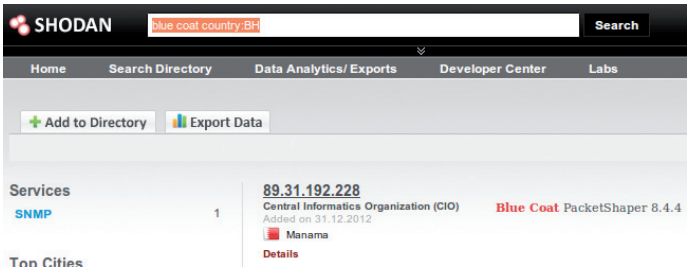
E-government Authority : dans sa volonté de numériser toutes ses activités, le gouvernement bahreini a créé l'EGA, dont le but à peine voilé est de récupérer le plus de données possibles sur les citoyens du Royaume. À l'initiative du CIO, (alors dirigé par Sheikh Ahmed Bin Atteyatallah Al-Khalifa), l'EGA a lancé une vaste campagne d'identification en ligne (National Authentication Framework) afin de "faciliter l'accès aux services" aux utilisateurs d'Internet. Compte tenu de l'omniprésence de la famille royale dans les structures de gestion des télécommunications et de surveillance, une telle initiative apparaît particulièrement inquiétante.

Un arsenal technologique de surveillance

Le Bahreïn semble s'être doté des tout derniers logiciels et matériels de surveillance sur le marché. En pointe sur la technologie, le gouvernement bahreini peut surveiller le réseau à tous les niveaux.

- Blue Coat : dans son rapport Planet Blue Coat, CitizenLab a décelé un outil de Deep Packet Inspection (DPI) produit par la société Blue Coat appelé PacketShaper. Cet outil permet de reconnaître et d'analyser le trafic Internet afin de bloquer l'accès à certains contenus. Selon l'un des rédacteurs de ce rapport, le matériel Blue Coat au Bahreïn est installé dans les locaux du CIO, qui gère le réseau de tout le pays.

- Gamma/FinFisher : il a également été démontré par BahrainWatch et CitizenLab qu'un produit de la firme Gamma était utilisé au Bahreïn : FinSpy, de la suite FinFisher. Les produits FinFishers peuvent potentiellement surveiller tous les ordinateurs, contrôler les webcams, enregistrer toutes les frappes au clavier, les conversations Skype et même les conversations sur les mobiles [15].



10 http://www.indexoncensorship.org/tag/cybercrime/

11 http://www.tra.org.bh/en/pdf/Nonotalk_order_press_statment_en.pdf

12 http://www.bahrainrights.org/en/node/3265

13 http://files.bici.org.bh/BICIreportEN.pdf pp. 243 à 245

14 http://fr.rsf.org/bahrein-le-fondateur-du-journal-al-wasat-18-04-2011,40036.html

15 http://www.bloomberg.com/news/2012-08-29/spyware-matching-finfisher-can-take-over-iphone-and-blackberry.html

Gamma se défend en annonçant que l'un de ses produits FinSpy a été volé lors d'une démonstration [16] et utilisé au Bahreïn. S'il apparaît pour le moins étonnant qu'une entreprise spécialisée dans la sécurité informatique comme Gamma ait réussi la performance de se faire voler un de ses propres produits de sécurité lors d'une démonstration, il est encore plus étonnant de constater que les produits FinFisher trouvés au Bahreïn par CitizenLab ont été mis à jour [17]. En effet, selon Bill Marczak, membre de BahrainWatch et rédacteur du rapport de CitizenLab sur le Bahreïn, les versions de FinSpy découvertes au Bahreïn en mars 2012 étaient des modèles FinSpy 4.01 alors que plus tôt, un modèle 4.00 avait été identifié16.

- Trovicor : selon nos sources, le Bahreïn possède également sur son territoire des produits de la société Trovicor depuis la fin des années 1990. Comme FinFisher, les produits Trovicor permettent la surveillance des conversations sur Internet ou téléphones portables et des SMS. Par le passé, d'autres entreprises, comme Nokia Siemens Networks, ont déjà été sommées de cesser la vente de leurs produits de fichage au Bahreïn [18]. NSN, dont le centre de données a été racheté par... Trovicor, vendait effectivement des produits de surveillance favorisant les arrestations et la torture des opposants politiques.

Le logiciel SmartFilter, de la société américaine McAfee, était également utilisé conjointement aux outils DPI jusqu'en 2011 [19].

Principales violations de la liberté de l'information

Depuis trois ans, avant même le début du mouvement de contestation populaire dans la mouvance des printemps arabes, Reporters sans frontières note une sévère recrudescence des violations de la liberté de l'information au Bahreïn. Le Bahreïn offre l'exemple d'une répression réussie grâce au blackout de l'information rendu possible par un impressionnant arsenal de mesures répressives accompagnées d'une généralisation de la surveillance : mise à l'écart des médias étrangers ; harcèlement des défenseurs des droits de l'homme ; arrestations de blogueurs et net-citoyens ; poursuites judiciaires et campagne de diffamation contre des militants de la liberté d'expression.

Plusieurs journalistes, net-citoyens et membres d'organisations de promotion des droits de l'homme sont actuellement en prison ou risquent des peines de prison pour un tweet, un article, une photo, un statut Facebook.

Le rôle de ces acteurs de l'information est d'autant plus primordial que nombre de journalistes étrangers ne parviennent pas à entrer sur le territoire bahreini. Ainsi en fin d'année 2012 Asem Al-Ghamedi d'*Al-Jazeera* [20], Nicholas Kristof du New-York Times ainsi qu'un correspondant du Frankfurter Allgemeine Zeitung [21] se sont vu interdire l'accès au pays ; les autorités prétextent parfois des vices de procédure dans l'obtention de visas [22].

Au 1er mars 2013, sont détenus ou risquent une peine de prison

Dr Abduljalil Al-Singace, défenseur des droits de l'homme et blogueur fait partie des vingt-et-un suspects condamnés, le 22 juin 2011, à de très lourdes peines de prison pour "appartenance à des organisations terroristes" et "tentatives de renversement du régime". Tous les recours étant désormais épuisés, il purge une peine d'emprisonnement à perpétuité.

Ali Abdulemam, jugé par contumace dans cette même affaire, a, lui, écopé d'une peine de quinze ans de prison. Suite à la publication du rapport Bassiouni, les autorités judiciaires bahreïnies ont ordonné, le 30 avril 2012, la tenue d'un nouveau procès, au civil cette fois-ci, devant la Cour d'appel.

Ahmed Humaidan, photojournaliste, lauréat de 143 prix internationaux [23], est détenu depuis le 29 décembre 2012 pour avoir documenté des violations des droits de l'homme. Il a déclaré à sa famille avoir fait l'objet de mauvais traitements, voire de torture depuis son placement en détention. Il est accusé d'avoir participé à l'attaque d'un commissariat en 2011, alors même qu'il était sur place pour couvrir l'incident.

Hassan Salman Al-Ma'atooq : photographe en prison depuis mars 2011, il est accusé notamment de "fabrication d'images de blessés et diffusion de fausses images et fausses informations".

16 http://www.guardian.co.uk/world/2013/feb/02/uk-firm-spyware-bahrain

17 http://bahrainwatch.org/blog/2013/02/06/uk-spyware-in-bahrain-companys-denials-called-into-question/

18 http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

19 http://online.wsj.com/article/SB10001424052748704438104576219190417124226.html

20 http://thepeninsulaqatar.com/qatar/219431-al-jazeera-journalist-denied-entry-bahrain-rejects-charge.html

21 http://bahrainwatch.org/access/

22 http://byshr.org/?p=942

23 http://www.bahrainrights.org/en/node/5586

Parmi les défenseurs des droits de l'homme et acteurs de l'information également victimes de la répression, Nabeel Rajab, président du Centre du Bahreïn pour les droits de l'homme (BCHR), et Said Yousif Al-Muhafdha, vice-président par intérim du Centre du BCHR [24].

Les net-citoyens victimes de violences et d'actes de torture

Le citoyen-journaliste Ahmed Ismail Hussain a été tué alors qu'il couvrait une manifestation pacifique à Salmabad le 31 mars 2012. Les coupables n'ont toujours pas été arrêtés. En revanche, il apparaît que **Karim Fakhrawi,** fondateur et membre du directoire d'Al-Wasat et **Zakariya Rashid Hassan,** blogueur, sont tous deux décédés en détention, après avoir subi la torture des services gouvernementaux. Aucune des personnes impliquées dans leur mort n'a été inquiétée par la justice bahreïnie.

Reporters sans frontières condamne ces dénis de justice. A la fin de l'année 2012, deux sinistres exemples de mascarade judiciaire ont une nouvelle fois montré le sort réservé aux journalistes :

la condamnation de la journaliste Reem Khalifa, accusée à tort d'avoir agressé trois médecins lors d'une conférence de presse en juillet 2011 alors que l'inverse s'était produit : elle avait été agressée.

la décision du tribunal de grande instance d'innocenter le lieutenant Sarah Al-Moosa, poursuivie pour 'torture' sur la journaliste Nazeeha Saeed. Suite à ce jugement, Reporters sans frontières, a d'ailleurs saisi, le 23 octobre 2012, le Rapporteur spécial des Nations unies sur l'indépendance des juges et des avocats [25] sur la question de l'impunité dont bénéficient les auteurs de violences à l'égard des journalistes au Bahreïn.

Quelques solutions techniques

Les logiciels espion sont largement utilisés au Bahrein. La suite Fin fisher n'est que très rarement détectée par les anti virus. La seule manière efficace de se prémunir contre ces logiciels est de prendre des mesures de précautions efficaces en amont afin déviter l'infection de son ordinateur ou téléphone portable :

N'installer aucun logiciel reçu par email.

N'installer aucun logiciel exceptés ceux récupérés sur un site en https. Les certificats garantissant l'identité d'un site https, le risque d'usurpation d'identité (phishing) est réduit.

N'installer aucun logiciel provenant d'une source qui ne vous est pas familière, même si l'installation est recommandée par une fenêtre surgissante.

Faire systématiquement les mises à jour de votre système d'exploitation et des logiciels qui y sont installés. Les mises à jour comblent souvent des failles de sécurité

Ne pas utiliser Internet Explorer pour surfer. Ce navigateur étant parmi les plus utilisés, il est la cible des attaques de pirates informatiques. Préférez lui Firefox ou Chrome.

L'un des autres enjeux en matière de sécurité est la protection de l'anonymat en ligne. De nombreux dissidents qui twittaient de manière anonyme ont été interpellés après avoir cliqué sur un lien redirigeant vers une page malveillante destinée à récupérer les adresse IP afin de récupérer l'identité des blogueurs anonymes auprès des fournisseurs d'accès. L'utilisation d'un VPN ou de Tor permet de se prémunir de ce type de danger. type de situations.

De nombreux fournisseurs de solutions VPN, tels que Astrill VPN, Pure VPN et HMA par exemple.

Le Guardian Project propose un ensemble de logiciels à installer qui permettent de préserver son anonymat et sa vie privée lors de l'utilisation d'un téléphone Androïd et notamment Orbot, une version de Tor pour téléphones portables.

L'ONG Access Now a publié un guide pratique sur la protection des données et des communications à destination des populations du moyen-orient avec une partie tout particulièrement dédiée aux téléphones mobiles.

Enfin, il existe des système d'exploitation conçus pour la protection de l'anonymat de son utilisateur. Tails est un système qui permet d'utiliser Internet de manière anonyme quasiment sur n'importe quel ordinateur sans laisser aucune trace des actions effectuées.

24 http://fr.rsf.org/bahrein-nabeel-rajab-a-nouveau-emprisonne-10-07-2012,43003.html

25 http://fr.rsf.org/bahrein-denis-de-justice-et-condamnations-14-11-2012,43677.html

VIETNAM

Confrontés à un dilemme courant dans les pays autoritaires, les dirigeants vietnamiens sont tiraillés entre la volonté d'un développement économique favorisé par les nouvelles technologies [1] et la peur de l'instabilité politique que ces dernières peuvent engendrer.

Internet au Vietnam

- Population : 91 500 000
- Nombre d'utilisateurs d'internet : 31 000 000
- Taux de pénétration d'internet : 33,9%
- Journalistes emprisonnés : 2
- Net-citoyens emprisonnés : 31

Sources : [2]

État du réseau

Connecté depuis la fin des années 90, le pays s'est doté d'infrastructures et d'institutions au milieu des années 2000. La création du Comité national de pilotage pour les nouvelles technologies d'information et de communication (TIC) et le lancement du Plan national pour le développement des TIC [3] en 2005 ont favorisé le développement d'Internet dans le pays. Cette expansion du réseau coïncide avec l'éclosion des blogs et des cyber-cafés et l'apparition d'outils de surveillance et de contrôle du Net.

Aujourd'hui, le Parti communiste vietnamien (PCV) affiche ses ambitions sur le terrain des télécommunications, un marché très dynamique au Vietnam [4]. Les internautes sont de plus en plus nombreux : un habitant sur sur trois est connecté. À Hanoi et Hô-Chi-Minh-Ville, 95% des 15-22 ans ont accès Internet [5]. La jeunesse de la population vietnamienne et l'urbanisation à venir du pays laissent présager d'une explosion du nombre d'internautes dans les prochaines années.

Médiocre qualité et vitesse du réseau Internet

Malgré tous ces facteurs, le réseau Internet vietnamien "*ne décolle pas*". Sa qualité et sa vitesse sont en dessous de celles des autres pays d'Asie. Selon le rapport Akamai 2012 sur le réseau Internet mondial, le Vietnam dispose d'une vitesse de connexion de 1,25 Mbps au troisième trimestre 2012, qui le place derrière la Thaïlande ou la Malaisie [6] et bien en dessous de la moyenne internationale de 2,3 Mbps. La vitesse de connexion a même baissé depuis le début de l'année 2012. La raison est simple : le Parti limite volontairement la vitesse du réseau, par l'intermédiaire des fournisseurs d'accès à internet (FAI) qu'il contrôle.

Des fournisseurs d'accès à Internet aux mains du Parti

La plupart des seize fournisseurs d'accès est contrôlée directement ou indirectement par le Parti communiste [7]. Le leader, Viet Nam Posts and Telecommunications (VNPT), qui représente 74% du marché, appartient à l'État, tout comme VietTel (propriété de l'armée populaire vietnamienne). FPT Telecom est une entreprise privée mais doit rendre des comptes au Parti et est dépendante de la bande passante octroyée par les leaders du marché.

Il existe une distinction entre fournisseurs d'accès qui permettent aux particuliers et aux entreprises d'accéder à Internet et les Points d'échange Internet (IXP), qui octroient de la bande passante aux FAI. Selon le droit vietnamien, si les premiers peuvent être des sociétés de droit privé, les seconds sont obligatoirement des entreprises d'État [8]. Ce système permet aux autorités de décider des contenus accessibles, par le biais d'entreprises qu'elles possèdent ou à travers les Points d'échange Internet.

Dispositif de surveillance

Les fournisseurs d'accès à Internet sont les premiers outils de contrôle et de surveillance. Ils bloquent l'accès aux sites jugés non conformes par le Régime. Ils utilisent la technique de blocage DNS (Domain Name Server) qui permet de supprimer l'accès à un site en fonction du nom de domaine utilisé. Le blocage DNS permet de bloquer l'ensemble d'un site mais pas une page en particulier. Chaque fournisseur à la liberté de supprimer des contenus sans avoir à se concerter avec les autres acteurs du marché.

1 Whitebook "Viet Nam Information and Communication Technolology" - 2011. p.5
2 http://www.itu.int, http://data.worldbank.org et http://mic.gov.vn/
3 http://opennet.net/research/profiles/vietnam#footnoteref2_g3yqrfg
4 Ibid p.49
5 http://www.economist.com/blogs/banyan/2012/08/internet-freedom-vietnam
6 http://english.vietnamnet.vn/en/science-technology/22586/internet-speed-unimproved-owing-to-the-lack-of-content.html
7 http://english.mic.gov.vn/Statistics/staticstics_open/Trang/operators.aspx
8 http://www.business.gov.vn/assets/fbbc1d48c42d4f36a161a8a3d8749744.pdf art. 13.

À titre d'exemple, Facebook est censuré par VNPT alors que les deux autres fournisseurs principaux en autorisent l'accès. Le centre de recherche OpenNet Initiative a établi en 2012 un panorama des sites censurés au Vietnam. Parmi les contenus bloqués, on trouve des sites de journaux et des blogs (vietnamiens et étrangers), des contenus d'opposition politique, de droits de l'homme etc.

Certains blogueurs utilisent des logiciels de contournement (proxy, VPN, Tor) pour mettre en échec ce blocage. Ces outils ne sont pas toujours fiables. Les autorités ont la capacité de bloquer les ports destinés au transport de données chiffrées et de rendre inutilisable ces solutions. Les blogueurs surveillés par le régime subissent fréquemment des attaques Man-in-the-Middle dont le but est d'intercepter les données envoyées lors de l'accès à des sites web sécurisés (https). Ce type d'attaque ne peut être effectué que par les administrateurs du réseau vietnamien, à savoir les fournisseurs d'accès Internet. Il n'est pas rare que les mots de passes soient piratés et que les connexions soient ralenties les jours d'arrestation ou de procès de dissidents.

Abonnement et données personnelles sous contrôle

Pour souscrire un abonnement à une ligne fixe (téléphone et internet), il faut fournir quantité de documents contenant les données personnelles des citoyens : nom, prénom, date de naissance, numéro de téléphone, fonction, employeur et justificatif de domicile. Au Vietnam, le seul justificatif de domicile qui soit reconnu est le ***hộ khẩu***, document délivré par la police qui permet le contrôle de la population. Sans ***hộ khẩu***, il n'est pas possible de louer un logement, de trouver un travail officiel, passer le permis ou s'abonner à internet. Trois pays dans le monde utilisent ce genre de document : la Chine, la Corée du Nord et le Vietnam.

La téléphonie mobile sous surveillance

Les principaux fournisseurs d'accès à internet sont également fournisseurs de téléphonie, fixe ou mobile. Les recettes approximatives du marché de la téléphonie mobile étaient évaluées en 2012 à 500 millions [9]. Le Vietnam recense 119 millions d'abonnés pour 91 millions d'habitants ! [10] Trois grands opérateurs mobiles [11], dont VietTel se partagent 90% de cet immense marché. Tous sont contrôlés par l'État.

Selon un rapport de Freedom House daté de juillet 2012, 91% des personnes interrogées accèdent à Internet via leur terminal mobile. Le surf Internet sur mobile est peu sécurisé et peut être facilement surveillé. Surtout lorsque l'État possède les opérateurs. D'après ce rapport, l'État écoute les conversations et retrace les appels de citoyens sur liste noire, souvent considérés comme "activistes" ou "réactionnaires". L'accès au téléphone ou à internet de certains d'entre eux a été coupé [12].

Un arsenal juridique liberticide

La loi sur la presse [13] de 1989 est claire sur le rôle que doit jouer la presse au Vietnam. "*La presse dans la République socialiste du Vietnam englobe tous les médias indispensables à la vie sociale, elle constitue la voix du Parti, des organisations publiques et sociales ainsi qu'une plateforme pour l'expression de la volonté du peuple.*" Cette législation conditionne les domaines de la presse traditionnelle et les publications sur Internet. Ainsi, la liberté de la presse, la liberté d'expression et le droit à l'information ont été consacrés dans l'article 69 de la Constitution vietnamienne de 1992. Dans les faits, ces libertés passent à la trappe dès qu'elles contreviennent à la ligne définie par le parti communiste.

Dans la droite ligne de la loi de 1989, le décret 55/2001/ND-CP d'aout 2001 pose les bases d'un Internet surveillé par le Parti. L'article 6 précise que les informations publiées sur Internet doivent être conformes à la loi sur la presse ; l'article 8 de ce décret énonce clairement que "le contrôle des informations sur Internet doit être effectué par les agences d'État compétentes" ; l'article 11 interdit l'utilisation d'internet pour s'opposer à la république socialiste du Vietnam. Ce décret indique également que les points d'échanges d'internet (voir plus haut) ne peuvent être détenus que par l'État (article 13). En 2003, un nouveau décret (92/2003/QD-BBCVT) interdit "l'envoi ou la réception de matériel anti-gouvernemental". Ce décret oblige également les propriétaires de sites à s'enregistrer auprès du Vietnam internet network information center, lié au ministère de l'Information et de la Communication. Depuis juin 2006 (décret 56/2006/ND-CP), les journalistes et blogueurs sont tenus de respecter la ligne révolutionnaire sous peine de se voir accuser de "*disséminer une idéologie réactionnaire*" ou de "*propagande contre la Répu-*

9 Rapport Freedom House de juillet 2012 : Safety on the Line-Exposing the myth of mobile communication security p. 148 http://www.freedomhouse.org/sites/default/files/Safety%20on%20the%20Line%20vFINAL.pdf

10 http://www.itu.int/ITU-D/ict/statistics/

11 http://mic.gov.vn/Attach%20file/sachtrang/sachtrang2011.pdf p.51

12 Rapport Freedom House de juillet 2012 : Safety on the Line-Exposing the myth of mobile communication security p. 148 http://www.freedomhouse.org/sites/default/files/Safety%20on%20the%20Line%20vFINAL.pdf

13 http://www.cov.gov.vn/cbqen/index.php?option=com_content&view=article&id=606&Itemid=75

blique socialiste du Vietnam", un délit passible de 3 à 20 ans de prison et d'une amende de 2 000 dollars.
Les cyber-cafés, très populaires au Vietnam, font l'objet d'une réglementation stricte. Une décision du Comité du peuple d'Hanoï de 2010 [14] oblige leurs propriétaires à installer du matériel de surveillance fourni par le gouvernement permettant de tracer les activités sur internet et de bloquer l'accès à certains sites. Les internautes doivent fournir leur carte d'identité et les cyber cafés ont l'obligation de conserver ces données en cas de contrôle par les autorités. Selon nos sources, les gérants de cyber-cafés ferment souvent les yeux sur ces obligations pour des raisons économiques. Les clients changent en effet d'établissement lorsqu'il leur est demandé leur carte d'identité. Les cyber-cafés sont cependant tenus de garder tous les historiques de navigation.

En avril 2012, Reporters sans frontières a dénoncé le dangereux projet de décret "sur le management, la provision et l'utilisation de services internet et de contenus d'information en ligne". Censé remplacer un décret de 2008 (lui même amendement du décret de 2001), ce projet a pour ambition

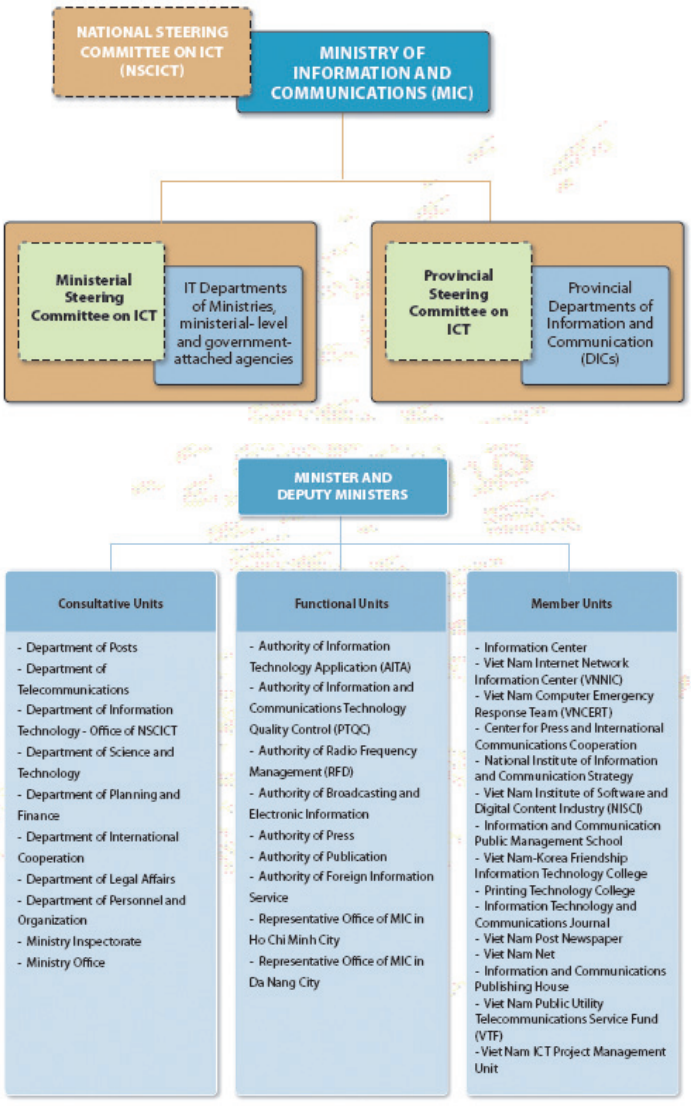
- de supprimer l'expression anonyme sur Internet. Il sera désormais "strictement interdit" aux net-citoyens d'utiliser des données fictives ou de masquer leurs données.
- d'interdire les faux noms sur les réseaux sociaux
- de demander aux administrateurs de sites de dénoncer les activités illégales aux autorités.
- d'obliger les blogueurs à signer sous leurs vrais noms (ces derniers se servent souvent de noms d'emprunt pour tenter d'échapper à la surveillance)
- de demander aux entreprises étrangères de localiser leurs centres de données au Vietnam (et donc d'autoriser le Parti à y accéder).
- d'obliger les entreprises étrangères à fournir les informations personnelles de leurs utilisateurs (nom, prénom adresse) et de coopérer avec les agences gouvernementales [15].

Un contrôle au cœur des institutions

Les décisions relatives à la surveillance d'Internet émanent principalement des ministères de l'Information (MIC) et des communications et de la Sécurité publique (MSP).

Ministère de l'Information et de la Communication

Le MIC dirige les principaux fournisseurs d'accès à internet, le Vietnam Internet Network Information Center, et publie la plupart des décrets relatifs à Internet. Ce ministère travaille de pair avec le Comité national de pilotage pour les nouvelles technologies d'information et de communication, présidé directement par le Premier ministre [16].



Source : White Book 2011 Viet Nam Information and Communication Technology

14 http://www.fidh.org/IMG/pdf/bloggers_report_in_english.pdf p.9

15 http://english.vietnamnet.vn/en/science-technology/23242/new-internet-draft-decree-favors-foreign-businesses.html

16 http://www.action.vn/news/hot-news/594-prime-minister-will-be-the-chairman-of-the-national-ict-committee

Ministère de la Sécurité publique

Ce ministère gère davantage la législation et les sanctions à l'encontre des publications jugées réactionnaires que les problématiques "techniques" liées à la surveillance du réseau. Toutefois, il dirige la cyber-police Công An **Mạng** (CAM), fondée initialement pour lutter contre la cyber-criminalité, comme les fraudes de cartes de crédit, hacking etc. Mais cette police dispose aussi de toute latitude pour faire fermer les sites ou blogs gênants et en arrêter les auteurs. Le Lieutenant Col. Đinh **Hữu** Tân, chef du Bureau de la "Sécurité politique interne" à Hanoï estime que le rôle de cette police est de "surveiller les contenus Internet de toute forme, toutes les publications, incluant les articles de presse, les blogs ou les commentaires." [17]

Si la surveillance d'Internet est officielle, les effectifs, moyens et méthodes de cette cyber-police restent volontairement inconnus.

Cyber armée

Malgré les lois et les institutions relatives à la surveillance et la censure du net, et la forte répression exercée à l'encontre des acteurs de l'information, la Toile vietnamienne fait preuve d'une vitalité rare. Les blogs politiques et sociaux et les commentaires contestaires y fleurissent. Pour les contenir, les autorités font appel à des cyber-soldats, dévoués à la cause et entendant lutter contre "les propos anti-patriotiques et réactionnaires". La cyber armée n'est pas officiellement un organe gouvernemental, même si les autorités de Ho Chi Minh-Ville ont fait état de «pigistes de l'opinion sociale» [18]. "Red guards" ou "cyber-espions", la population ne connaît pas leur identité mais on estime qu'ils sont plus de quatre-vingt mille dans tout le pays. Sur le modèle chinois, cette milice conduit la propagande du régime et dénonce les activistes, blogueurs et net-citoyens aux autorités. Un millier [19] de cyber-policiers officiellement adoubés par le gouvernement ont pour but d'infiltrer les terrains privilégiés des acteurs de l'information : réseaux sociaux et blogs [20].

Principales violations de la liberté d'information

Phénomène provoquant autant d'intérêt pour les internautes que de craintes pour le régime, le blog est la première cible des autorités. Huynh Ngoc Chenh (lauréat du Prix du net-citoyen 2013) résume ainsi la situation : "*Toutes les communications sont contrôlées par l'État. Les opinions opposées à l'État ne sont pas rendues publiques. La liberté d'expression est presque inexistante au Vietnam. Donc beaucoup de gens se servent de blogs pour diffuser leurs propres opinions. Mais ces blogs sont fermés par le gouvernement. Et de nombreux blogueurs sont arrêtés. ils ont été harcelés, ainsi que leurs familles. Ils ont reçu des menaces et subi des pressions du gouvernement*". Le blog représente certes un formidable espace d'expression, mais également une exposition aux lourdes sanctions.

En septembre 2012, le décret 7169/VPCP-NC a ciblé directement trois des blogs les plus influents au Vietnam [21]: Danlambao, Quanlambao et Biendong. Leurs auteurs, qui écrivent tous sous pseudonymes, risquent de lourdes peines de prison si le Parti découvre leur véritable identité. L'anonymat est très répandu dans la blogosphère vietnamienne. Le Parti ne se décourage pas pour autant et utilise les outils de surveillance à sa disposition pour découvrir l'identité de certains blogueurs. Ceux-ci risquent de lourdes sanctions si leur identité est découverte.

Ce fut le cas de **Le Nguyen Sang et Huynh Nguyen Dao** en 2006. Alors qu'ils signaient tous deux leurs articles sous pseudonymes (Nguyen Hai Son ou Nguyen Hoang Long), ils ont été identifiés par la cyber-police et condamnés respectivement à quatre et deux ans et demi de prison. Tran Huynh Duy Thuc en 2009 et **Lu Van Bay** en 2011 ont également été arrêtés alors qu'ils signaient leurs articles sous de faux noms. Le premier purge actuellement une peine de seize ans de prison. Lu Van Bay, qui utilisait quatre pseudonymes différents a lui écopé de quatre ans. Le blogueur Panh Thanh Hai et l'écrivain **Pham Chi Dung** (ancien membre du comité du peuple de Ho-Chi-Minh-Ville, qui a ensuite collaboré avec des sites "non autorisés", comme Phiatruoc ou Quanlambao) ont été arrêtés de la même manière. Ils signaient également leurs articles de pseudonymes.

17 http://www.fidh.org/IMG/pdf/bloggers_report_in_english.pdf

18 http://fr.canoe.ca/techno/internet/archives/2013/01/20130118-100258.html

19 http://techpresident.com/news/wegov/23377/vietnams-government-hired-propaganda-bloggers?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+techpres+%28techPresident%29

20 http://www.bbc.co.uk/news/world-asia-20982985

21 http://finance.yahoo.com/news/under-fire-vietnamese-blogger-vows-dissent-093346513.html

La surveillance des acteurs de l'information est constante. Que ça soit la filature ou l'intimidation [22] pour ceux dont l'identité est connue ou les tentatives de hameçonnage[b] et l'espionnage informatique pour les blogueurs choisissant un nom d'emprunt. L'un de ces acteurs de l'information, qui a purgé une peine de prison et souhaite garder l'anonymat, a expliqué à Reporters sans frontières comment il avait été arrêté, alors qu'il écrivait sous pseudonyme. "*En prison, ils m'ont montré les articles que j'avais écrit, signés avec un nom d'emprunt, les e-mails que j'avais envoyé à des collègues et même mes conversations téléphoniques*". Son cas n'est pas isolé. Et pour connaître ces informations, la cyber-police utilise toutes les méthodes possibles : attaques Man-in-the-middle pour récupérer les mots de passe, cyber-attaques, espionnage des téléphones mobiles etc. Outre leur identité, la cyber-police tente également d'identifier les réseaux des blogueurs.

Les motifs sont toujours les mêmes : "*coopération avec des organisations réactionnaires basées à l'étranger*", "*tentative de renversement du régime*" ou "*propagande contre l'État*". Les accusations de corruption ou de fraude fiscale sont aussi régulièrement avancés à l'encontre de journalistes et de blogueurs. Comme ce fut le cas en 2008 pour le célèbre blogueur Dieu Cay, condamné à dix ans de prison. Cette chasse aux sorcières touche à la fois les blogs "individuels" comme ceux de Nguyen Van Dai, Pham Thanh Nghien, Le Cong Dinh, Dinh Dang Dinh, J.B Nguyen Huu Vinh, Nguoi Buon Gio, Nguyen Quang Lap etc. ou collectifs, comme BachDang, Quanlambao, Bauxite Viet Nam, Dong Chua Cuu The, Nu Vuong Cong Ly. La liste est encore longue et le bilan s'alourdit chaque année. Le 9 janvier 2013, quatorze militants, blogueurs et net-journalistes ont été condamnés à des peines allant de trois à treize ans de prison. Accusés, en vertu des clauses 1 et 2 de l'article 79 du code pénal, de "*participation à une tentative de renversement du gouvernement*" ou "*organisation de renversement du gouvernement*", ils représentent une peine cumulée de 113 ans de prison.

Cette surveillance de tous les instants a un impact sur l'autocensure des acteurs de l'information, dont les familles subissent les pressions du gouvernement. Malgré tout, la toile vietnamienne reste très active. Car le Parti ne peut actuellement pas surveiller la totalité de la Toile, ni empêcher l'éclosion des blogs. Certains blogueurs utilisent des outils de contournement de la surveillance, comme les proxies[c], pour continuer à publier leurs informations. Mais ils sont également encore nombreux à utiliser leur véritable identité, et dénoncer publiquement les activités du Parti. À l'image d'un administrateur de Danlambao : «*Personne ne peut nous faire taire ou stopper notre liberté d'expression. C'est notre mission, nous continuerons à n'importe quel prix* [23]»

Quelques solutions techniques

Afin de protéger leur anonymat, dans un pays où l'infrastructure réseau ne permet pas d'intercepter les communications chiffrées (pas de DPI), les blogueurs vietnamiens ont tout intérêt à utiliser des moyens de communication chiffrés. Il faut donc préférer l'usage de VPN aux proxies. Si les prox[d]ies permettent de contourner le blocage, ils ne chiffrent pas les communications contrairement aux VPN. Les services de mails jetables sont un bon moyen de conserver son anonymat. L'utilisation de service de mails anonymes et sécurisés tels que riseup.net ou hushmail couplé au système de chiffrement PGP peuvent également être utiles.

Les conversations sur VoIP ou par téléphones sont à éviter. La surveillance au Vietnam est aussi physique. L'un des moyens d'intercepter les conversations VoIP ou téléphonique est l'utilisation de microphone à longue portée déployé aux environs du domicile de supposés activistes. L'utilisation d'un service de messagerie instantané, Google chat, ICQ, IRC, Yahoo, etc. couplé à un logiciel de chiffrement tel que OTR permet de déjouer ce type de surveillance tout en chiffrant ses échanges. OTR ne conserve aucune trace des discussion sur le poste de l'utilisateur.

22 http://fr.rsf.org/vietnam-arrestations-surveillance-et-18-07-2012,43059.html

23 http://finance.yahoo.com/news/under-fire-vietnamese-blogger-vows-dissent-093346513.html

SYRIE

La Syrie, déjà qualifiée "d'Ennemi d'Internet" par Reporters sans frontières, renforce la censure du Net et la cybersurveillance à mesure que le conflit se durcit. Depuis le début du soulèvement populaire, le 15 mars 2011, le régime a mis en place les moyens nécessaires pour tenter d'empêcher la diffusion d'informations et d'images sur la répression. Grâce à une architecture ultra centralisée, le gouvernement syrien a la capacité de couper le pays du reste du monde, comme ce fut le cas le 29 novembre 2012.

Internet en Syrie

Population : 22 500 000
Nombre d'utilisateurs d'Internet : 5 000 000
Taux de pénétration d'Internet : 22,5 %
Journalistes emprisonnés : 22
Net-citoyens emprisonnés : 18
Tué en 2012 : 18

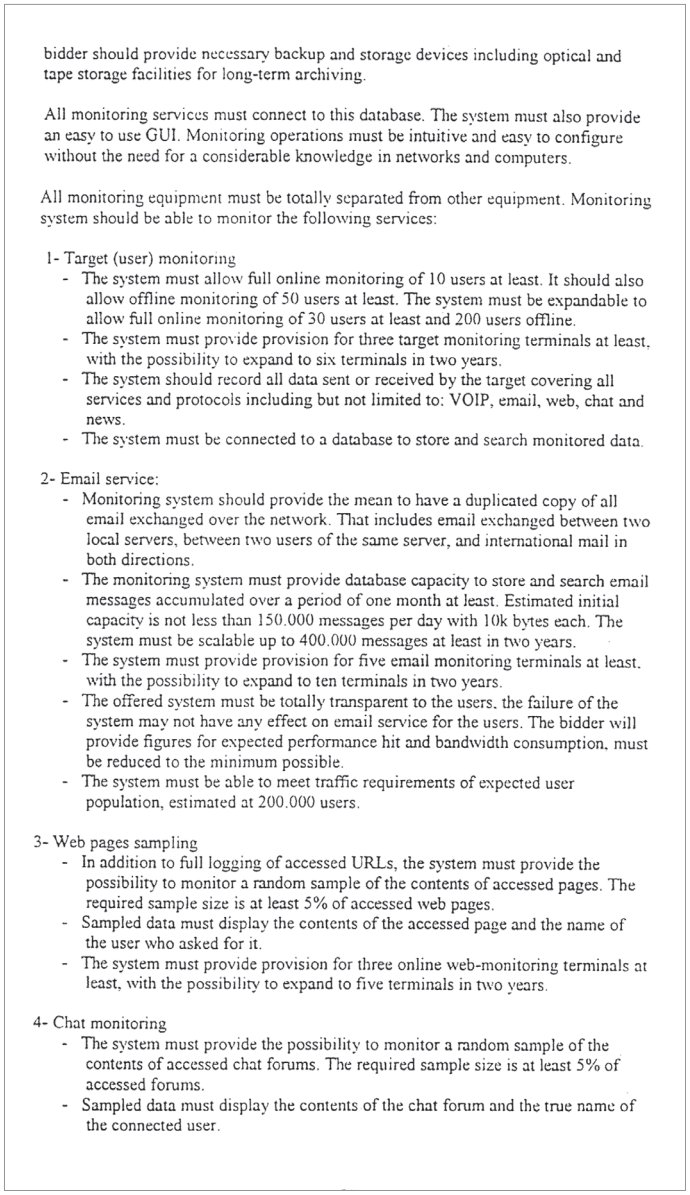
Source : Internet World Stats

Surveillance du réseau

Le réseau Internet syrien est contrôlé par deux entités : la Syrian Computer Society (SCS) et la Syrian Telecommunications Establishment (STE). Fondée par Bachar Al-Assad, la première détient l'infrastructure 3G sur le territoire syrien.

Placée sous la tutelle du ministère des Télécommunications et des Technologies, la seconde, la STE, contrôle la majorité des connexions fixes. À ce titre, elle met son câblage à disposition des autres opérateurs ADSL ou par ligne fixe et modem 56 kbits. Elle gère tous les points d'interconnexion du pays avec le World Wide Web. Lorsque les autorités ordonnent le blocage d'un mot clé, d'une URL ou d'un site, c'est la STE qui transmet les instructions aux opérateurs.

Reporters sans frontières s'est procuré un document inédit : l'appel d'offre publié en 1999 par la STE, pour la mise en place du réseau national Internet en Syrie (PDF, 7,3Mo). À la lecture de ce document, il apparait clairement que le réseau Internet syrien a été conçu pour intégrer des fonctionnalités étendues de filtrage et de surveillance.



bidder should provide necessary backup and storage devices including optical and tape storage facilities for long-term archiving.

All monitoring services must connect to this database. The system must also provide an easy to use GUI. Monitoring operations must be intuitive and easy to configure without the need for a considerable knowledge in networks and computers.

All monitoring equipment must be totally separated from other equipment. Monitoring system should be able to monitor the following services:

1- Target (user) monitoring
- The system must allow full online monitoring of 10 users at least. It should also allow offline monitoring of 50 users at least. The system must be expandable to allow full online monitoring of 30 users at least and 200 users offline.
- The system must provide provision for three target monitoring terminals at least, with the possibility to expand to six terminals in two years.
- The system should record all data sent or received by the target covering all services and protocols including but not limited to: VOIP, email, web, chat and news.
- The system must be connected to a database to store and search monitored data.

2- Email service:
- Monitoring system should provide the mean to have a duplicated copy of all email exchanged over the network. That includes email exchanged between two local servers, between two users of the same server, and international mail in both directions.
- The monitoring system must provide database capacity to store and search email messages accumulated over a period of one month at least. Estimated initial capacity is not less than 150.000 messages per day with 10k bytes each. The system must be scalable up to 400.000 messages at least in two years.
- The system must provide provision for five email monitoring terminals at least, with the possibility to expand to ten terminals in two years.
- The offered system must be totally transparent to the users, the failure of the system may not have any effect on email service for the users. The bidder will provide figures for expected performance hit and bandwidth consumption, must be reduced to the minimum possible.
- The system must be able to meet traffic requirements of expected user population, estimated at 200.000 users.

3- Web pages sampling
- In addition to full logging of accessed URLs, the system must provide the possibility to monitor a random sample of the contents of accessed pages. The required sample size is at least 5% of accessed web pages.
- Sampled data must display the contents of the accessed page and the name of the user who asked for it.
- The system must provide provision for three online web-monitoring terminals at least, with the possibility to expand to five terminals in two years.

4- Chat monitoring
- The system must provide the possibility to monitor a random sample of the contents of accessed chat forums. The required sample size is at least 5% of accessed forums.
- Sampled data must display the contents of the chat forum and the true name of the connected user.

Extrait de l'appel d'offre publié en 1999 par la STE, pour la mise en place du réseau national Internet en Syrie.

Le descriptif général du projet (5.1) précise que la société STE sera la seule structure à assurer la liaison avec le réseau Internet. Cet appel d'offre requiert que le futur prestataire implémente des mécanismes de filtrage et d'inspection du trafic Internet au coeur du réseau. Le chapitre *Monitoring system* (6-1-8) de l'appel d'offres détaille les mécanismes de surveillance que la STE entend mettre en place. La totalité des requêtes effectuées sur les moteurs de recherches devront être stockées dans une base de données pendant un mois.

Dans la même section figure l'ensemble des activités à surveiller :
1. Le système doit pouvoir enregistrer les activités en ligne et hors-ligne, VoIP, chat, surf et email, d'une soixantaine d'individus ciblés.
2. Il doit fournir une copie de l'ensemble des emails échangés en Syrie
3. Toutes les URLs des pages web visitées doivent être enregistrées.
4. Le système doit pouvoir surveiller de manière aléatoire le contenu de messages postés sur des forums auquel doit être associé le véritable nom de l'expéditeur.
5. Les "newsgroups" peu utilisés aujourd'hui mais très courants en 1999, font aussi partie du périmètre de surveillance du régime.
Les connexions chiffrées ne sont pas oubliées puisque le prestataire devra décrire en détails les possibilités d'interception et de blocage de toute donnée chiffrée.
S'il est impossible de savoir si le système mis en place en Syrie au début des années 2000 répond point par point aux demandes extravagantes du cahier des charges, l'appel d'offres témoigne en tous cas d'une volonté farouche des autorités de surveiller le réseau Internet.

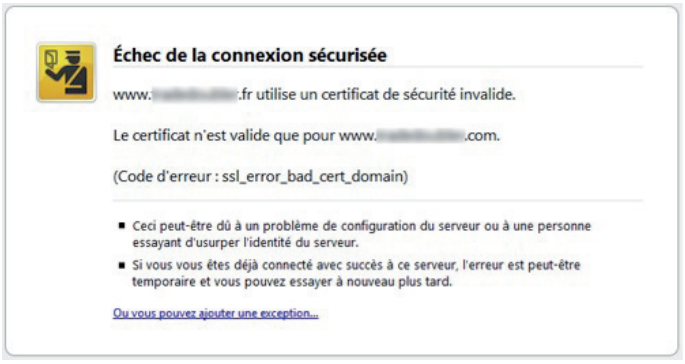
Perfectionnement des moyens de filtrage et de surveillance

En 2011, les autorités ajoutent de nouvelles technologies à leur dispositif de surveillance. Le site reflets.info, en collaboration avec le groupe d'activiste Telecomix et le portail tunisien fhimt.com, révèle la présence de serveurs mandataires (proxy) Blue Coat en Syrie et en publie les preuves sur son site : un scan du réseau syrien sous forme de fichier numérique librement accessible pour analyse. Dans un premier temps, la société Blue Coat nie avoir vendu des proxys au gouvernement syrien. Après la publication de preuves par reflets.info, Blue Coat admettra la présence d'au moins treize de ses serveurs en Syrie, semble-t-il vendus par un intégrateur, une société habilitée à revendre et installer des solutions Blue Coat, située à Dubaï. En décembre 2011, la société Blue Coat déclare (finalement?) ne plus fournir de support ni de mises à jour pour les serveurs installés en Syrie et ne pas disposer de moyens pour désactiver ses serveurs à distance. D'après des tests réseau menés en juillet 2012 par le Citizen Lab, les serveurs Blue Coat situés en Syrie ne communiquent plus avec les services de la maison mère, ce qui créditerait la thèse de l'entreprise.

Chronologie des attaques de l'homme du milieu (*Man In The Middle*)

Février 2011,alors que les printemps arabes débutent, le gouvernement syrien rend à nouveau accessibles les sites qui ont précisément permis aux Tunisiens et aux Égyptiens de se mobiliser : YouTube, Facebook, Twitter, bloqués depuis plusieurs années.

Mai 2011, l'Electronic Frontier Foundation, une ONG de défense des droits numériques, rapporte une première attaque man-in-the-middle visant les utilisateurs syriens se connectant sur la version sécurisée de Facebook (https://www.facebook.com) (cf lexique). Les internautes se connectant à Facebook ont vu apparaître dans leur navigateur une alerte de sécurité leur indiquant que le certificat (le document certifiant l'identité d'un site) n'était pas valide. Ceux qui se sont connectés sur leur compte en dépit de cet avertissement ont permis aux attaquants de récupérer leurs noms d'utilisateurs et leurs mots de passe.



Un exemple d'alerte de sécurité du navigateur Firefox lors d'une attaque MITM

Juillet 2011-La société éditrice de certificat Diginotar détecte une intrusion dans son réseau.
Entre juillet et août 2011, le groupe d'hactivistes Telecomix lance l'opération #OPSyria et récupère plus de 54 Go d'informations sur le fonctionnement des serveurs Blue Coat.

En août 2011, les versions https de Facebook et de Yahoo! sont bloquées en Syrie et automatiquement redirigées vers des versions non sécurisées (http), forçant ainsi les internautes souhaitant accéder à ces sites à envoyer leurs mots de passe en clair. Lors de ce type de manoeuvres, le seul indice permettant de vérifier que les mots de passe sont chiffrés lors de l'envoi sur Internet est la lettre 's' dans l'URL et le logo d'un cadenas affiché à côté. Les internautes les moins vigilants se font piéger.
Fin août 2011, Google détecte l'utilisation d'un certificat de DigiNotar frauduleux en Iran.

Les fichiers récupérés lors de l'#OPSyria laissent supposer que les autorités syriennes ont mis en place des attaques MTIM très évoluées. Les journaux de connexion des serveurs Blue Coat ne devraient normalement pas enregistrer d'informations lorsqu'un internaute accède à un site sécurisé (https). Pourtant, lors de l'accès à des sites parmi les plus consultés en Syrie, ces journaux de connexion révèlent que les serveurs Blue Coat ont enregistré un nombre anormalement élevé d'informations non accessibles en temps normal puisque chiffrées. Cet état de fait est probablement lié au vol de certificats de la société Diginotar..

Attaques ciblées

Les armes numériques dont le régime syrien s'est doté ne se limitent pas à la seule analyse du trafic Internet. Bloomberg et le Citizen Lab rapportent que les autorités syriennes disposent également de méthodes de surveillance extrêmement ciblées..

Un cas emblématique : Karim Taymour

Dans son article "Hackers in Damascus", le journaliste de Bloomberg Stefan Faris détaille le cas de Karim Taymour, un activiste syrien arrêté et torturé par le régime. L'histoire est la suivante. Le 26 décembre 2011, alors qu'il se rend à un rendez-vous avec l'un de ses contacts, Karim Taymour est arrêté par les forces de police syriennes. Les deux hommes s'étaient donné rendez-vous le matin même par Skype. Mais les autorités ont été aussitôt au courant. Karim Taymour passera 71 jours en détention. Lors de son interrogatoire, alors qu'il refusera de dévoiler ses activités et contacts, l'activiste se verra présenter une pile de plus de 1000 pages détaillant conversations et fichiers échangés sur Skype. Malgré la résistance qu'il oppose à ses bourreaux, ceux-ci en savent déjà beaucoup grâce à son ordinateur.
En janvier 2012, moins d'un mois après la libération de Karim Taymour, Morgan Marquis Boire, un expert en sécurité chez Google, récupère l'ordinateur d'un membre d'une ONG basée en Syrie. Ce dernier pense que son matériel a été infecté. Après une analyse poussée, Morgan Marquis Boire découvre que l'ordinateur a en effet été compromis une première fois le 26 décembre, quelques heures seulement après le début de la détention de Karim. Le logiciel espion a été transmis au membre de cette ONG par un message sur Skype, dont l'expéditeur n'était autre que Karim Taymour. Le logiciel espion était dissimulé dans un document que ce dernier avait finalisé la veille de son arrestation.

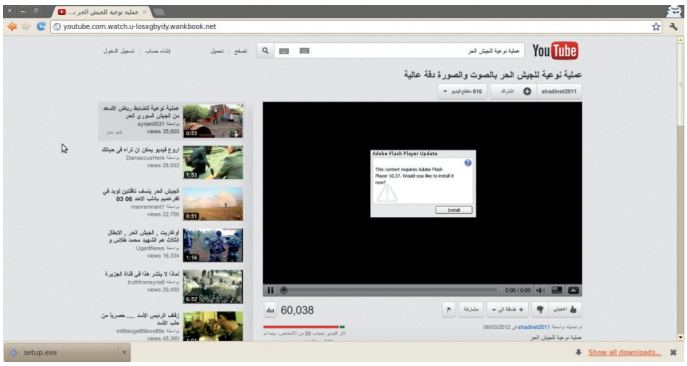
Phishing et ingénierie sociale

Le cas de Karim Taymour est représentatif des méthodes utilisées par le régime syrien pour surveiller et arrêter les net-citoyens. Le schéma d'attaque est souvent le même : lors d'une conversation, un contact propose à son interlocuteur de télécharger une vidéo, un document ou une image. Le lien proposé est un logiciel espion qui, une fois le lien cliqué, s'installe sur l'ordinateur. Les comptes Skype utilisés sont ceux de net-citoyens arrêtés ou dont l'ordinateur a déjà été compromis. Des comptes créés spécialement pour piéger les net-citoyens sont également utilisés. La campagne d'infection Blackshade, du nom du logiciel espion utilisé, menée à partir de juin 2012 en Syrie a été découverte grâce à un message envoyé depuis un compte Skype compromis à un membre de l'opposition syrienne.

السلام عليكم
في شخص بيكرهك وعم يجيب سيرتك وانا صورت المحادثة ياريت الانتباه من هذا الشخص وبيعرفك شخصي
هذه صورة عن المحادثة
http://14wre.co.za/new.zip

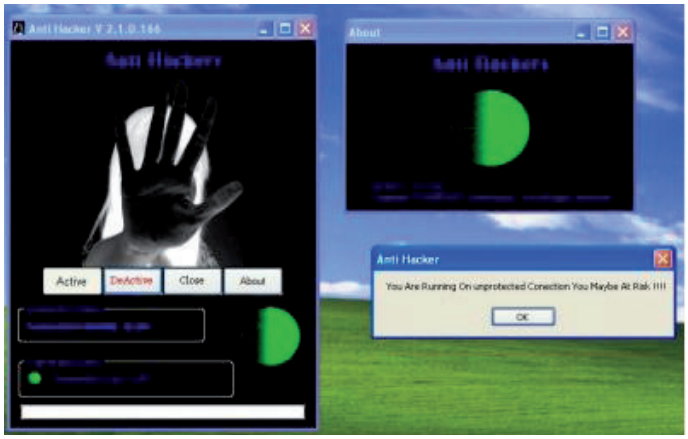
Capture écran issue de l'article de l'EFF détaillant cette campagne (licence Creative Commons)

La traduction du message est la suivante : "*Il y a quelqu'un qui te déteste et qui n'arrête pas de parler de toi. J'ai pris une capture écran de la conversation. Tu devrais te méfier de cette personne parce qu'elle te connaît personnellement. Voici la capture de la conversation*".
Lorsque l'internaute clique sur le lien, le malware s'installe sur l'ordinateur de la victime.
Le régime utilise aussi des attaques de type phishing, également hameçonnage. Ce type d'attaque consiste à mettre en place une copie d'un site connu tel que YouTube ou Facebook, qui demande à l'internaute d'entrer des informations personnelles pour des raisons apparemment crédibles. Il lui est proposé de remettre à jour son profil ou d'accepter une nouvelle politique de confidentialité.
En mars, une fausse page YouTube censée héberger des vidéos de l'opposition demandait aux internautes d'entrer leur login et mot de passe pour déposer des commentaires. Elle permettait également d'installer un logiciel espion sur le poste des visiteurs en leur demandant de télécharger une mise à jour du lecteur Adobe Flash (un logiciel permettant de regarder des vidéos en ligne).



Capture écran issue de l'article de l'EFF (licence Creative Commons)

En avril 2012, l'EFF a dénombré au moins cinq tentatives de hameçonnage ciblant les utilisateurs de Facebook. L'une d'entre elles a été véhiculée par des messages laissés sur les comptes Facebook de leaders de l'opposition syrienne, dont Burhan Ghalioun. Cliquer sur les liens laissés sur ces pages renvoyait vers une fausse page Facebook proposant d'installer une application, FacebookWebBrowser.exe, censée améliorer la sécurité des comptes Facebook. FacebookWebBrowser.exe est un logiciel espion permettant de récupérer l'ensemble des caractères entrés via un clavier et de voler les noms d'utilisateurs et mots de passe de comptes email, YouTube, Facebook et Skype.
En août 2012, l'EFF a identifié une autre vague de diffusion de logiciel espion. C'est sous la forme d'un programme appelé Antihacker, censé protéger l'ordinateur de celui qui l'installe, que cette campagne a été lancée. Antihacker n'est pas un logiciel espion en tant que tel, seulement, une fois installé, celui-ci récupère et installe sur le poste de la victime une version de DarkComet, un logiciel malveillant capable d'enregister des images via la webcam du poste, de désactiver les notifications de certains logiciels antivirus, d'enregistrer les frappes clavier et de récupérer des mots de passe.



L'écran d'installation du bien mal nommé AntiHacker

La plupart des attaques ciblées ont été réalisées à l'aide des mêmes logiciels espion (RAT- cf lexique) : DarkComet ou BlackShade. Une fois installés sur un ordinateur ou un téléphone, ces logiciels permettent d'avoir accès à la webcam, aux mots de passe de comptes emails, YouTube, Facebook, aux conversations Skype et aux frappes clavier. Les informations récupérées par ces logiciels malveillants sont envoyées vers des serveurs dont l'adresse IP est située en Syrie et laissent supposer que ces attaques proviennent du même groupe, l'armée électronique syrienne. Ce groupe pro-gouvernemental serait également à l'origine de la conception de la fausse page youtube qui a servi pour une attaque lors de l'attaque de phishing de

mars 2012 décrite pus haut. En juillet 2012, il diffuse 11 000 noms et mots de passe de "soutien de l'ONU", comprendre d'ennemis du régime. D'après certains experts, ce groupe paramilitaire travaillerait en étroite collaboration avec les services secrets syriens.

Quelques solutions techniques

La première mesure à prendre en Syrie, si l'on considère attentivement le type d'attaques menées, est de protéger son ordinateur des logiciels malveillants.

Protéger votre ordinateur

Pour ce faire, il faut respecter quelques conseils de base :

1. N'installer aucun logiciel reçu par email.
2. N'installer aucun logiciel exceptés ceux récupérés sur un site en https. Les certificats garantissant l'identité d'un site https, le risque d'usurpation d'identité (phishing) est réduit.
3. N'installer aucun logiciel provenant d'une source qui ne vous est pas familière, même si l'installation est recommandée par une fenêtre surgissante.
4. Faire systématiquement les mises à jour de votre système d'exploitation et des logiciels qui y sont installés. Les mises à jour comblent souvent des failles de sécurité
5. Ne pas utiliser Internet Explorer pour surfer. Ce navigateur étant parmi les plus utilisés, il est la cible des attaques de pirates informatiques. Préférez lui Firefox ou Chrome.

Éradiquer les logiciels malveillants

Darkcomet étant l'un des logiciels espions le plus souvent utilisé en Syrie, le logiciel permettant de le supprimer est disponible ici : http://www.phrozensoft.com/dcrem.more. L'EFF a publié un guide permettant de supprimer un logiciel espion largemment utilisé : Xterm Rat. Si vous pensez que votre ordinateur a été infecté, la meilleure solution est de réinstaller le système d'exploitation sur votre machine..

Protéger votre surf et prémunissez vous contre les MITIM

Il existe des solutions permettant de se protéger contre les attaques MITM. La plus simple est de ne pas ignorer les avertissements de sécurité du navigateur Internet lorsqu'on se connecte à un site https. Il existe des extensions pour les navigateurs Chrome et Firefox qui permettent de déceler les attaques *Man In the Middle* :

https everywhere : cette extension vérifie pour chaque site si une version https (chiffrée) existe et si oui redirige le visiteur redirige vers celle-ci. Plusieurs scénarios sont possibles :

- Si une tentative de hameçonnage vise les utilisateurs de Facebook, ceux qui auront installé cette extension seront redirigés vers la version https du site.
- Si l'attaque est basique, l'internaute est redirigé vers la véritable version https de Facebook.
- Si l'attaque est élaborée et si l'attaquant a mis en place une version https du site de phishing, les internautes recevront une alerte de sécurité leur indiquant que le site en question n'est pas celui qu'il dit être.
- Si l'attaque est très élaborée et si les attaquants ont réussi à compromettre le certificat de Facebook, il faut alors vérifier manuellement l'authenticité du certificat.

Https everywhere est utile au quotidien : à chaque fois que vous envoyez des données sur Internet en utilisant un formulaire par exemple, il est indispensable d'utiliser le protocole https plutôt que http. Si vous ne le faites pas, toutes vos données seront alors transmises en clair, à vos risques et périls.

Certificate Patrol

Cette extension vérifie les certificats (les papiers d'identité d'un site) à l'arrivée sur un site https. Elle avertit l'utilisateur qu'un changement de certificat est décelé. Indispensable contre les attaques Man in the middle et pour s'assurer que les requêtes https sont chiffrées correctement.

VPN et Tor

L'utilisation de VPN et de Tor, lorsque c'est possible, est un moyen efficace de se prémunir des attaques MITIM et du phishing. En utilisant Tor ou un VPN, l'internaute ne surfe pas sur le réseau syrien mais sur son point de sortie, en Suède, aux États-Unis ou ailleurs, et s'affranchit ainsi des attaques menées sur le réseau syrien.

Les VPN et les outils tels que Tor sont de très bons moyens de se soustraire à la surveillance du réseau puisqu'ils masquent l'adresse IP des utilisateurs.

Les solutions VPN ont un avantage supplémentaire puisque le trafic envoyé lors de l'utilisation du VPN est chiffré, contrairement au réseau Tor, qui ne fait qu'anonymiser l'internaute.

IRAN

- Population : 77 000 000
- Nombre d'utilisateurs d'Internet : 25 200 000
- Taux de pénétration d'Internet : 32,8 %
- Journalistes emprisonnés : 26
- Net-citoyens emprisonnés : 20
- Tué en 2012 : 1

Source: Banque Mondiale [1]

Réalités et fantasmes du réseau iranien

L'Iran est connecté au réseau Internet depuis le milieu des années quatre-vingt-dix. Pour des raisons économiques et politiques, les autorités ont développé les infrastructures au point de faire de l'Iran le pays de la région doté du plus grand nombre d'internautes [2]. Ce réseau est tenu par le régime des Mollahs, qui contrôle infrastructures, technologies, organes de régulation et a mis en place une législation liberticide.

Si la grande majorité des Iraniens s'informe par la télévision [3], la Toile joue un rôle essentiel de circulation de l'information grâce à l'action des dissidents et des acteurs de l'information, qui relaient des faits ou des opinions non présentés dans les médias traditionnels et témoignent de la répression. Le régime accuse régulièrement les réseaux sociaux d'être des instruments à la solde des puissances occidentales supposées comploter contre le régime. La vitesse de la bande passante en Iran est devenue un indicateur de la situation politique et du degré de surveillance par les autorités. À la veille d'échéances sensibles susceptibles de susciter des manifestations, la bande passante est ralentie pour éviter l'échange de photos et vidéos. La Toile iranienne n'est pas plus politisée qu'une autre, mais incontestablement plus surveillée. La spécificité du filtrage dans le pays : tout ce qui s'éloigne de la ligne officielle est automatiquement réputé "politique", et à ce titre filtré ou surveillé. Des sites de mode, de cuisine ou de chansons se retrouvent souvent bloqués, à l'instar des sites indépendants d'information ou d'opposition.

"Internet halal"

Serpent de mer depuis dix ans, le projet dément de créer un "Internet propre" (c'est-à-dire en accord avec les "valeurs" de la Révolution) en Iran commence à prendre forme. En septembre 2012, le gouvernement de Mahmoud Ahmadinejad a accéléré sa mise en place, la justifiant par les vagues de cyberattaques contre ses installations nucléaires [4]. Il a bénéficié du soutien de l'Ayatollah Ali Khamenei, Guide suprême de la République islamique.

La construction de ce réseau parallèle, doté d'une vitesse de connexion élevée, mais surveillé et censuré dans son intégralité, doit se terminer rapidement. A terme, les serveurs locaux sont censés héberger tous les sites iraniens. Les applications et services tels que boîtes mails, moteurs de recherche, réseaux sociaux et opérateurs devraient être développés sous le contrôle du gouvernement [5]. Le lancement imminent de cet Intranet à l'échelle nationale est inquiétant. Il permettra le gommage systématique des voix dissidentes et la surveillance à grande échelle des internautes iraniens.

Seules les administrations sont pour l'instant connectées au réseau national, mais il est à craindre que les citoyens iraniens n'aient à terme pas d'autre choix que de leur emboîter le pas. Selon des informations collectées par Reporters sans frontières, le gouvernement projette d'abaisser la vitesse de connexion du réseau international (pourtant plafonné aujourd'hui à seulement 128Kb/s [6]) et d'en augmenter le prix d'abonnement, rendant ainsi l'offre d'abonnement à l'Internet national bien plus intéressante, et plus rapide.

1 http://data.worldbank.org/indicator/IT.NET.USER.P2/countries/1W?display=graph

2 Les chiffres sont toutefois régulièrement "gonflés" par le ministère de la Communication iranien.

3 http://www.global.asc.upenn.edu/fileLibrary/PDFs/FindingaWay.pdf

4 http://fr.rsf.org/iran-lancement-imminent-de-l-internet-21-09-2012,43430.html

5 https://citizenlab.org/2012/11/irans-national-information-network/

6 http://www.lemonde.fr/proche-orient/article/2012/12/05/iraniens-encore-un-effort-pour-nationaliser-l-internet_1798592_3218.html

Dispositif de surveillance

"In reference to the Cyber Crimes Law, access to the requested website is not possible."

La République islamique d'Iran dispose d'un arsenal technologique et législatif lui permettant de surveiller son réseau. Filtrage, mainmise sur les fournisseurs d'accès à Internet, interdictions et espionnage des contenus de mails, discussions tchat ou VoIP sont devenus légaux en Iran.

La complexité de la politique intérieure du pays et l'imminence des échéances électorales ajoutent à la surveillance "légale" un caractère opaque, imprévisible et parfois "illogique". En témoignent les blocages de sites pro-régime ou l'imbroglio administratif qui a suivi le filtrage de Google en Iran.

Surveillance "officielle" et guerres intestines

La situation politique est telle qu'il est aujourd'hui presque impossible de définir exactement la nature des contenus filtrés. Depuis l'accès au pouvoir de Mahmoud Ahmadinejad, les autorités, institutions, commissions et comités responsables de la gestion du réseau se sont multipliés. Ils font la pluie et le beau temps de l'Internet iranien sans logique et sans concertation, en raison d'intérêts politiques parfois divergents.

Les fournisseurs d'accès à Internet ont l'obligation de s'identifier auprès du gouvernement et les sites Internet doivent obtenir une licence auprès de la Telecommunication Company of Iran (TCI). Les blogs doivent également "s'enregistrer" auprès du ministère de la Culture et de l'orientation islamique (MCOI) avant d'être passés au crible par le groupe de travail de détermination de contenus criminels [7] et le "Conseil suprême du cyberespace", dirigé par Mahmoud Ahmadinejad et composé de ministres, de Gardiens de la Révolution et de proches du Guide suprême [8].

Pour que les informations circulant sur Internet ne contreviennent pas à l'esprit et aux "valeurs de la Révolution", le filtrage est effectué à tous les niveaux par listes noires, mots-clés, URL [9], IP etc., en fonction des des tensions politiques internes. Plusieurs sites d'opinions, y compris conservateurs (comme les blog d'Amir Hassan Sagha ou de Mehdi Khazali [10]) et proches de la présidence (comme le site d'information Shomanews) ont ainsi été bloqués. En 2012, plusieurs blogueurs proches de Mahmoud Ahmadinejad ont été poursuivis sur initiative du procureur de Téhéran, pour avoir dénoncé les proches de l'Ayatollah Ali Khamenei. Les rivalités au sommet du pouvoir entre les clans d'Ali Khamenei et de Mahmoud Ahmadinejad font de plus en plus de victimes au sein des médias conservateurs.

La censure concerne également des sujets moins polémiques, comme la mode ou certains jeux en ligne, comme Travian [11]. Les mots-clés relatifs à la pornographie étant "évidemment" bannis des moteurs de recherches.

Les dirigeants iraniens surveillent à la fois l'accès aux sites d'informations hébergés à l'étranger et en Iran. Les sites de médias étrangers (en anglais comme en farsi) sont très fréquemment bloqués, voire copiés ou détournés. La BBC a ainsi découvert en janvier que les internautes iraniens souhaitant accéder au site bbcpersian.com, ont en réalité été redirigés vers persianbbc.ir, dont les contenus sont bien plus en adéquation avec les valeurs de la Révolution [12]. De même, les sites de Voice of America, Kaleme ou Jaras sont inaccessibles sans l'utilisation d'outils de contournement.

---

7 Ce comité est placé sous la responsabilité du parquet de Téheran.
8 http://fr.rsf.org/iran-iran-12-03-2012,42014.html
9 Liste des URL bloquées : https://citizenlab.org/data/iranreport/
10 http://fr.rsf.org/iran-la-repression-sans-fin-du-regime-06-03-2012,42003.html
11 http://www.bbc.co.uk/persian/science/2013/01/130104_na_travian_blocked_iran (farsi)
12 http://www.guardian.co.uk/world/2013/jan/24/iran-fake-blog-smear-campaign-journalist-bbc

Les médias sociaux dans le collimateur

Le chef de la police iranienne, Esmaeil Ahmadi Moghadam, a annoncé [13] en janvier 2013 que le gouvernement développait une technologie permettant de mieux surveiller les réseaux sociaux, Twitter et Facebook en tête. Un "contrôle intelligent" permettant "d'éviter les maux des réseaux sociaux" tout en "bénéficiant de leurs applications utiles". De cet aphorisme sibyllin, il faut comprendre que le compte Twitter du Guide suprême sera accessible au contraire de ceux d'opposants politiques ou de journalistes occidentaux. Alors que les officiels du régime iranien sont présents sur les réseaux sociaux, Esmaeil Ahmadi Moghadam a estimé que ce contrôle serait "plus efficace" que les blocages purs et simples.

S'il y a de quoi douter des capacités de l'Iran à mettre en place les infrastructures nécessaires [14], le projet n'en est pas moins effrayant. D'autant que les principaux réseaux sociaux Facebook et Twitter, jusqu'alors bloqués, sont à nouveau accessibles depuis le 20 février 2013 [15]. Loin d'être une bonne nouvelle, cette ouverture est probablement une nouvelle tentative de surveillance des utilisateurs.

Outils techniques

Parmi les outils dont dispose par le pouvoir iranien pour contrôler son réseau, on retrouve des outils de filtrage mais aussi, selon des sources interrogées par Reporters sans frontières, des outils d'interception de données type DPI (Deep Packet Inspection). Des rapports [16] et enquêtes ont fait état de produits chinois aidant le régime iranien à surveiller sa population, mettant en cause notamment les géants ZTE [17] et Huawei) [18]. Le DPI fourni par Huawei à Mobin Net, principal fournisseur national de réseau sans fil haut débit permet entre autre d'analyser les contenus d'e-mails, retracer les historiques de navigation ou bloquer l'accès à des sites. Les produits de la firme ZTE, vendus à la Telecommunication Company of Iran (TCI), offrent sensiblement les mêmes services, ainsi qu'une solution de surveillance du réseau mobile [19].

D'autres solutions d'espionnage et d'analyse de données proviennent d'entreprises européennes. On retrouve des produits conçus notamment par les entreprises Ericsson [20] ou Nokia Siemens Networks [21] (puis Trovicor). Ces entreprises ont vendu en 2009 à Mobile Communication Company of Iran et Irancell, les deux plus importantes entreprises de téléphonie mobile du pays, des produits permettant l'interception de SMS ou la localisation des utilisateurs [22]. Ces produits ont été utilisés pour identifier les citoyens iraniens lors du soulèvement post-électoral de 2009.

Plus étonnant, du matériel de surveillance israélien a été répertorié parmi les outils utilisés par le régime. La solution de gestion et surveillance de trafic NetEnforcer a effectivement été fournie par Israël au Danemark, avant d'être revendue en Iran [23]. De la même manière, du matériel américain s'est retrouvé sur le territoire iranien par le biais de l'entreprise chinoise ZTE [24]. Outre ces solutions de surveillance, les dirigeants iraniens utilisent les attaques de type man-in-the-middle afin d'intercepter les données envoyées lors de l'accès à des sites web sécurisés en https [25].

Un puissant appareil institutionnel

L'État dirige ou contrôle presque toutes les institutions de régulation, de gestion ou de législation relatives aux télécommunications dans le pays. La création du Conseil suprême du cyberespace en mars 2012 démontre que le pouvoir centralise ses compétences en matière de surveillance d'Internet. Ce conseil dirige désormais la politique numérique. Le Guide suprême a nommé Mahmoud Ahmadinejad a à sa tête. Le Conseil a autorité sur les fournisseurs d'accès à Internet. Selon son secrétaire général Mehdi Akhavan Behabadi, il lui revient de prendre les décisions majeures et de coordonner les institutions relatives à Internet.

---

13 http://www.dw.de/intelligent-software-set-to-control-social-media/a-16507868

14 https://citizenlab.org/2013/01/middle-east-and-north-africa-cyberwatch-january-2013/

15 information en date du 1er mars 2013

16 http://www.freedomhouse.org/sites/default/files/77_121312.pdf

17 http://www.reuters.com/article/2012/04/10/us-zte-iran-aryacell-idUSBRE8390T720120410

18 http://www.washingtonpost.com/world/national-security/iran-preparing-internal-version-of-internet/2012/09/19/79458194-01c3-11e2-b260-32f4a8db9b7e_story.html

19 http://www.reuters.com/article/2012/12/05/us-huawei-iran-idUSBRE8B409820121205?utm

20 http://www.reuters.com/article/2012/11/20/us-iran-ericsson-idUSBRE8AJ0IY20121120

21 http://online.wsj.com/article/SB124562668777335653.html

22 http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html

23 http://www.bloomberg.com/news/2011-12-23/israel-didn-t-know-high-tech-gear-was-sent-to-iran-via-denmark.html

24 http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322

25 http://gallery.mailchimp.com/7fdb14e291091d23007369520/files/IIIP01.pdf

Lors de la privatisation du secteur en 2009, les Gardiens de la Révolution ont remporté (on imagine sans mal) un appel d'offres leur permettant d'acquérir la Telecommunication Company of Iran (TCI) La TCI est le propriétaire du principal fournisseur d'accès à internet du pays. Les Gardiens de la Révolution dirigent le Centre de surveillance des délits organisés et son site officiel Gerdab. Le site a activement participé à la traque des net-citoyens, appelant à leur dénonciation [26]. Les Gardiens de la Révolution, qui contrôlent également le puissant groupe de travail de détermination de contenus criminels, sont ainsi à l'origine d'un grand nombre de censures sur Internet et d'arrestations d'acteurs de l'information.

Les ministères de la Culture et de l'Orientation islamique (MCOI), des Renseignements et des Technologies d'Information et de Communication ont leur part dans le contrôle d'Internet. Mais leurs décisions n'échappent pas aux conflits politiques internes. Récemment, le MCOI, proche d'Ahamadinejad, a demandé aux opérateurs de téléphonie mobile de surveiller les messages textes en vue des prochaines élections [27]. Cette décision n'a pas fait l'unanimité à la tête de l'État puisque l'Autorité de Régulation des communications a nuancé l'annonce et précisé que seuls les messages "commerciaux" seraient bloqués.

Le 26 février 2013, Mahmoud Ahmadinejad a placé à la tête du ministère des Technologies d'information et de communication l'un de ses lieutenants, Mohamed Hassan Nami [28], doctorant en stratégie d'État à l'université de... Pyongyang [29]. Nul doute qu'un militaire formé en Corée du Nord ne devrait pas adoucir les législations liées aux nouvelles technologies d'information et de communication.

Outre ces entités législatrices, il existe une cyberpolice (FETA). Cet organe est à l'origine notamment d'un décret de janvier 2012 sur les nouvelles régulations pour les cybercafés. Les clients doivent désormais présenter leur identité et accepter d'être filmés par des caméras de surveillance. Les gérants des établissements ont l'obligation de conserver les enregistrements vidéos, les coordonnées complètes des usagers et la liste des sites visités pendant six mois.

Une législation de plus en plus liberticide

En 1979, la Constitution iranienne inscrivait dans le marbre la liberté d'expression et proscrivait l'usage de la surveillance non prévue par la loi : "l'inspection et l'interception de courriers, la divulgation et l'enregistrement des conversations téléphoniques, ou la divulgation de communications télégraphiques ou télex, la censure, l'écoute, et toute forme de surveillance est interdite, à moins d'indication par la règle de droit" indique l'article 25. De même, l'article 24 stipule que "les publications et la presse jouissent de la liberté d'expression, sauf s'ils portent atteinte aux principes de l'Islam et à la morale publique" [30].

Toutefois, les exceptions prévues par ces deux articles ont été largement exploitées par les autorités. La loi de 1986 sur la presse (amendée en 2000 et en 2009 pour englober les publications en ligne) permet au pouvoir de vérifier que les acteurs de l'information ne "portent pas atteinte à la République islamique", "n'offensent pas le Guide suprême" ou ne "diffusent pas de fausses informations". Les amendements de la loi sur la presse obligent les publications en ligne à obtenir une licence.

La République islamique a franchi un pas de plus vers le renforcement de la cybercensure en 2009, quinze jours après la réélection contestée de Mahmoud Ahmadinejad, en signant la Computer Crime Law (CCL). Cette loi a permis la création du Groupe de travail de détermination de contenus criminels, qui décide désormais de ce qui est conforme ou pas aux lois de la République islamique (et donc in fine ce qui est publiable et ce qui ne l'est pas). La CCL oblige tous les fournisseurs d'accès à Internet à enregistrer toutes les données échangées par leurs utilisateurs pendant six mois sous peine de sévères sanctions à l'égard des FAI ne remplissant par leur rôle. Les internautes publiant des contenus illégaux ou se servant de moyens détournés pour accéder aux contenus bloqués sont passibles de lourdes peines de prison. Les membres du groupe de travail ne s'accordent pourtant pas sur le caractère illégal d'outils de contournements, comme le VPN, par exemple [31]. Malgré le fait que la République islamique produise et vende elle-même des VPN dits "halal".

26 http://www.gerdab.ir/fa/pages/?cid=407

27 http://www.roozonline.com/persian/news/newsitem/archive/2013/january/14/article/-c463e593b1.html

28 http://www.president.ir/en/cabinet

29 http://articles.washingtonpost.com/2013-02-18/world/37155039_1_kim-il-sung-university-north-korea-key-post

30 Troisième chapitre de la constitution de la République islamique d'Iran, principes 24 et 25.

31 http://opennet.net/sites/opennet.net/files/iranreport2013.pdf pp. 20-21

Principales violations de la liberté de l'information

La combinaison de ces puissants arsenaux technologiques, d'un carcan législatif et d'un contexte politique interne divisé forme un cocktail explosif dont la première victime est le peuple iranien, qui voit sa liberté d'information foulée aux pieds. Le début de l'année 2013 a été marqué par une vague d'arrestations "préventives" dans la perspectives de l'élection de juin 2013. Le régime anticipe le scrutin afin d'éviter une vague de protestations - relayée par les médias et sur Internet - du même type que celle de juin 2009.

Le 27 janvier 2013, lors du "Dimanche noir", le régime a mené une opération coup de poing, perquisitionnant les sièges de cinq publications téherénaises (Etemad, Arman, Shargh, Bahar et Aseman), arrêtant une quinzaine de journalistes et annonçant que de nombreux journalistes seraient convoqués devant les tribunaux [32]. Surveillés par les renseignements iraniens, ces journalistes sont accusés de "collaborer avec des Occidentaux et des contre-révolutionnaires basés à l'étranger". Vingt jours plus tard, une autre dizaine de journalistes, net-citoyens, activistes politiques et membres de la société civile ont été convoqués ou arrêtés dans le pays [33]. Durant leurs interrogatoires, ils ont été menacés et enjoints de ne mener aucune activité dans le cadre de l'élection présidentielle de juin 2013. Il leur a été demandé de révéler l'identité de leurs contacts Facebook ou Twitter et les raisons pour lesquelles ils étaient "connectés" avec ces derniers.

Le 18 février, Ahmad Bakshaysh, membre de la Commission de la Sécurité nationale du Parlement, avait déclaré au journal Roozonline que le responsable des Affaires culturelles du ministère des Renseignements lui avait dit que "ces arrestations sont préventives ; elles ont pour but d'empêcher l'activité d'un réseau à l'intérieur et extérieur du pays, à l'approche de l'élection présidentielle de juin 2013 […]. Ce réseau encourage ses journalistes à interviewer les différents responsables du régime pour montrer leurs divergences […]. A l'issue de leur détention, certains d'entre-eux ont compris leur erreur et sont prêts à témoigner dans ce sens […]".

Ahmad Bakshaysh conclut : "*Je pense qu'il faisait référence aux aveux télévisés". Car en plus de la surveillance avouée de ces journalistes et des intimidations qui leur ont été faites, «les inspecteurs exercent des pressions psychologiques lors des interpellations pour que les journalistes avouent des activités d'espionnage*" raconte Reza Tajik, journaliste iranien réfugié en France. "*Ces aveux sont filmés et diffusés ensuite à la télévision*".

Ces rafles ponctuent un second mandat de Mahmoud Ahmadinejad marqué par la surveillance, la censure et l'arrestation de nombreux journalistes ou blogueurs. Reporters sans frontières rappelle la mort en détention du blogueur Sattar Beheshti, incarcéré le 31 octobre 2012, dans des circonstances toujours inconnues. Les éléments actuels portent à croire qu'il a succombé à des coups reçus lors de son interrogatoire. Les responsables de sa mort n'ont pas été inquiétés et aucune enquête indépendante n'a été menée.

Le régime tente d'infiltrer les réseaux des journalistes, à l'intérieur comme à l'extérieur du pays. Arrêté en 2010, le journaliste Saeid Pourheydar raconte avoir subi des mauvais traitements lors de son interrogatoire. Les agents du renseignement iranien lui ont brandi les retranscriptions de ses conversations téléphoniques, ses mails et ses SMS [34]. Les prisonniers qu'il a rencontrés ont relaté des faits similaires. Cette méthode est courante et démontre le niveau élevé de surveillance des journalistes en Iran.

Les journalistes exilés ou émettant de l'étranger - et notamment ceux qui collaborent avec Radio Free Europe et la BBC - reçoivent régulièrement des emails contenant des logiciels malveillants. Certaines tentatives d'hameçonnage ont été fructueuses. Les journalistes étrangers autorisés à se rendre sur le territoire iranien sont surveillés de près, ainsi que leurs activités sur Internet. S'ils se connectent sur les réseaux iraniens, leurs données sont immédiatement épiées s'ils n'utilisent pas d'outils de sécurisation des communications ou d'anonymisation.

A l'approche de l'échéance électorale de juin 2013, la répression ne devrait pas cesser de se renforcer.

32 http://fr.rsf.org/iran-le-guide-supreme-ali-khamenei-28-01-2013,43959.html
33 http://fr.rsf.org/iran-le-ministere-des-renseignements-20-02-2013,44098.html
34 http://www.bloomberg.com/news/2011-10-31/iranian-police-seizing-dissidents-get-aid-of-western-companies.html

Quelques solutions techniques

Réseau privé virtuel (VPN)

Afin de contourner le blocage et la censure de contenus en Iran, les citoyens peuvent utiliser les technologies de réseau privé virtuel (virtual private network : VPN). L'état iranien vend d'ailleurs ce type de technologie, afin de profiter d'un marché florissant en Iran et pour empêcher que les net-citoyens ne se fournissent à l'extérieur. Malgré les réglementations de la Computer Crime Law (CCL, voir plus haut), l'utilisation de VPN iranien est légale en Iran. Les VPN étrangers sont en revanche interdits. Pourtant, ce sont bien ceux-là qu'il est recommandé d'utiliser. L'État iranien ne fournit pas innocemment des technologies pour contourner sa propre censure. Le fournisseur de VPN a la possibilité d'observer et d'analyser tout le trafic passant par le VPN. En effet, si le trafic est chiffré entre le client (l'ordinateur de l'internaute) et le serveur, entre le serveur VPN et Internet, le trafic n'est plus chiffré. Celui qui contrôle le serveur, les autorités iraniennes dans le cas des VPN d'État, a alors toute latitude pour observer et analyser le trafic.

The Onion router (Tor)

Tor est un outil d'anonymisation, protégeant les données privées de ses utilisateurs lors de leur navigation sur internet. En Iran, Tor est utilisé pour pallier aux VPN, lorsque ceux-ci se retrouvent bloqués. Son utilisation réduit cependant considérablement la vitesse de navigation. Les internautes préfèrent utiliser les VPN et considèrent Tor comme une solution de remplacement. L'utilisation seule de Tor est à bannir, car l'Etat iranien a la possibilité de demander aux fournisseurs d'accès d'identifier le trafic Tor, aisément reconnaissable, et donc d'en connaître la provenance.

Il existe toutefois une possibilité pour les citoyens de déguiser le trafic Tor : Obfsproxy. Selon les développeurs de cette solution, les fournisseurs d'accès à internet ne peuvent plus détecter le trafic Tor lorsque Obfsproxy est lancé.

Conseils

Les moyens de surveillance du régime iranien évoluent constamment, les conseils prodigués ci-dessous sont donc à prendre avec précaution car s'ils sont valables aujourd'hui, ils ne le seront peut-etre plus demain. L'essentiel est de bien connaître et de constamment évaluer le contexte dans lequel on évolue et les menaces auxquelles l'on est est exposé afin d'être en mesure de mettre en place les solutions adaptées.

1. Ne pas utiliser les VPN nationaux. Utiliser un VPN controlé par les autorités iraniennes équivaut à court ou moyen terme à se jeter dans la gueule du loup.
2. Le régime n'a aujourd'hui pas les moyens de surveiller des millions de citoyens. Quelques précautions de base telles que la mise à jour régulière de son système d'exploitation et des logiciels installés, l'utilisation d'un anti-virus, d'un VPN et l'utilisation systématique du protocole https lorsque cela est possible permettent de se prémunir d'une grande partie des menaces.
3. Une bonne "hygiène électronique", ne pas cliquer sur des liens envoyés par un destinataire inconnu, ne pas télécharger de logiciels dont on ne connaît pas la provenance, ne pas accepter de demandes de contacts de la part d'inconnus sur les réseaux sociaux, identifier systématiquement l'expéditeur d'un email avant d'ouvrir les pièces jointes associées, permet d'éviter l'infection de son ordinateur par un Spyware.
4. Lorsque des sites bloqués depuis longtemps, tels que Facebook, Youtube ou Twitter, sont de nouveau accessibles, c'est souvent pour les autorités un moyen de récupérer les noms d'utilisateurs et mots de passe grâce à la mise en place d'une attaque Man-in-the-middle. L'utilisation d'un VPN ne permet pas seulement de contourner la censure, il permet également et surtout de se soustraire aux moyens de surveillance d'un réseau grâce au chiffrement des communications échangées entre le serveur et le client.

CHINE

Internet en Chine

- Population : 1 343 000 000
- Nombre d'utilisateurs d'Internet : 564 000 000
- Taux de pénétration d'Internet : 42,1%
- Nombre de journalistes emprisonnés : 30
- Nombre de net-citoyens emprisonnés : 69
- Classement : 173e

Le Parti communiste chinois est à la tête de l'un des principaux empires numériques du monde, si ce n'est le plus grand. Dans l'Empire du Milieu, les points d'accès à Internet sont la propriété exclusive de l'Etat, qui est le plus souvent un faux nez du Parti. Les particuliers et les entreprises ont l'obligation de louer leur bande passante à l'Etat chinois ou à une entreprise contrôlée par lui. Les quatre réseaux nationaux, CTNET, Chinanet, Cernet et CHINAGBN représentent l'épine dorsale de l'Internet. En 2008, une restructuration du réseau a permis l'apparition de trois grand fournisseurs d'accès nationaux, China Telecom, China Unicom et China Mobile, contrôlés majoritairement par l'État chinois. L'accès public à Internet est délégué à des compagnies régionales.

Dans un rapport daté de janvier 2013, le très officiel China Internet Network Information Center (CNNIC) revendique un taux de pénétration de 42,1%. Selon lui, la Chine compte 564 millions d'internautes, dont 277 millions accèdent à Internet via un terminal mobile.

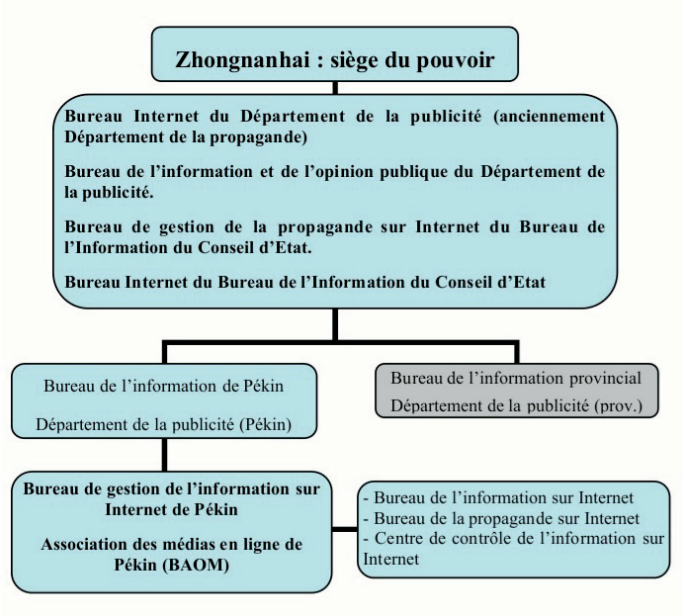
Bien qu'il soit difficile d'evaluer le nombre d'utilisateurs des réseaux sociaux bloqués en Chine,, d'après les les estimations les plus optimistes, Facebook compterait 63.5 millions d'utilisateurs et Twitter 35 millions. Le réseau social chinois Weibo aurait également multiplié par trois le nombre estimé de ses utilisateurs pour atteindre le chiffre atteint 504 000 000.

Le coût d'accès d'une connection DSL avec un débit de 1Mbit est compris, selon les provinces, entre 10$ et 20$ par mois.

Surveillance du réseau

Une affaire d'Etat

De nombreux départements étatiques sont impliqués dans la censure et la surveillance du Web :
1. Le Bureau Internet et le Centre d'étude de l'opinion publique du Bureau de l'information du Conseil d'Etat (équivalent du gouvernement) ;
2. Le Bureau Internet et le Bureau de l'information et de l'opinion publique duDépartement de la publicité (ancien Département de la propagande) ;
3. Le ministère de l'Industrie de l'Information (MII) ;
4. Le Bureau de surveillance et de sécurité des informations sur Internet du ministère de la Sécurité publique ;
5. Le Centre d'enregistrement des informations illégales et inconvenantes sur Internet du ministère de l'Industrie de l'information (MII).



Les organes de contrôle de l'État

Les deux derniers organes 4) et 5) gèrent les questions de la pornographie, de la violence et de la fraude électronique. Le MII ne participe pas directement au contrôle d'Internet. Les organes influents sont le Bureau de l'information du Conseil d'Etat et le Département de la publicité.

La Grande Muraille électronique de Chine

L'ensemble des outils mis en place pour filtrer et surveiller Internet en Chine est connu sous le nom de Great Firewall of China ou Grande Muraille électronique de Chine. Lancé en 2003, ce système permet de filtrer l'accès aux sites étrangers. Au-delà des règles classiques de routage permettant de bloquer l'accès à une adresse IP ou à un nom de domaine, la grande muraille électronique de Chine utilise massivement les technologies de DPI pour la détection et le blocage de mots clés.

Selon le rapport Planet Blue Coat de Citizen Lab, centre de recherche lié à l'Université de Toronto, au moins trois serveurs Blue Coat sont utilisés sur le réseau du fournisseur d'accès China Net (contrôlé par l'État Chinois) dans la province du Sichuan. Leur présence a été détectée fin 2012. Pour mémoire, Blue Coat est une société spécialisée dans la surveillance des réseaux. Les serveurs identifiés en Chine sont de type PacketShaper. Ils permettent d'identifier et de contrôler le trafic en bloquant certains flux ou contenus jugés indésirables.

Accès aux outils de contournement

Les moyens permettant d'échapper à ce système de surveillance orwellien, proxy, VPN, Tor, sont nombreux mais relativement peu utilisés à l'échelle de la population chinoise.

Les VPN payants chinois ne sont pas très populaires. Ils nécessitent l'utilisation d'une carte de crédit, un moyen d'identification très efficace. Sachant que toute société commercialisant un service de VPN en Chine doit s'enregistrer auprès du ministère de l'industrie et des technologies de l'information, leur usage s'avère encore plus dangereux.

Les outils de contournement gratuits tels que Tor ou Freegate sont la cible continuelle des autorités, ce qui les rend lents et instables. Leur utilisation est donc loin d'être systématique.

Restent les solutions fournies par des sociétés situées hors de Chine. Elles constituaient jusqu'ici une alternative de choix pour les citoyens chinois.

La mise à jour de Grande Muraille électronique

A l'occasion de la tenue du 18ème congrès du Parti communiste en novembre 2012, les autorités chinoises ont procédé à une mise à jour de la Grande Muraille Électronique de Chine afin de verrouiller le contrôle de l'information : les solutions de VPN fournies par des sociétés étrangères ont été neutralisées. Les principaux utilisateurs de VPN hébergés à l'étranger ont vu leurs connections bloquées. La Grande Muraille Électronique de Chine a désormais la capacité de bloquer dynamiquement les connexions chiffrées. L'un des principaux fournisseurs d'accès Internet du pays, China Unicom, met automatiquement fin à toute connexion dès lors que le contenu transmis est chiffré.

A ce jour, seuls les services VPN de la société Astrill semblent être en mesure de permettre aux citoyens chinois de passer au travers de la Grande muraille électronique de Chine et de rester anonymes sur Internet. Les autres grands fournisseurs de VPN (Witopia, StrongVPN, AirVPN, etc.) restent bloqués.

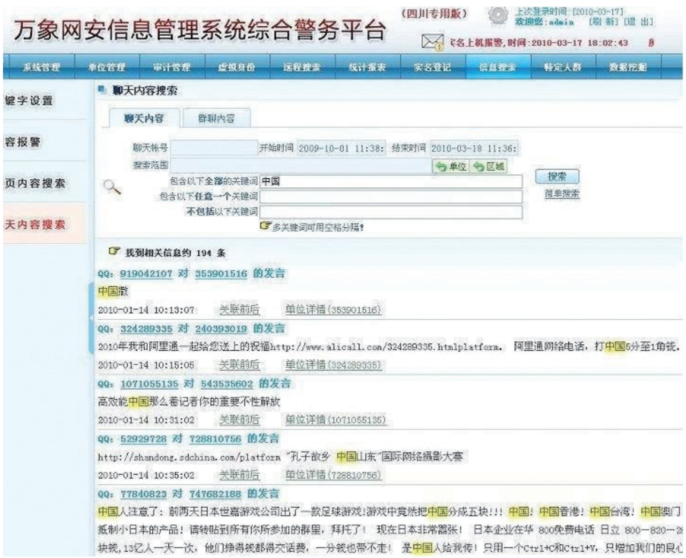
Blocage des solutions de contournement : les net-citoyens plus exposés

L'utilisation de VPN permet non seulement de contourner le blocage imposé par les autorités mais aussi de masquer son adresse IP et de chiffrer ses communications sur Internet. La mise à jour de la Grande muraille électronique de Chine et le blocage des moyens de chiffrement présente l'inconvénient d'exposer les communications des journalistes et net-citoyens chinois au système de surveillance des autorités.

Dispositif de surveillance intégré

Le dispositif de surveillance mis en place par la Chine ne se limite pas à la seule Grande Muraille Électronique, à l'identification et au blocage des communications entrantes et sortantes. Les moyens de surveillance sont intégrés dans les réseaux sociaux, services de chat et de VoIP. Les entreprises privées sont directement chargées par les autorités chinoises d'assurer une veille de leur réseau afin d'empêcher la diffusion de messages interdits.

Propriété de la société Tencent, le logiciel QQ permet notamment aux autorités de surveiller avec précision les échanges de tous les internautes, en recherchant certains mots clés ou expressions. L'identification de l'auteur de chaque message est rendue possible grâce au numéro d'utilisateur du logiciel. Le logiciel QQ est en soi un gigantesque cheval de Troie (lien en chinois).



Le logiciel QQ permet notamment aux autorités de surveiller avec précision les échanges de tous les internautes.

Depuis mars 2012, une nouvelle législation oblige tout nouvel utilisateur de sites de micro blogging en Chine à s'enregistrer sous son vrai nom et à donner son numéro de téléphone.

Afin de forcer les utilisateurs déjà existants à se soumettre à cette volonté de contrôle, dans le cadre de l'évolution de ses conditions générales d'utilisation, le site Sina Weibo a mis en place deux mois plus tard un véritable permis à points. Il est attribué à chacun des 300 millions d'utilisateurs de Weibo 80 points de départ. Pour chaque infraction aux conditions d'utilisation, un nombre prédéfini est retiré. Lorsque le nombre de points atteint zéro, le compte de l'utilisateur est fermé. Les utilisateurs avec peu de points peuvent en regagner s'ils ne commettent pas d'infractions pendant deux mois ou s'ils participent à des activités non spécifiées de promotion.

En février 2013, l'application mobile d'envoi de messages textes et vocaux WeChat, extrêmement populaire, a modifié ses conditions d'utilisation. Les utilisateurs publics de l'application, dont nombre de sociétés et célébrités, doivent désormais fournir un numéro de carte nationale d'identité et un numéro de téléphone portable. Ils doivent également envoyer une photocopie de leur carte d'identité.

Pour parfaire le contrôle et couper court à toute tentative d'anonymisation, le Congrès national du peuple chinois a adopté en décembre 2012 une mesure obligeant les citoyens souhaitant souscrire à un abonnement Internet ou mobile à fournir leur véritable identité.

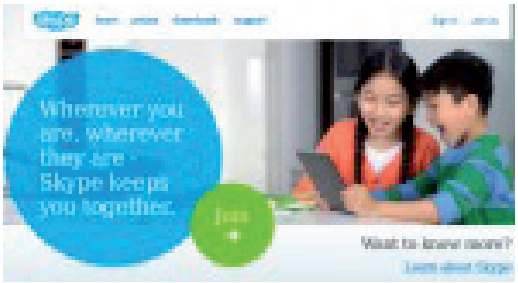
TOM Skype

Les réseaux sociaux ne sont pas les seuls touchés par ces mesures de contrôle. Skype, l'un des outils de téléphonie sur Internet les plus populaires au monde, est placé sous surveillance étroite. En Chine, les services de Skype sont distribuées dans le cadre d'un partenariat avec la société locale Tom. La version chinoise de Skype, dénommée Tom Skype, diffère légèrement des versions téléchargeables dans les autres pays.

Afin de se conformer aux restrictions imposées par le gouvernement chinois, le logiciel Tom Skype est équipé d'un filtre automatique. Lorsque certains mots-clés sont détectés dans un message instantané, celui-ci est bloqué et, selon un rapport de Open Net Initiative Asie, stocké sur un serveur. Un étudiant de l'université dAlbuquerque au Nouveau Mexique a réussi à recréer cette liste de mots clé. "Human Right Watch", "Amnesty International", "Tiananmen", "BBC News" et ... "Reporters Without Borders" sont autant de mots et expressions interdits en Chine.

La surveillance et l'interception des messages instantannés Tom Skype ne se baserait pas uniquement sur certains mots-clés mais également sur le nom de certains utilisateurs de Tom Skype. Le rapport de Open Net Initiative Asie fait état de conversations banales stockées sur des serveurs. Dès lors, le nom de l'expéditeur ou du destinataire constituerait un critère suffisant à l'interception et au stockage de conversations.

En Chine, sans l'utilisation de moyens de contournement du type Tor ou VPN, le site officiel de Skype (http://www.skype.com) renvoie vers le site Tom Skype. Les deux sites étant semblables, certains utilisateurs de Tom Skype ne savent probablement pas qu'ils utilisent une version modifiée de Skype et que leur sécurité est potentiellement menacée.



En janvier 2013, Reporters sans frontières a signé, avec d'autres ONG, une lettre ouverte demandant à la société Skype des précisions sur ses relations avec la société chinoises Tom Skype ainsi sur les mécanismes de surveillance et de censure implantés dans ses logiciels.

Demande de collaboration aux sociétés étrangères

Le Comité pour la Protection de la Qualité des Marques est un groupe représentant plusieurs multinationales en Chine telles que Apple, Nokia, Toyota, Audi etc. Ce comité a envoyé un message électronique à ses 216 membres les informant des inquiétudes des autorités chinoises quant à l'utilisation de VPN par ces multinationales permettant aux employés d'échanger des informations sans que le contenu de ces communications puisse être intercepté ou contrôlé par la Grande Muraille Électronique. Il faisait état d'une possible visite de la police chinoise à quelques unes de ces sociétés. À Pékin, Hebei et Shandong, la police aurait demandé à certaines d'entre elles d'installer un logiciel permettant de surveiller leur réseau. En cas de refus, les autorités chinoises auraient menacé de couper l'accès internet de ces sociétés.

Dommages collatéraux

L'un des freins dans la mise en place d'outils de surveillance et de contrôle du réseau en Chine, au-delà des atteintes à la liberté d'expression, à laquelle le gouvernement chinois n'accorde que peu d'importance, est l'impact économique de ces mesures pour les sociétés chinoises et étrangères. À l'ère d'Internet, la surveillance a en effet un coût qui se répercute sur la compétitivité des entreprises.

Les dirigeants des portails en ligne sont frustrés par l'énergie et le temps investis pour mettre en oeuvre des mécanismes de censure. Tencent, le géant chinois du web, doit investir de lourdes ressources pour mettre en oeuvre les mécanismes de censure dans son service de chat en ligne, WeChat. Lors de la dernière mise à jour de la Grande Muraille Électronique et du blocage systématique des connexions chiffrées, de nombreuses sociétés étrangères implantées en Chine ayant recours à des services de VPN pour accéder à leurs données situées hors du pays ont été pénalisées.

L'un des épisodes récents démontrant les limites économiques du système de censure et de contrôle du réseau chinois concerne la plus grosse plate-forme d'hébergement et de mise à disposition de projet libre au monde : GitHub. GitHub héberge des logiciels open source et de nombreuses bibliothèques de codes, indispensables pour de nombreux développeurs informatiques. Suite à la publication de la liste des contributeurs du code de la grande muraille électronique de Chine et aux nombreux commentaires déposés sur le site, les autorités chinoises ont tenté de bloquer l'accès à GitHub. Or, le site GitHub utilise le protocole https, empechant ainsi les autorités chinoises de bloquer uniquement la page hébergeant les noms des contributeurs de la Grande Muraille Électronique. L'autre option des autorités chinoises était de bloquer l'intégralité du site. Ce site et les nombreuses lignes de code qu'il héberge étant indispensables pour les nombreuses sociétés chinoises travaillant dans le domaine des nouvelles technologies, un blocage complet n'était pas envisageable. Le seul outil permettant de régler ce problème est l'attaque dite de l'homme du milieu (Man In The Middle). En se faisant passer pour une autorité de certification, un tiers peut se placer entre le site https et l'internaute et intercepter les communications chiffrées.

L'attaque n'est cependant pas transparente et la plupart des navigateurs (chrome et firefox) affichent des alertes de sécurité prévenant l'utilisateur. C'est pour cette solution qu'ont opté les autorités chinoises. Le 26 janvier 2013, les internautes chinois se connectant à GitHub ont reçu une alerte de sécurité les informant qu'un tiers se faisait passer pour le site. L'attaque Man In The Middle lancée par les autorités chinoises n'a duré qu'une heure et s'est révélée assez grossière et facile à identifier. Pendant cette heure cependant, les internautes ayant ignoré les alertes de sécurité de leur navigateurs ont pu être trackés sur le site, leur IP enregistrée et leurs mots de passe interceptés.

Surveillance interne et externe

La Chine n'a pas hésité à étendre son périmètre de surveillance au delà de ses frontières. Le 30 janvier 2013, le New York Times a révélé avoir été la cible d'attaques émanant du gouvernement chinois. Les premières intrusions auraient eu lieu le 13 septembre 2012, alors que le journal s'apprêtait à publier son reportage sur la fortune amassée par les proches du Premier ministre sortant Wen Jiabao. D'après le journal, ces attaques avaient pour objectif d'identifier les sources ayant informé le New York Times sur la corruption de l'entourage du premier ministre. Le Wall Street journal et CNN ont également déclaré avoir été la cible de cyber-attaques en provenance de Chine. En février, Twitter a révélé que les comptes de quelque 250 000 utilisateurs avaient été victimes d'attaques informatiques similaires à celles portées contre le New York Times, également en provenance de Chine.

Mandiant, la société de sécurité informatique mandatée par le NYT pour sécuriser son réseau, affirme que les attaques émanaient d'un groupe de hackers baptisé Advanced Persistant Threat 1. D'après un rapport publié par la même société, ce groupe serait localisé dans un immeuble de douze étages dans les faubourg de Shangaï et compterait "des centaines, voire des milliers d'employés". Il bénéficierait du soutien direct du gouvernement chinois et constituerait une filiale de l'armée de libération du peuple. Si l'on ne peut douter de la réalité et de la provenance des attaques contre le New-York Times, le Washington Post et Twitter, la polémique qu'a suscité le rapport de Mandiant a offert à cette société, qui a pour autre client illustre le gouvernement américain, une exposition médiatique inespérée. La limite entre une opération de communication réussie et un rapport circonstancié est difficile à fixer.

Principales violations de la liberté de l'information

La Chine est la plus grande prison du monde pour les acteurs de l'information. A ce jour 30 journalistes et 69 net-citoyens sont détenus. Parmi ceux-ci, quelques cas emblématiques de la répression, qui connaît des période d'accalmie puis des mouvements de crispation, notamment au début des Printemps arabes, ou en amont et pendant le dernier Congrès qui a porté Xi Jinping à la tête du pays.

De nombreux journalistes étrangers en Chine ont rapporté à Reporters sans frontières qu'ils travaillent avec comme postulat de base que leurs téléphones sont sur écoute et que leur adresse e-mail est surveillée. Les journalistes locaux rapportent également que les conditions dans lesquelles ils travaillent ont empirées. Beaucoup se méfient de leurs collègues étrangers.

Le cyber dissident Hu Jia a purgé un peine de trois ans et demi en prison pour incitation à la subversion. Libéré le 26 juin 2011, Hu Jia reste privé de tous ses droits civiques et placé en résidence surveillé. Quelque mois après sa libération, les autorités chinoises ont confisqué son ordinateur personnel pour récupérer ses contacts et données sensibles.

La surveillance des moines, qui représentent l'un des derniers vecteurs d'information au Tibet, est devenue banale. Les autorités n'hésitent pas à pratiquer de véritables raids dans les monastères. Le 1er septembre, à 10 heures du matin, une soixantaine de véhicules des forces armées de sécurité chinoises, ont débarqué au monastère de Zilkar. Des ordinateurs, les DVD, les documents et les photos se trouvant dans les chambres des moines du monastère ont été saisis.

Dans la nuit du 5 novembre 2012, quelques jours avant l'ouverture du congrès du Parti Communiste Chinois, l'avocat blogueur Shu Xiangxin, spécialiste des droits terriens dans la province orientale du Shandong, a été arrêté et son ordinateur saisi.

Le 9 novembre 2012, le blogueur Cheng Zuo Liang a été emmené au commissariat de la ville de Ningbo (Est) pour subir un interrogatoire au sujet de son implication dans une affaire de construction d'une usine de produits chimiques polluants. Lors de cette arrestation, la police a rappelé au blogueur qu'il avait interdiction de parler à Hu Jia pendant toute la durée du 18ème Congrès. La police a alors fait part de détails de conversations téléphoniques et d'échanges de messages entre les deux dissidents, confirmant que Hu Jia est bien sous surveillance policière.

En avril 2012, l'artiste et militant des droits de l'homme, Ai Wei Wei, avait tourné en dérision le dispositif de surveillance chinois en plaçant 4 webcams dans son bureau et sa chambre le filmant 24 heures sur 24. Le site d'auto surveillance de Ai Wei Wei a été bloqué au bout de quelques heures.

Quelques solutions techniques

Les sites tels que GitHub, qui combinent un service indispensable d'un point de vue économique et des fonctions sociales, sont un véritable challenge pour les autorités chinoises. Les autorités ne peuvent les bloquer ou les surveiller sous peine de pénaliser un pan entier de leur économie. Ce type de service est donc un véritable casse-tête pour les surveillants du web chinois et constitue une porte de sortie pour les internautes chinois.

D'autres services tels que les services de dépôts, des serveurs hébergeant le code source d'applications linux, présentent exactement les mêmes caractéristiques que GitHub et sont un moyen idéal, bien que difficilement accessible aux non informaticiens, pour passer à travers la Grande Muraille électronique.

Après la mise à jour de la Grande Muraille électronique de Chine, les fournisseurs de solutions VPN gratuites et payantes ont fait évoluer leurs technologies. À ce jour, le VPN gratuit Freegate est toujours utilisé et fonctionnel. Du côté des solutions payantes, la société Astrill a été la plus réactive et sa solution parvient encore à contourner les blocages en Chine.

L'année 2012 a démontré que les autorités chinoises sont réactives et savent faire évoluer leur Grande Muraille électronique à l'occasion d'événements majeurs, tel que le scandale Bo Xilai ou le 18e congrès du parti. C'est à un véritable jeu du chat et de la souris que se livrent les techniciens de l'État et les hacktivistes ou les sociétés offrant des solutions de chiffrement et de contournement de la Grande Muraille. Afin de rester efficaces, il faut parvenir à conserver "un coup d'avance" déclare un ingénieur de Freegate, et garder en réserve des mises à jour futures pour les technologies de contournement. La difficulté majeure dans ce "jeu" est de parvenir à fournir aux journalistes et net-citoyens sur le terrain les dernières versions de ces logiciels.

TOUR D'HORIZON DE LA CYBERCENSURE

Une sélection de faits marquants liés à la censure et à la surveillance du Net

RECONNAISSANCE ONUSIENNE DU DROIT À LA LIBERTÉ D'EXPRESSION SUR INTERNET

Le 5 juillet 2012, le Conseil des droits de l'homme de l'ONU affirme pour la première fois le droit à la liberté d'expression sur Internet. La haute instance de Genève affirme que les droits en vigueur dans le monde physique doivent être reconnus également sur Internet indépendamment des frontières. La résolution appelle les Etats "à promouvoir et à faciliter l'accès à Internet et la coopération internationale visant à faciliter le développement des médias et des communications dans tous les pays".

La Conférence mondiale des télécommunications internationales (CMTI)

En décembre 2012 à Dubaï, la Conférence mondiale des télécommunications internationales, organisée par l'Union internationale des télécommunications (UIT), est le théâtre d'une confrontation, voire d'un affrontement, entre des visions de la gouvernance d'Internet et du futur de l'information en ligne. A l'issue des travaux, moins de la moitié des Etats membres de l'UIT (89 sur 193) signent le nouveau traité révisant le Règlement des télécommunications internationales (RTI). Une coalition de 55 États refuse de signer le traité. Parmi ces réfractaires, les États-Unis et les États de l'Union européenne, qui pointent certaines dispositions sur la gestion des spams et la sécurité des réseaux, ainsi qu'une résolution impliquant l'UIT dans la gouvernance du Web, adoptée dans la confusion la plus totale (résolution PLEN/3). Ils clament que ces dispositions pourraient légitimer les efforts de censure et la mise en place de blocage et de filtrage par des pays aux traditions de contrôle du Web.

L'absence de participation de la société civile et de transparence des procédures est vivement critiquée sur le moment par nombre d'ONG, appuyées par le Rapporteur Spécial pour la liberté d'expression aux Nations Unies, Frank La Rue. Occasion manquée de préserver Internet en tant qu'espace d'échanges et de liberté, le sommet de Dubai révèle des luttes d'influence en ligne entre les États. Plus d'informations : Center for Technology and Democracy.

Le traité anti-contrefaçon ACTA rejetée par l'UE

Le 4 juillet 2012, le Parlement européen rejette le traité anti-contrefaçon ACTA, qui menaçait les libertés fondamentales en ligne, et notamment la liberté d'information, la neutralité du Net, l'innovation, l'accès et le partage des technologies libres. Une victoire pour la mobilisation citoyenne qui a vu le jour grâce à l'action de groupes comme La Quadrature du Net et Panoptikon.

Les Pays-Bas et la Slovénie font avancer la neutralité du net, le Brésil piétine

Après les Pays-Bas ou le Chili, au tour de la Slovénie d'adopter, en décembre 2012, une loi qui consacre la neutralité du net et interdit aux fournisseurs d'accès à Internet de discriminer différents types de trafics en ligne. L'adoption de la proposition de loi "Marco Civil" au Brésil continue d'être renvoyée aux calendes grecques suite aux pressions de l'industrie du film et de la musique. Largement soutenue par la société civile brésilienne, qui la considère comme une loi modèle, cette disposition entend définir les droits et devoirs de l'État, des usagers mais aussi des intermédiaires techniques en matière d'usage du réseau Internet, de droit d'auteur et de protection des données personnelles, tout en préservant la neutralité du Net, la vie privée et la liberté de circulation de l'information en ligne.

Le filtrage contraire aux droits fondamentaux ?

Le 18 décembre 2012, dans une décision rendue contre la Turquie, la Cour Européenne des Droits de l'Homme a jugé pour la première fois qu'une mesure de blocage d'un site Internet était contraire à l'article 10. Les juges ont précisé que : "Internet est aujourd'hui devenu l'un des principaux moyens d'exercice par les individus de leur droit à la liberté d'expression et d'information ; on y trouve des outils essentiels de participation aux activités et débats relatifs à des questions politiques ou d'intérêt public". La Cour de justice de l'Union européenne avait déjà précisé dans une décision du 24/11/2011 que le filtrage généralisé portait atteinte aux droits fondamentaux.

Les intermédiaires techniques jouent la carte de la transparence

La dernière édition du "Rapport Transparence" de Google, rendue publique en novembre 2012, indique une forte hausse de la cybersurveillance gouvernementale et montre que "les requêtes gouvernementales relatives aux données des utilisateurs ont régulièrement augmenté depuis la publication de notre premier Transparency Report". En juin 2012, Google s'inquiétait de la recrudescence des demandes de suppression de pages où sont publiés des messages politiques. Il est possible de consulter pays par pays l'évolution des demandes de renseignements sur les utilisateurs ici et les demandes de suppression des contenus ici.

La démarche de Google fait des émules. Twitter lance en juillet 2012 son propre rapport sur la transparence. Il met en avant les requêtes gouvernementales relatives aux données personnelles d'utilisateurs (les Etats-Unis occupent la première place), aux retraits de contenus par des gouvernements ou des ayants-droits. Twitter s'engage également à indiquer par un message tout tweet retiré pour des raisons de copyright et de les transmettre au site Chilling Effects.

OFFENSIVE LEGISLATIVE OU HEMORRAGIE LEGISLATIVE

Surveillance généralisée pour assurer la cybersécurité ?

Les régimes autoritaires n'ont pas le monopole des initiatives législatives liberticides. Des pays considérés comme démocratiques et respectueux des libertés individuelles prennent des initiatives d'autant plus préoccupantes qu'elles justifient ensuite les dérives des premiers.

Grande-Bretagne

En décembre 2012, le Premier ministre adjoint Nick Clegg annonce le retrait du British Communications Data Bill. Ce texte sera donc revu. La première mouture du projet, rendue publique au printemps 2012, visait à instaurer un dispositif de surveillance généralisée des communications en mettant à la disposition du renseignement britannique tous les relevés de communication téléphonique et électronique des citoyens, au nom de la lutte contre les cybercrimes.

Etats-Unis

La proposition de loi américaine Cyber Intelligence Sharing and Protection Act (CISPA) a été accusée par ses détracteurs d'autoriser des violations de la vie privée au nom de la protection de la cybersécurité. Alors qu'elle semblait susciter un large soutien au sein du Congrès américain, elle s'est heurtée à un tollé général qui a permis des modifications substantielles en terme de protection de la vie privée, la menace d'un veto de la Maison Blanche et un nombre très éloquent de votes "contre". Une nouvelle version de CISPA est introduite en janvier 2013 et pourrait être examiné par le Congrès dès avril 2013.

Le Foreign Intelligence Surveillance Amendments Act (FISAA) de 2008 a été renouvelé en décembre 2012 pour une période s'étendant jusqu'à 2017. Ce texte octroie un pouvoir de surveillance exceptionnel à l'État américain. Il autorise celui-ci à accéder aux données des citoyens non américains si ceux-ci utilisent un service de cloud computing mis à disposition par une société américaine.
À titre d'exemple, après l'émission d'un mandat secret émis par un tribunal spécial, ce texte permet aux autorités américaines d'obliger Google à donner accès à l'ensemble des données (emails, documents, contacts, agenda) de l'un de ses clients pour peu que celui-ci ne soit pas citoyen américain. Le parlement européen s'est inquiété de l'étendue de ces nouveaux pouvoirs de surveillance sélectifs dans un rapport, Fighting cyber crime and protecting privacy in the cloud, publié fin 2012.

Pays-Bas

Accusant les outils d'anonymisation tels que Tor de rendre plus difficile la traque des cybercriminels et des pédophiles, le gouvernement a fait pression sur les députés afin qu'ils adoptent une loi destinée à renforcer les pouvoirs de surveillance de la police, y compris hors des frontières nationales. Cette dernière serait ainsi en mesure d'installer des logiciels espions, de fouiller des ordinateurs dans le pays et à l'étranger et de supprimer des fichiers jugés illégaux sur des ordinateurs situé à l'extérieur du pays sans demander auparavant l'assistance légale des gouvernements concernés. Lire l'analyse de Electronic Frontier Foundation.

Philippines

Le 9 octobre 2012, la Cour suprême des Philippines suspend l'application du Cybercrime Prevention Act 2012 (Republic Act n° 10175), qui intégrait la diffamation sur Internet parmi les "cybercrimes". Après avoir reçu une quinzaine de pétitions lui demandant de se prononcer sur la validité de la loi, la Cour s'est prononcée à l'unanimité. Reporters sans frontières demande l'abrogation de ce texte qui, sous couvert d'une lutte légitime contre la cybercriminalité, présente une véritable menace pour la liberté de l'information.

Malawi

Le projet de loi E-Bill obligerait les responsables de publications en ligne à rendre leurs coordonnées personnelles publiques et créerait une cyberpolice chargée d'inspecter les sites Internet à la recherche d'activités illégales. D'après le Media Institute of Southern Africa (MISA), les autorités cherchent ainsi à réguler et contrôler les publications en ligne.

Pérou

Une proposition de loi sur le cybercrime risque de mettre en place de potentielles restrictions à la liberté sur Internet. A l'initiative de l'ONG Access, des universitaires et membres de la société civile péruvienne ont adressé une lettre ouverte au parlement péruvien pour dénoncer ce texte.

Irak

Le Parlement irakien a révoqué en janvier 2013 la loi sur le cybercrime, critiquée pour sa définition très large des délits ("violation des principes religieux, moraux et sociaux") et les sanctions très lourdes prévues (perpétuité pour "utilisation d'ordinateurs" dans le but de "porter atteinte à la réputation du pays"). Lire l'analyse de Access Now.

Protection de l'enfance, l'alibi parfait

Russie

Au nom de la "protection de l'enfance", une liste noire a été mise en place le 1er novembre 2012 par une agence fédérale, pour répertorier les sites Internet "néfastes" promis au blocage sans débat contradictoire ni décision judiciaire. La définition vague et large des contenus visés (pornographie, extrémisme, apologie du suicide et de l'usage de drogue...) et le manque d'indépendance de l'instance de contrôle ouvrent la porte au surblocage.

En outre, un marquage par catégorie d'âge ("interdit aux moins de 6, 12, 16 ou 18 ans") a été imposé à l'ensemble des sites d'information en ligne. Pour garantir une meilleure application de ces dispositions, un projet de loi destiné à interdire les outils de contournement de la censure en ligne a été introduit en commission parlementaire à la Douma.

Canada

Déposé à la Chambre des Communes en février 2012 par le ministre de la Sécurité publique, le projet de loi C-30, appelé Protecting Children from Internet Predators Act, entérine une surveillance disproportionnée de tous les internautes et permet aux autorités d'obtenir des renseignements d'utilisateurs sans mandat judiciaire. Les fournisseurs d'accès à Internet (FAI) et opérateurs de téléphonie mobile pourraient ainsi être obligés de mettre en place des outils pour surveiller et enregistrer les communications de leurs abonnés. La police pourrait également installer, sans mandat judiciaire, un dispositif permettant de relever l'adresse IP de tout appareil connecté à Internet.

Copyright vs liberté d'expression en ligne

Etats-Unis

Les propositions de loi américaines antipiratage, «Stop Online Piracy Act» (SOPA) et «Protect IP Act» (PIPA) ont suscité une énorme mobilisation dans le pays et à l'international, dénonçant des risques de censure du Net sans précédent. En obligeant notamment un site tiers à bloquer l'accès à d'autres sites soupçonnés de violation du droit d'auteur, dont la définition reste vague, elles affecteraient ainsi un nombre incalculable d'internautes sans aucun lien avec des actions de violation de la propriété intellectuelle. Ces deux propositions de loi ont finalement été enterrées. Jusqu'à quand ?

Panama

En septembre 2012, le Parlement adopte la loi 510 qui restreint la liberté d'expression et l'accès à l'information en ligne. Elle donne naissance à une autorité administrative, le Directorat général du copyright, chargée d'identifier les responsables d'infractions et le cas échéant de les condamner - sans décision de justice - à de lourdes amendes. Des ONG et des membres de la société civile ont adressé une lettre ouverte au Président Ricardo Martinelli, lui demandant de ne pas signer la loi, qualifiée de "pire loi de toute l'histoire sur la protection du droit d'auteur". Lire les réactions de net-citoyens sur Global Voices.

Autre législation inquiétante

En Malaisie, un amendement à la Loi sur les preuves de 1950 crée une présomption de culpabilité contre le propriétaire du réseau sur lequel transitent des publications en ligne jugées diffamatoires. Propriétaires de cybercafés ou responsables de plate-formes de blogs sont dans la ligne de mire des autorités. Le Center for Independent Journalism a organisé un mouvement de protestation autour de cette législation.

FILTRAGE À TOUT VA

Internationale du filtrage

Le film L'Innocence des Musulmans est certainement à ce jour l'un des contenus filtrés dans le plus grand nombre de pays. Sa diffusion en ligne a engendré des actions en justice ou des décisions administratives et des blocages de YouTube, voire des communications en Arabie Saoudite, en Afghanistan, au Pakistan, au Bangladesh, en Egypte, en Turquie, en Russie, au Kazakhstan, au Kirghizstan, en Inde, au Bahreïn, etc.

Chine - Course à la montre

Les censeurs chinois ont eu fort à faire pour tenter d'endiguer la diffusion en ligne d'informations sur des affaires sensibles qui se sont multipliées ces derniers mois :
- enquête du New York Times sur la fortune du Premier ministre Wen Jiaobo et de sa famille,
- résistance à la censure de l'éditorial du Nouvel An du Nanfang Zhoumo appelant à des réformes constitutionnelles en Chine,
- multiplications des immolations au Tibet,
- affaires de corruption,
- critiques de la gestion des inondations de l'été 2012.

Un effort particulier a été fourni à l'approche du Congrès du parti communiste qui a désigné la nouvelle équipe dirigeante et placé Xi Jinping à la tête du pays.

La censure d'Internet gagne du terrain en Asie centrale

Au-delà de l'Ouzbékistan et du Turkménistan, "ennemis d'Internet" de longue date, la cybercensure tend à se banaliser en Asie centrale.

Au Tadjikistan, l'année 2012 a été marquée par plusieurs vagues de blocage de sites d'information de référence tels que Asia Plus, RIA-Novosti, BBC, Radio Ozodi, Lenta.ru, Fergananews.com, Centrasia.ru, ainsi que YouTube et Facebook. Le service national des Télécommunications a pris l'habitude d'intimer des ordres de blocages aux fournisseurs d'accès pour empêcher la circulation d'informations sensibles : enquêtes mettant en doute la stabilité du régime, couverture d'affrontements armés, critiques à l'encontre du Président de la République sur les réseaux sociaux...

En décembre 2012, la justice kazakhe a interdit les principaux médias d'opposition nationaux, jugés "extrémistes" au terme de parodies de procès. Cette mesure implique le blocage au Kazakhstan de l'ensemble des sites Internet relayant les journaux Respublika et Vzgliad, ainsi que leurs comptes sur les réseaux sociaux. La chaîne de télévision en ligne K+ et le portail d'information Stan.tv ont également été bloqués.

En Inde, la censure pour étouffer les rumeurs ?

En août 2012, pour tenter de mettre un terme à de violents troubles inter-ethniques, les autorités indiennes ont ordonné aux fournisseurs d'accès à Internet, de bloquer l'accès à plus de 300 contenus en ligne. Si certains incitaient en effet à la violence en relayant des rumeurs infondées, d'autres présentaient un caractère informatif (des pages du site d'informations de la chaîne australienne ABC et d'Al-Jazeera, ainsi que des photos de l'AFP - voir la liste publiée par le Center for Internet and Society).

La Grande Muraille électronique pakistanaise : réalité ou fiction ?

Un projet gouvernemental de filtrage du Web au Pakistan a été révélé en début d'année 2012. Il viserait à mettre en place un système permettant de filtrer et bloquer des millions de sites web "indésirables", en utilisant la technologie "DPI" (Deep Packet Inspection). D'après le Daily Times, le Fonds national de recherche et développement rattaché au ministère des Technologies et de l'Information aurait émis un appel d'offres pour un montant de 10 millions de dollars, en février 2012, auxquelles plusieurs entreprises étrangères auraient répondu. Une pétition a été lancée pour appeler les entreprises à ne pas répondre à l'appel d'offre du gouvernement. Des articles de presse ont ensuite relayé des déclarations de responsables politiques s'opposant au projet. La société civile pakistanaise reste vigilante.

ACCÈS RESTREINT ?

Deux milliards de personnes bénéficient à ce jour d'un accès à Internet. Un tiers d'entre elles souffre d'un accès limité en raison de censure gouvernementale, de filtrage et de surveillance. Des problèmes de développement d'infrastructures limitent parfois l'extension de cet accès. Tout comme des considérations purement politiques.

Internet national en Iran

En septembre 2012, le gouvernement accélère la mise en place d'un réseau parallèle, doté d'une vitesse de connexion élevée, surveillé et censuré dans son intégralité. Justification officielle? Les cyberattaques contre les installations nucléaires du pays. A terme, les serveurs locaux sont censés héberger tous les sites iraniens. Les applications et services tels que boîtes mails, moteurs de recherche, réseaux sociaux et opérateurs devraient être développés sous le contrôle du gouvernement. Seules les administrations sont pour l'instant connectées au réseau national, mais il est à craindre que les citoyens iraniens n'aient à terme pas d'autre choix que de leur emboîter le pas. (Lire le chapitre Iran - Champion de la Surveillance).

Coupures régulières en Syrie

Des suspensions de communications et d'Internet se produisent régulièrement dans des endroits ciblés. Il faut également compter sur les coupures d'électricité. Fin novembre 2012, la Syrie est complètement déconnectée d'Internet au moment où le régime est accusé de planifier un massacre à l'échelle nationale.

Le haut-débit et la fibre optique enfin disponible à Cuba ?

Le câble sous-marin vénézuélien apportant la fibre optique et le haut-débit à Cuba, opérationnel depuis 2011, a été mis en service seulement en août 2012, comme l'a constaté la société spécialisée en réseaux, Renesys. D'après Global Voices, un article du quotidien officiel Granma note que la phase de test a beau être terminée, les Cubains ne doivent pas s'attendre à une augmentation drastique de leurs opportunités d'accès au Web à court terme. Jusqu'ici, l'île utilisait des liaisons satellites pour des accès très limités au Web (lire le chapitre Cuba des Ennemis d'Internet 2012).

Discriminations régionales

Le Tibet et le Xinjiang sont coutumiers des suspension de l'accès à Internet ou des communications en période de crise (lire le chapitre Chine des Ennemis d'Internet 2012).

En août dernier, jour de la célébration du 66ème anniversaire de l'indépendance de l'Inde, un événement sensible, les opérateurs téléphoniques suspendent leur service dans la vallée du Cachemire, suite à une décision du gouvernement de l'Etat du Jammu-Cachemire.

A l'occasion de l'anniversaire de l'indépendance du Pakistan en août 2012, les réseaux de téléphones portables sont coupés temporairement dans la province du Balouchistan.

NET-CITOYENS PRIS POUR CIBLES

Hommage

Quarante-sept net-citoyens et citoyens-journalistes ont été tués dans le monde en 2012, la plupart en Syrie. Sans l'action de ces reporters, photographes ou vidéastes, le régime syrien serait en mesure d'imposer un blackout total de l'information dans certaines régions et de massacrer à huis clos.

En Iran, le blogueur **Sattar Beheshti,** incarcéré le 31 octobre 2012, a perdu la vie dans des circonstances inconnues. Les éléments actuels portent à croire qu'il a succombé à des coups reçus lors de son interrogatoire. Les responsables de sa mort n'ont toujours pas été inquiétés.

Au Bangladesh, le blogueur **Ahmed Rajib Haider** a été égorgé en 15 février 2013 près de son domicile dans la capitale, Dacca.

Au Pakistan, la jeune blogueuse **Malala Yousufzai,** 14 ans, cible des Taliban, a échappé de peu à la mort.

D'arrestations en rafles

Près de 180 net-citoyens sont incarcérés à ce jour pour leurs activités d'information. Les cinq plus grandes prisons du monde pour les net-citoyens sont dans l'ordre la Chine (69), Oman (32), Vietnam (31), l'Iran (20) et la Syrie (18).

Des arrestations en masse - voire des rafles - se sont déroulées en Syrie, mais également dans le Sultanat d'Oman ou en Iran, lors du "Dimanche noir". Au Sri-Lanka, ce sont neuf employés du journal en ligne Sri Lanka Mirror qui ont été pris dans un coup de filet en juillet 2012.

Le Vietnam continue d'arrêter des net-citoyens à tour de bras et de les condamner à de lourdes peines de prison, en témoignent les douze années de prison dont a écopé le célèbre blogueur Dieu Cay. Des moines tibétains soucieux de témoigner des immolations finissent derrière les barreaux. L'Azerbaïdjan s'en prend aux blogueurs qui s'écartent de la ligne officielle.

Les conditions de détention de ces net-citoyens sont très souvent déplorables, les mauvais traitements récurrents. Certains - notamment en Iran - ne reçoivent pas les soins médicaux adéquats. Leurs jours sont en danger.

Violences et menaces

Au Bangladesh, en février 2013, ce sont 19 blogueurs qui ont été ouvertement menacés sur des sites Internet islamistes, et au cours de manifestations, en marge du procès de plusieurs anciens leaders de partis islamistes, dont le parti Jaamat-E-Islami.

Au Mexique, une page Facebook "Courage for Tamaulipas", qui couvre les violences infligées à la région par le crime organisé, suscite l'ire des trafiquants. Ces derniers promettent 600 000 pesos (soit près de 46 000 USD) à qui découvrira la véritable identité du responsable de cette page Facebook.
Des menaces ont conduit le blogueur Ruy Salgado, responsable du site El Santuario, notamment célèbre pour ses couvertures d'affaires de corruption, à abandonner ses activités en ligne.

Les proches des net-citoyens engagés, notamment des détenus, subissent souvent harcèlement, pression et font l'objet de menaces. C'est le cas en Iran, en particulier pour les familles des journalistes ou blogueurs iraniens basés à l'étranger, mais aussi au Vietnam. Ta Phong Tan, créatrice du blog La justice et la vérité, qui a écopé de dix années de prison, a payé encore plus cher le prix de son engagement : en juillet 2012, sa mère s'était donné la mort en s'immolant devant les bureaux du Comité populaire de Bac Lieu.

Procès de Bradley Manning, "donneur d'alerte" pour WikiLeaks

Le soldat américain Bradley Manning a reconnu, le 28 février 2013, devant la cour martiale qui le juge, avoir transmis des documents militaires et diplomatiques au site WikiLeaks. Qu'aurait-il transmis ? Des câbles diplomatiques américains, des dossiers de détenus de Guantanamo, des vidéos de frappes aériennes dans lesquelles des civils ont trouvé la mort. La vidéo la plus célèbre, Collateral Murder, montre une attaque aérienne de l'armée américaine en Irak en juillet 2007, au cours de laquelle deux employés de l'agence Reuters et une dizaine d'autres personnes avaient été pris pour cibles et tués. La motivation de Manning : "éclairer le public sur ce qui se passe" et "susciter un débat sur la politique étrangère". Il a expliqué avoir tenté en vain de transmettre ces documents au New York Times et au Washington Post. Et avoir choisi avec soin les documents révélés afin que leur publication ne soit pas nuisible. Il risque 20 ans de prison. De nombreuses ONG ont dénoncé les conditions dégradantes de détention dont il a fait l'objet.

Parallèlement, la société DataCell, qui collectait les donations pour WikiLeaks, a saisi la Commission européenne, pour violation des règles communautaire de concurrence, suite à la suspension des moyens de paiement à WikiLeaks (mise en place) par Visa Europe, Mastercard et American Express en décembre 2010. La Commission a indiqué dans une décision préliminaire que cette suspension n'était probablement pas de nature à violer le droit européen de la concurrence.

ACTES DE RÉSISTANCE MOBILISATION EN LIGNE

Face à l'offensive des gouvernements et groupes d'intérêts soucieux de contrôler le Web, les net-citoyens et acteurs de l'information en ligne ont su se mobiliser et faire acte de résistance, avec plus ou moins de succès.

Parmi les initiatives notables de ces derniers mois :

- Le phénomène des "mèmes" Internet, ces éléments ou phénomènes repris et déclinés en masse sur Internet, donnant naissance à une forme de culture populaire sur le Web. Ils utilisent, notamment en Chine, l'humour et des montages avec Photoshop pour se moquer de problèmes sociaux ou politiques et contourner ainsi les filtres des censeurs. Pour exemple, Grass Mud Horse ou les graines de tournesol de l'artiste Ai Weiwei room full of sunflower seeds.

- La résistance en ligne contre la censure de l'éditorial du journal chinois Nanfang Zhoumo réclamant, à l'occasion de la Nouvelle année, des réformes constitutionnelles.

- Le rôle joué par WCITLeaks pour plus de transparence dans la négociation sur le nouveau traité de l'UIT à la Conférence mondiale des Télécommunications de Dubaï, en décembre 2012

- La campagne de La Quadrature du Net contre le traité anti-contrefaçon ACTA

- La première campagne Stop Cyber Spying, une semaine de mobilisation en ligne contre la proposition de loi américaine Cyber Intelligence Sharing and Protection Act of 2011 (CISPA), et la nouvelle campagne du même nom en réponse à la proposition de loi américaine Cybersecurity Act of 2012 (CSA).

- La campagne Save Your Voice, fruit de la mobilisation de la société civile et des internautes indiens demandant l'abrogation des IT Rules, une législation dangereuse pour la liberté d'expression sur Internet. Deux cyberactivistes ont même mené une grève de la faim.
- Le blackout de 500 sites Internet en Jordanie le 29 août 2012 pour protester (#BlackoutJO et #FreeNetJO) contre des amendements liberticides à la loi sur la presse et les publications.

- La campagne Stop Online Spying, lancée en septembre dernier par l'organisation canadienne Open Media avec une pétition contre le projet de loi C-30.

- La campagne pour un Internet libre en Azerbaïdjan, menée à l'occasion de la tenue du 7e Internet Governance Forum à Bakou en novembre 2012 (en particulier, par la plate-forme Expression Online)

- L'initiative Rublacklist, lancée par le Parti pirate russe en réponse au filtrage du Net : l'équipe réalise un monitoring régulier des blocages, propose des outils de contournement de la censure en ligne, et fournit des sites miroirs ou des solutions d'hébergement aux sites bloqués injustement.

Envoyez-nous des informations sur les campagnes de défense de la liberté d'expression et d'information en ligne portées à votre connaissance.

LEXIQUE

Cloud computing
également appelé "informatique en nuage" désigne l'utilisation de serveurs distants pour accéder et stocker des informations. Gamil, evernote, Dropbox sont parmi les service de cloud computing les plus connus du grand public. Le Cloud computing permet d'accéder à ses données à tout moment de puis n'importe quel poste, ordinateur ou téléphone portable. L'inconvénient de cette facilité d'accès est que le propriétaire des données n'a pas la maîtrise pas de la localisation de ses informations.

DPI
Le Deep Packet Inspection, littéralement "inspection en profondeur des paquets" permet d'intercepter et d'inspecter les paquets de données transitant sur le réseau Internet. Dans un contexte de surveillance, l'utilisation du DPI peut permettre d'accéder au contenu d'emails, de conversations instantanées et d'échanges par VoIP et de découvrir si une communication est chiffrée ou non. Plus le type d'information recherchée est précis, plus les ressources nécessaires pour les systèmes de DPI sont importantes.

ETSI
l'Institut européen des normes de télécommunication. L'ETSI est un organisme à but non lucratif dont le butr est de pondre des normes de télécommunications.

Hacktivistes
contraction du mot "hacker" et activiste. Les hacktivistes sont des hackers qui mettent leurs compétences informatiques au service de leurs convictions politiques. Le champs d'action de l'hacktivisme s'étend de la formation, du développement d'outils de contournement de la censure à destination de militants des droits de l'homme, jusqu'aux opérations coup de poings telles que l'intrusion informatique, le détournement de données et le défaçage de sites.

HTTPS
https, hyper text transfer protocol secured, est un protocole de transport d'information sur Internet. Il combine le protocole http, permettant d'afficher les pages sur le web, avec une couche de chiffrement, TLS ou SSL. Ce protocole permet de s'assurer que la liaison entre l'ordinateur accédant à une page web et le serveur qui l'héberge est chiffrée de bout en bout. Le protocole https est souvent utilisé dans le cadre de transactions financières sur Internet afin de protéger les coordonnées bancaires des internautes. La sécurité du protocole https repose sur l'échange de certificats, assimilable à la carte d'identité du site web et du navigateur de l'internaute, entre le serveur et le visiteur. Dans le cadre d'un réseau surveillé, si les certificats des serveurs ne sont pas compromis, l'utilisation du protocole https empêche tout attaquant d'accéder aux données échangées sur un site web, données de formulaires envoyées ou pages consultées.

MITM
Man in the Middle Attack ou Attaque de l'Homme du Milieu, cette attaque permet de casser le chiffrement des données échangées par l'intermédiaire d'une connection SSL ou TLS, dans le cas de l'accès à un site en https par exemple. L'attaquant se place entre le client (l'internaute) et le serveur (le site web https) et usurpe l'identité du serveur à l'aide d'un faux certificat ou d'un certificat reconnu mais compromis. Des attaques MITM très sophistiquées ont été utilisées en Iran en 2011 lorsque la société Diginotar, éditrice de certificats, avait vu ceux-ci compromis par des pirates informatiques.

Neutralité du Net
C'est un principe qui garantit la non discrimination dans le traitement de flux internet. Sur Internet, un paquet de données doit être acheminé de la même manière quel que soit le contenu transporté, emails, message instantanné, page Web, VoIP, vidéo, etc. et quels qu'en soient l'expéditeur et le destinataire.
En assurant l'égal traitement des flux d'information, la neutralité du Net permet de garantir à chacun de s'exprimer librement, dans les limites fixées par la loi, et d'accéder à l'information ou aux services qui lui plaisent, qu'ils soient payants ou non.

Phishing ou hameçonnage
technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance - banque, administration, etc. -afin de lui soutirer des renseignements personnels
mot de passe, numéro de carte de crédit, date de naissance, etc.

Proxy ou serveur mandataire
Un proxy est un logiciel qui s'intercale entre deux éléments d'un circuit de transmission de données. A l'échelle nationale, un proxy placé entre les utilisateurs d'un réseau et le reste du monde permet de mettre en place un système de filtrage et de surveillance. Ces logiciels reçoivent toutes les requêtes Web effectuées par les utilisateurs, les interceptent et les transmettent vers les sites légitimes demandés. Pendant l'interception, selon le paramétrage du proxy, il est possible de bloquer des sites web, d'identifier quel internaute se connecte sur quel site, et de récupérer des informations personnelles (mots de passe, nom d'utilisateur, adresse IP).

RAT, spyware, malware, trojan
Les RAT (Remote Acces Trojan) sont des logiciels espions, également appelés malware ou spyware trojan ou chevaux de Troie. Une fois installés sur un ordinateur ou un téléphone, ils permettent d'accéder à l'ensemble des fichiers d'une machine. Ces logiciels peuvent avoir accès au micro, à la webcam et aux frappes clavier permettant ainsi de récupérer non seulement des mots de passe mais également des conversations skype ou d'espionner une personne à son insu. L'ensemble des informations obtenues est envoyé à un serveur permettant à l'attaquant de les récupérer.

VPN
un VPN (Virtual Private Network) permet de créer un tunnel (une liaison virtuelle) entre deux réseaux physiques géographiquement distants. Les données envoyées au travers de ce tunnel sont chiffrées. Ceci garantit aux utilisateurs d'un VPN qu'en cas d'interception malveillante (espionnage, intrusion, etc), les données soient illisibles pour des tiers. Lisez l'article sur les VPN dans notre kit de survie numérique.

REPORTERS WITHOUT BORDERS
FOR FREEDOM OF INFORMATION

SECRÉTARIAT INTERNATIONAL DE REPORTERS SANS FRONTIÈRES

47 rue Vivienne, 75002 Paris, France - Tel : 33 1 4483-8484 - Fax : 33 1 4523-1151 - Site internet : www.rsf.org - E-mail : rsf@rsf.org - Ambroise Pierre - Bureau Afrique : afrique@rsf.org - Benoît Hervieu - Bureau Amériques : ameriques@rsf.org - Benjamin Ismaïl - Bureau Asie : asie@rsf.org - Johann Bihr - Bureau Europe : europe@rsf.org - Soazig Dollet - Bureau Moyen Orient : moyen-orient@rsf.org - Lucie Morillon - Bureau Internet : internet@rsf.org - contactPresse : presse@rsf.org

Equipe éditoriale : Grégoire Pouget, Hauke Gierow, Reza Moini, Benjamin Ismail, Pierre Belmont, Soazig Dollet, Benoît Hervieu, Johann Bihr, Ambroise Pierre, Antoine Héry, Olivier Basille | Maquette : Sandrine Edery | Rédactrice en chef : Lucie Morillon