IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

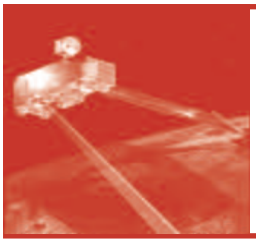
OBSERVATOIRE GÉOSTRATÉGIQUE
DE L'INFORMATION

2 mai 2012

Technologies de libération vs contrôle technologique

SOUS LA DIRECTION
DE FRANCOIS-BERNARD HUYGHE

CHERCHEUR A L'IRIS



OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

Contrôle et guérilla à l'ère numérique

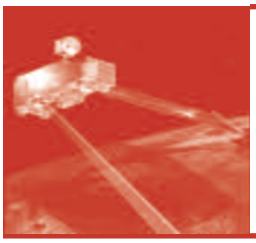
Il y a environ un an, nous consacrions un numéro aux révoltes du monde arabe. Certains les baptisaient « 2.0 », aussi irrésistibles et contagieuses que le numérique lui-même. Nous disions que la question n'était pas seulement d'une part, des réseaux sociaux dans les événements, mais aussi la lutte qui allait opposer méthodes et outils aidant la contestation (pas forcément démocratique) à s'exprimer et s'organiser (dont les médias sociaux accessibles à chacun), et d'autre part, les moyens qui permettent de les surveiller et de les réprimer. Des exemples comme celui de la Syrie ne nous ont pas démentis. D'où ce premier bilan du rapport entre innovation technologique ou stratégique et lutte politique.

Plusieurs auteurs, qui ne sont d'ailleurs pas forcément d'accord entre eux, s'y expriment. Lucie Morillon dresse un bilan peu rassurant des méthodes, nombreuses et efficaces, employées par des États pour lutter contre la cyberdissidence. Nicolas Arpagian montre le lien entre demande de sécurité ou pratiques commerciales de nos pays et techniques de surveillance des dictatures. Adrien Gévaudan souligne que l'enjeu des techniques de contrôle et de cyberdissidence concerne aussi les démocraties du Nord

Bertrand Boyer traite de l'anonymat des utilisateurs, véritable interface avec la « vraie vie » où l'on se fait vraiment arrêter. Et du côté des technologies de libération (terminologie à laquelle nous consacrons une analyse) ? Une interview de Philippe Blanc éclaire l'exemple des PirateBox. Charles Bwele applique au cas chinois le « dilemme du dictateur » c'est-à-dire le développement des réseaux au risque de contestations politiques ou leur refus qui se paie en termes de développement. Yannick Harrel pose la question de l'épée et du bouclier. Quelles technologies l'emporteront ? Celles qualifiées de « libération » ou plutôt celles de « contrôle » ? Nous avons finalement fait débattre ces deux auteurs avant de présenter un glossaire pour éclairer l'aspect technique inévitable de la question.

Sans déterminisme technologique nous avons voulu fournir quelques éléments de réponse à la question : qui gagne ? Il y a plusieurs décennies que l'on oppose un Big Brother technologique (tout laisse une trace, tout est surveillé) à une Agora électronique (tout le monde participe, rien n'est contrôlable)... Mais la question se pose maintenant en termes nouveaux avec des technologies pensées dans un dessein stratégique. ■

François-Bernard Huyghe



OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

Internet : l'impossible contrôle ?

par Lucie Morillon
Responsable du bureau Nouveaux médias à Reporter sans frontières (RSF)

Les « Printemps arabes » ont vu la consécration du rôle de mobilisation et d'information joué par le Web. Déclenchant une riposte cinglante de régimes désireux d'asseoir leur contrôle de l'information. Des plus radicaux aux plus subtils, tout un éventail de moyens ont été déployés. Après le Népal en 2005, puis la Birmanie en 2007, l'Egypte a eu recours, en 2011, à une coupure totale de l'accès à Internet. Le Tibet ou la région de Janaozen au Kazakhstan ont également été déconnectés lors de révoltes.

Développement de réseaux parallèles et ségrégation digitale

Le régime birman a lancé, en 2010, un nouveau portail Internet national, qui permet aux autorités d'une part, et au reste de la population d'autre part, d'avoir accès au Web via des fournisseurs d'accès différents. Se donnant ainsi les moyens, à la prochaine crise, de couper l'accès « seulement » au citoyen lambda. A Cuba, deux réseaux co-existent : un intranet ultra-censuré et un accès au World Wide Web réservé principalement aux touristes et à l'élite. L'Iran a annoncé le lancement d'un « Internet national » ou « Web propre » destiné à défendre les valeurs de la République islamique.

Ralentissement de la bande passante. L'Iran est passé maître en la matière. En amont de manifestations, l'envoi d'images devient alors extrêmement laborieux voire impossible.

Immobilisation par attaques DDoS. Sous la forme de dénis de service distribués (DDoS), les sites visés sont alors paralysés. Plusieurs sites d'informations russes ont ainsi été rendus inaccessibles pendant les élections législatives de décembre 2011. Des sites érythréens, sri lankais, vietnamiens... sont souvent victimes de ce type d'attaques.

Fermetures de sites. Des gouvernements ont la possibilité de faire fermer des sites, dès lors qu'ils sont hébergés dans le pays concerné.

Filtrage du Net : blocages et mots clés. Quand la fermeture pure et simple n'est pas une option, le filtrage du Net s'exerce sous la forme d'un blocage technique, selon trois méthodes différentes : le blocage par URL, par adresse IP, ou par nom de domaine. L'Arabie Saoudite, la Thaïlande, l'Iran, la Chine et même la Turquie, pour n'en citer que quelques-uns, en ont fait une routine. Le filtrage est souvent basé sur des listes noires gérées par des autorités administratives opaques, et/ou effectué via des logiciels tels que Smartfilter. Certains pays appliquent un blocage par « mots clés ». Des URL ou des résultats de moteurs de recherche sont alors bloqués en fonction de mots « interdits », par exemple « femme » en Iran ou « jasmin » sur le Web chinois. Le filtrage peut aussi s'effectuer avec l'aide des moteurs de recherche, qui acceptent de s'autocensurer, comme Yahoo! et Bing en Chine. Via le « notice and take down », si un site est basé dans la juridiction compétente, les autorités ont la possibilité de contacter l'hébergeur concerné pour réclamer le retrait de contenus, sous peine de poursuites ou de dommages et intérêts. Si le filtrage du Net a été renforcé ces derniers mois, la surveillance est la priorité absolue des censeurs. Les dissidents arrêtés au Bahreïn sont torturés pour les obliger à donner les identifiants et mots de passe de leurs comptes Facebook, Twitter, Skype, etc. Le recours au hameçonnage (« phishing ») se répand. ■■■

Le déblocage de Facebook en 2011 en Syrie a été suivi par des attaques destinées à subtiliser les codes d'accès des internautes à Facebook par l'utilisation de certificats de sécurité frauduleux. Des entreprises occidentales comme BlueCoat, AreaSpa ou Amesys, ont été publiquement épinglées pour avoir fourni à des régimes qui violent de manière flagrante les droits de l'homme du matériel de censure et de surveillance fournissant des capacités de tracer les communications et leurs contenus, souvent par l'utilisation de la technique du Deep Packet Inspection. Ces entreprises sont les nouveaux mercenaires de l'ère digitale.

Infiltration/compromission

La protection de leurs réseaux demeure l'un des enjeux majeurs rencontrés par les militants. Les autorités n'hésitent pas à tenter d'infiltrer les groupes de dissidents sur les réseaux sociaux. Désormais, à côté de l'armée traditionnelle, des cyberarmées se forment, avec un but très clair : le contrôle de l'information en ligne. La cyberarmée syrienne noie régulièrement les commentaires critiques du pouvoir dans une masse de commentaires positifs.

Sabotage en ligne. Au Bélarus, le fournisseur d'accès BelTelecom a redirigé, en 2011, les internautes cherchant à se connecter au réseau social Vkontakte, très utilisé pour les mouvements pacifiques de protestation, vers des sites contenant des logiciels malveillants. Le régime syrien, en prenant le contrôle de comptes Facebook, a aussi voulu compromettre des militants en polluant leurs murs avec des informations fausses afin de remettre en cause leur crédibilité.

Propagande pure et dure

La propagande connaît de beaux jours. La Corée du Nord a porté sur le Web sa guerre de propagande contre les Etats-Unis et la Corée du Sud. A Cuba, les blogueurs critiques sont régulièrement attaqués dans les médias d'Etat et sur les blogs « révolutionnaires » et qualifiés de « mercenaires » à la solde des Etats-Unis. Les « 50 cent » en Chine – ces internautes à la solde du Politburo – ont tenté d'étouffer le scandale autour de la mort d'un berger de Mongolie intérieure, arguant qu'il s'agissait d'un simple accident de la route.

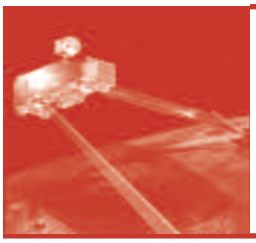
Chasse aux sorcières. De plus en plus de net-citoyens trouvent la mort. Ils étaient cinq en 2011, déjà certainement plus du double depuis le début de l'année 2012. Le nombre de net-citoyens arrêtés en 2011, soit de manière illégale, soit grâce au renforcement de l'arsenal législatif qui gouverne les activités en ligne, a augmenté de 30 % en un an. L'auto-censure en sort renforcée.

La censure du Net est-elle vaine ?

Toutes ces méthodes ont leurs limites : la coupure de l'accès coûte cher à l'économie d'un pays. Le filtrage est contournable et présente des risques de surblocage et de ralentissement de la bande passante. Un site fermé réapparaît souvent sous un autre nom de domaine. La surveillance peut être réduite par l'utilisation d'outils d'anonymisation et de protection des données et le développement de systèmes d'alerte et de collaboration entre dissidents, ONG et hacktivistes.

Plus que jamais, le bras de fer continue entre partisans d'un Internet libre et chantres du contrôle de l'information à l'ère digitale.

*
* * *
*



OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

IRIS INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

Société du fichage vs Société de défiance : qui remportera la mise ?

par Nicolas Arpagian,
Directeur scientifique du cycle Sécurité numérique à l'INHESJ,
Auteur, notamment, de* La Cybersécurité, *coll. Que Sais-Je ? (PUF)

Le début de l'enquête qui a suivi les assassinats de Toulouse et de Montauban intervenus au printemps 2012 a montré l'importance accordée désormais dans les investigations policières aux données de connexion : téléphoniques ou informatiques. Avec en conséquence, un sentiment d'impuissance lorsque les premiers indices ne font émerger aucun de ces identifiants numériques. Ce qui est le cas, par exemple, lorsque le criminel procède seul et n'échange donc pas de courriels avec des complices. De même lorsqu'aucune communication téléphonique entre acolytes ne vient renseigner les enquêteurs sur la présence de personnes sur la scène de crime ou sur d'éventuelles relations préalables entre comparses.

Dans de telles circonstances, l'absence de traces numériques favorise nettement les criminels qui peuvent se fondre plus durablement dans un anonymat qui les protège. Face à une possible impunité, l'opinion publique se réjouit alors que les moyens techniques de traçage numérique permettent d'identifier au plus vite les suspects potentiels. Afin d'accélérer le retour à la normale.

Vers la fin de l'anonymat ?

Le bien-fondé de la surveillance numérique ne fait alors plus débat pour l'essentiel de la population : c'est au contraire un bienfait qui permet d'impliquer les coupables et de disculper les innocents. Tout irait donc pour le mieux dans le meilleur des mondes possibles. D'ailleurs, les citoyens-consommateurs ont déjà depuis longtemps accepté de plein gré de renoncer à une part conséquente de leur anonymat sur les réseaux.

Qu'il s'agisse de choisir un téléphone Android ou Apple qui assure par défaut la géolocalisation constante de son propriétaire, aux applications qui vous incitent à vous localiser (FourSquare par exemple) à votre appareil photo qui mentionne par défaut les dates et horaires des prises de vue, ou à ses cartes de fidélité qui recensent et collationnent dans une base de données centrale le détail de vos achats. Dis-moi ce que tu consommes, où et quand… et je te dirai qui tu es !

Si la tendance d'inscriptions se poursuit, Facebook devrait compter au mois d'août 2012 un milliard d'inscrits. Même si de nombreux internautes y participent sous des identités multiples et si les comptes inactifs sont fréquents, il s'agit là d'une base de données personnelles sans équivalent à l'échelle planétaire. Cursus professionnel, centres d'intérêts, liens amicaux, réseaux de connaissances… un assemblage à très grande échelle de ce qui fait la singularité d'un individu. On imagine l'émoi dans la population si un Etat, même démocratique, s'ingéniait à stocker pour son compte une telle masse d'informations sur sa population.

Le fait qu'il s'agisse d'une firme soumise selon ses conditions générales d'utilisation au seul Droit des Etats-Unis ne semble pas susciter de discussion. Même si des procédures judiciaires en cours commencent timidement à ■■■

■■■ reconnaître la compétence des juridictions françaises pour traiter d'éventuels contentieux avec la compagnie fondée par Marc Zuckerberg. La capacité d'indignation relative au fichage des comportements sur la Toile semble donc toute relative… et à géométrie variable.

Vues des régies publicitaires de Google et de Facebook, ce suivi à la trace de la navigation sur la Toile est volontiers présenté comme une nécessité pour offrir à l'internaute un service toujours plus personnalisé, tandis que dans les régimes autoritaires un même pistage des échanges sur le Net sert à identifier les meneurs des mouvements de rébellion et à surveiller les mouvements d'opinion.

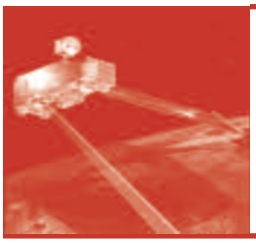
Pour mieux les contrecarrer. Il est d'ailleurs frappant de constater que si les chancelleries du monde entier peinent à aboutir à la rédaction d'un Droit international de l'Internet, les plus offensifs sur ce terrain de la surveillance numérique sont à ce jour les dictatures et… les puissances économiques. En effet, la fermeture début 2012 du site d'hébergement de contenus MegaUpload et l'avancée de textes comme le Protect Intellectual Property Act (Pipa), le Stop Online Piracy Act (Sopa) sont des illustrations flagrantes de l'édification d'une réglementation du Net largement poussée par les multinationales. Même si l'examen de ces textes est provisoirement suspendu le temps de l'élection étatsunienne, leur avancement tranche avec la décennie prise par de nombreux Etats occidentaux pour ratifier la Convention de Budapest de novembre 2001 du Conseil de l'Europe relative à la cybercriminalité. Rien de tel que des lobbyistes généreusement rémunérés pour donner du rythme à un calendrier politique.

Quelles limites pour quelles surveillances ?

Le constat est amer : les démocraties se font ici largement tenir la plume par les intérêts commerciaux. Et cela manque tragiquement de réflexion et d'apport politique sur le fond. Dans les régimes autocratiques, le contrôle du Net est devenu une composante indispensable d'un maintien en place ou pour le moins un relatif retard dans la chute du système.

Entre ces deux tendances concomitantes à la mise en coupe réglée des comportements sur la Toile, on constate un phénomène original de riposte militante. Qui tend à diffuser auprès d'un public qui va désormais au-delà de la communauté des informaticiens les techniques de base de chiffrement et de signature de leurs messages. Histoire de proposer des solutions alternatives à l'amorce d'une société du contrôle tous azimuts. D'autant plus que les mécanismes de surveillance tendent à se banaliser. Ainsi la Grande-Bretagne, patrie depuis le Haut Moyen-Âge de l'Habeas Corpus a-t-elle relancé le 1er avril 2012 un projet parlementaire déjà initié en 2009 de contrôle systématique des courriels et des communications sur les médias sociaux sur l'ensemble du territoire britannique. Sans que cela déchaine pour l'instant de tonnerres de protestations. Le débat parlementaire, lorsque le texte sera officiellement inscrit à l'ordre du jour, sera donc un bon indicateur de l'acceptation de la surveillance par les uns et des besoins de contrôle par les autres. A n'en pas douter, une étape majeure pour la construction démocratique moderne. ■

*
* * *
*



Cyberdissidence et changement social : les sociétés de l'information libre

par Adrien Gévaudan,
Consultant en intelligence économique,
Rédacteur pour Intelligence-Strategique.eu

Refuser la légitimité d'une autorité, contester un pouvoir en place, agir contre un système politique ; autant de manifestations de dissidence. Accoler le préfix cyber ne change en rien le sens fondamental de cette action essentiellement politique ; en revanche, cela indique les moyens utilisés pour mener cette action. La cyberdissidence désigne ainsi un comportement politiquement contestataire utilisant à ses fins le cyberespace et les technologies s'y rapportant.

Cependant, au-delà de toute définition (acadamico-)théorique, se pose la question pratique du rôle de cette nouvelle forme de dissidence dans les relations de pouvoir entre acteurs du monde de l'information. Les transforme-t-elle ? S'inscrit-elle dans la continuité des mouvements contestataires historiques ? Touche-t-elle uniformément les sociétés, les acteurs, les individus ? Autant de problématiques complexes auxquelles nous essaierons d'esquisser des réponses.

Une nouvelle dichotomie Sud-Nord

Il y a un peu plus d'un an, toujours prompts à s'enflammer au moindre fait divers croustillant, les médias louaient les révolutions arabes pour leur instrumentalisation novatrice des réseaux sociaux. Il faut cependant relativiser l'innovation et la portée de cette utilisation politique du cyberespace. Le propre de ce qui a été appelé le Web 2.0, contrairement à l'image que peut s'en faire le grand public, ne réside pas dans une hypothétique innovation technologique, mais bien dans la démocratisation de technologies existantes. Les réseaux sociaux existaient avant l'émergence du terme de Web 2.0 ; la révolution à la source de leur émergence a été la volonté simplificatrice : désormais, chacun peut créer en quelques clics un blog Wordpress, une page Facebook ou un compte Twitter.

Démocratisation d'un élitisme, le Web 2.0 donne la possibilité à chaque individu de devenir simplement un média indépendant.

Facebook et Twitter, des outils de cyberdissidence ? Voilà qui ne manque pas de sel, et démontre la force de la mentalité hacking de ces populations en révolte. Mais lorsque les révolutions arabes ont utilisé la simplicité de ces technologies pour contester les régimes en place, elles ont relégué dans l'ombre nombre de technologies beaucoup plus axées sur la cyberdissidence.

C'est tout le paradoxe de ces évènements géopolitiques : les réseaux sociaux ont eu un impact certain sur le succès des révolutions arabes ; mais la médiatisation de cette utilisation novatrice, du fait des puissances informationnelles occidentales, a conduit à l'oubli des échecs passés (Birmanie, mobilisations biélorusses en 2006, révolution verte iranienne en 2009). Enivrés par les succès arabes, les médias pouvaient croire que rien n'arrêterait jamais plus l'expression populaire, dont les capacités à se faire entendre en dépit de la censure semblaient d'autant plus absolues qu'elles étaient accessibles à tous. Plus dure fut la chute. ■■■

Force est donc de constater que le rôle de la cyberdissidence dans les révolutions arabes, s'il ne doit pas être minoré, a été idéalisé par les médias des pays qui avaient intérêt à ce qu'elles réussissent. D'où la création ex nihilo d'un peuple cyberdissident, rompu à Facebook, aux blogs et affamé de démocratie. Tout cela en dit bien plus sur le monde médiatique occidental que sur la cyberdissidence des populations du Sud.

Pouvoir(s) contre médias : conflit asymétrique occidentalo-occidental

En mai 2011, lors de la Journée mondiale de la liberté de la presse organisée par l'Unesco, j'avais tenté d'expliciter la nécessaire complémentarité qui devait lier le Sud et le Nord quant à l'avenir de la liberté d'expression, et tous les enseignements que l'on pouvait tirer des expériences tunisiennes et égyptiennes. Parmi les premiers, Jean-Marc Manach, journaliste à Owni, soulignait la nécessaire convergence qui devait s'opérer entre le métier de journaliste et la mentalité des hackers, et dénonçait implicitement le déficit de connaissance en sécurité de l'information de la grande majorité de ses collègues. Plus récemment, le spécialiste en cyberdéfense, Félix Aimé, tentait de montrer qu'un phénomène similaire médiatisait à outrance le mouvement Anonymous. D'une manière générale, et exception faite de sites à l'interface des différents domaines (Owni, Reflets.info, Intelligence-Strategique.eu), jamais un journaliste (généraliste) français n'est moins à l'aise que quand il doit traiter de VPN, chiffrement asymétrique ou même d'adresses IP.

Cette incompétence à traiter des problématiques cyber ne serait pas en soi dérangeante si elle n'impactait pas directement la sécurité même des journalistes.

Ainsi, au Sud, passée l'euphorie du succès, les temps sont aux constructions politiques post-mobilisations. D'abord idéalisés et admirés par le Nord (non sans une pointe de condescendance), les régimes de transition qui ont succédé aux autoritaires inquiètent. Quelles voies/voix vont-ils choisir ? Beaucoup déplorent ce qu'ils considèrent comme des dérives anti-démocratiques ce qui est d'abord la recherche d'un système politique adapté à des cultures fondamentalement différentes des européennes. Ils en oublient par là que les démocraties occidentales se sont construites identiquement, hybrides d'histoires, de cultures et de traditions. Il ne faut toutefois pas occulter que, si la cyberdissidence a joué les premiers rôles dans ces mobilisations d'un (relatif) nouveau genre, elle est aussi apparue en pleine lumière. Elle sera désormais attendue, et donc mieux contrôlée. Nombreux sont les Etats à avoir compris, souvent même avant les évènements géopolitiques de 2011, le rôle stratégique du contrôle du cyberespace.

En Iran, par exemple, le succès médiatique de la révolution verte, ayant démontré la potentielle puissance de réseaux sociaux comme Twitter, a convaincu le gouvernement de se lancer dans le développement d'un Internet local, coupé du réseau des réseaux ; une sorte d'intranet national, en somme. Si la réalisation de ce projet est sujette à caution, il faut noter que l'Iran n'est pas un cas isolé. Nombre d'autres (Birmanie, Chine, Cuba) explorent le même genre de pistes, l'Internet mondial étant vu comme un vecteur de démocratisation sous contrôle américain.

Au Nord, la multiplication des affaires d'écoutes, de corruption et d'espionnage (notamment des médias) est le signe d'un fossé technologique grandissant entre le pouvoir institutionnel et le monde médiatique. L'extraordinaire travail de l'équipe d'Owni, par sa volonté de sensibilisation aux thématiques numériques en général, et dans l'affaire Amesys en particulier, est un peu l'arbre qui cache la forêt. Pipa, Sopa, Acta, ou encore, récemment, l'invraisemblable proposition de Nicolas Sarkozy visant à la création d'un délit de consultation de sites Internet ; autant de projets populistes, réactionnaires et liberticides. Plus inquiétante encore est cette initiative britan-

■■■ -nique souhaitant charger le Government Communications Headquarters (GCH) de la surveillance généralisée et en temps réel de toutes les communications de l'ensemble des citoyens (appels téléphoniques, emails, SMS), au nom du sacro-saint prétexte de la lutte contre le terrorisme.

Il s'agit d'un arsenal institutionnel répressif en plein développement contre les journalistes dépassés par la précarisation galopante de leur métier : tel est le conflit asymétrique qui caractérise aujourd'hui nos sociétés tant vantées aux pays du Sud. Il faut cependant se retenir de tomber dans la simplification à outrance, mettant en scène un Sud libéré et un Nord autoritaire.

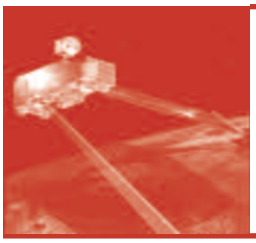
Un voyage chaotique vers de nouvelles sociétés de l'information ?

Industrie du Numérique, Web 2.0, Nouvelle économie, secteurs TIC ; autant de manières d'utiliser la sémantique pour ne pas traiter le problème sous-jacent : l'évolution des représentations. Qu'il soit question d'économie, avec la guerre interminable des brevets qui oppose Apple/Samsung/Google/Microsoft, ou celle que livrent les majors américains à tout ce qui ressemble de près ou de loin à du téléchargement ; de l'identité sur Internet, et des visions hégémoniques qui rassemblent Google et Facebook ; de politique, avec l'émergence de nouveaux mouvements, tel que le Parti Pirate ;que les orthodoxies périclitent, que les représentations évoluent et que les frontières s'effacent.

Même le système d'abonnement, modèle économique à la base de l'accès à l'Internet, est susceptible d'être remis en question. D'ailleurs, ce futur conflit viendra sans doute des technologies destinées aux cyberdissidents. En effet, les initiatives telles que le Hackerspace Global Grid (HGG) et surtout Commotion Wireless, si elles souhaitent permettre à tout un chacun d'échanger de façon sécurisée des informations ou des fichiers, pourraient également, à terme, conduire à la création des Internet-bis, où chaque utilisateur sera anonyme et ne pourra voir son comportement tracé, étudié ou espionné. Ainsi, le réseau Commotion utilise tout appareil équipé d'un chipset Wifi, créant autant de nœuds capables de communiquer les uns avec les autres, au sein d'un réseau pair-à-pair décentralisé. Suffisamment de nœuds ajoutés à un maillage important (au moins localement), donnera un réseau parallèle à l'Internet, mais basé sur l'anonymat et la sécurité des communications propres au système Commotion. Plus ambitieux, le Hackerspace Global Grid du Chaos Computer Club (CCC) souhaite utiliser des satellites en basse orbite pour permettre à de petites stations terrestres autonomes d'échanger des informations. Ces deux projets, non encore accessibles, ne pourront vraisemblablement pas concurrencer l'Internet actuel. Comme beaucoup d'autres technologies, leur efficacité viendra(it), au moins partiellement, du nombre d'utilisateurs. Mais elles auront le mérite d'offrir une alternative sécurisée aux moyens de communication électroniques actuels. Et rien n'empêchera les adeptes de jongler entre les différents réseaux, suivant leurs besoins d'anonymat et/ou de sécurité.

Ainsi donc les vieux modèles socio-économiques, concurrencés de toute part et parfois même victimes de leurs propres succès, se refusent à mourir et à laisser la place. De ce combat entre nouvelles et anciennes représentations peuvent sortir des sociétés de l'information, libres et plurielles… comme une résurgence des doctrines liberticides et sécuritaires. ■

*
* * *
*



Préserver l'anonymat par une identité numérique de confiance

par Bertrand Boyer,
Officier spécialiste sécurité des systèmes d'information

Une des caractéristiques souvent évoquée du cyberespace, et en particulier de l'Internet, est l'anonymat (réel ou supposé) qu'il procurerait à ceux qui s'en donneraient les moyens. Esquive numérique à une censure d'État, l'anonymat incarne également le principal obstacle à la mise en place de réponses juridiques réellement efficaces dans le cadre de la lutte contre la cybercriminalité. Il induit, de facto, la quasi impossibilité d'attribuer, dans des délais raisonnables, l'origine d'une action à un individu, un groupe organisé ou un État. Or, sans attribution sûre, il ne peut être question de légitime défense, ni de réponse adaptée et proportionnée.

Principal obstacle à la mise en œuvre des politiques de sécurité, l'anonymat est donc indistinctement l'atout premier de tout attaquant mais également le dernier rempart de protection pour de nombreux opposants à des régimes répressifs. La traçabilité des actions dans le cyberespace pose ainsi de nombreux problèmes à la fois techniques, éthiques et juridiques qui semblent pour l'heure indépassables. Une étude attentive des usages du cyberespace amène pourtant à considérer que l'anonymat est de plus en plus fragilisé par l'introduction de nouveaux terminaux et les pratiques qui en découlent. En effet, ce qui caractérise le milieu que nous considérons, c'est avant tout son évolutivité, son adaptabilité, sa capacité à muter, muer rapidement, rien n'est donc définitivement acquis.

Localiser, authentifier... oui ! Mais pour en faire quoi ?

L'arrivée massive de terminaux portables a, dans ce contexte, des conséquences majeures sur la gestion de la mobilité des utilisateurs du cyberespace. Plus que jamais, la localisation et l'authentification des usagers sont au centre des évolutions techniques et commerciales.

L'explosion de la consommation de bande passante engendrée par les smartphones impose de constantes modifications aux réseaux et pousse la mise en œuvre de solutions s'appuyant exclusivement sur la suite protocolaire IP. Les opérateurs collectent les données d'identification et de localisation, mettent en place des dispositifs pour limiter la consommation de certains services afin de garantir la qualité d'autres (priorité au trafic voix sur le trafic des données, par exemple). De tels dispositifs de limitation s'accompagnent déjà de solutions de filtrage et d'inspection en profondeur des paquets (DPI) de données échangées. Ainsi, la pratique des utilisateurs, qui réclament toujours plus de connectivité et un accès immédiat où qu'ils soient, entraine une traçabilité accrue et fragilise de plus en plus la notion d'anonymat. Face à la demande, la mise en œuvre par des acteurs non étatiques de solutions techniques toujours plus intrusives s'impose naturellement.

Progressivement et de façon quasi transparente pour les usagers, des données personnelles se trouvent manipulées, stockées, traitées par des tiers dont on ignore pratiquement tout. Dans ce domaine, les publications des chartes sur le respect de la vie privée, que bien peu lisent, relèvent souvent du pur exercice de style et la loi du plus fort s'applique en s'appuyant sur des situations de quasi monopole. ■■■

De la confiance dans les identités numériques

Comment alors sortir du paradoxe qui veut, qu'au motif de préserver la liberté, l'on s'oppose farouchement à toute intervention publique alors même que l'on subit les contraintes d'opérateurs privés dans le cadre d'une relation contractuelle ? Aujourd'hui un système d'identification fiable a été mis en place pour réguler la circulation maritime et aerienne, est-il improbable que de tels mécanismes voient le jour dans le cyberespace ? Un système d'identification de confiance n'est pas nécessairement synonyme d'atteinte aux libertés fondamentales, la régulation n'est pas systématiquement associé à la répression.

Si la question de la confiance dans les identités numériques s'avère fondamentale pour garantir les échanges et les relations entre individus connectés, la fiabilisation de celle-ci ne peut-être de l'unique ressort d'entités commerciales.

La mise sur pied d'un traité visant à réguler les pratiques et à faciliter l'identification des acteurs tout en garantissant leurs droits est, d'une part souhaitable, d'autre part extrêmement probable à moyen terme. Une telle réglementation redonnerait aux États la place de régulateur qu'ils doivent enfin assumer et garantirait un niveau de confiance suffisant entre usagers.

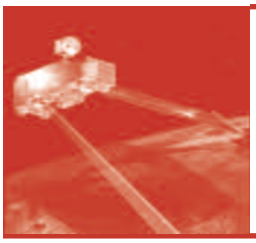
Au mois de septembre 2011, le démantèlement du botnet Kelihos s'est accompagné pour la première fois d'une plainte contre des personnes physiques. Microsoft a ainsi pu remonter jusqu'aux responsables qui se cachaient derrière ce réseau par l'intermédiaire des détenteurs de noms de sous-domaines.

Réglementer pour garantir les libertés individuelles

Ce mouvement vise donc à réduire les possibilités pour un utilisateur du réseau de dissimuler son identité et de se soustraire à sa responsabilité. Si des acteurs de poids tel que Microsoft et le département d'État américain se mettent en quête d'un système plus « transparent », il semble probable que des résultats soient observables dans de brefs délais. Cet exemple illustre la fragile réalité de la notion d'anonymat pour les acteurs du cyberespace. De puissants mouvements s'opposent et favorisent le développement de moyens de contournement toujours plus sophistiqués. Pourtant, ici encore, les pratiques des usagers peuvent se révéler paradoxalement contre-productives car pour préserver leur liberté et leur « droit à l'anonymat », les utilisateurs vont parfois avoir recours à des moyens qui, certes préservent leur identité, mais laissent des traces numériques tout à fait singulières. Ainsi, l'usage d'un VPN ou le chiffrement de messages, sont autant de pratiques qui « se voient » et peuvent singulariser leurs utilisateurs pour en faire alors les cibles privilégiées d'une surveillance et d'une répression qui n'ont parfois plus rien de numérique…

La mise en place d'une identité numérique fiable, permettra de sortir de l'impasse actuelle où, pour préserver ses données privées, l'utilisateurs « honnête » utilise les même procédés que les criminels. Dans le monde réel, la mise en place de « pièces d'identité » n'empêche certes pas les délinquants de se procurer des faux, mais présente l'intérêt de limiter justement ces pratiques aux dits fraudeurs. Par ailleurs, disposer d'une pièce d'identité n'est pas synonyme d'abandon d'anonymat au quotidien. La pièce d'identité n'est à présenter que lorsque qu'elle est demandée, un tel mécanisme peut tout à fait être mis en place dans le cyberespace. Ce mouvement doit être accompagné et porté par les citoyens et la représentation nationale. Dès lors, il n'est peut-être pas utopiste de penser que l'anonymat, la libre consultation de sites et l'inviolabilité de la correspondance puisse être garantis par une identité numérique fiable.

*
* * *
*



OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

PirateBox : mode d'emploi, quelles applications et quelles limites ?

Entretien avec Philippe Blanc,
Directeur technique informatique et hacktiviste
Propos recueillis par Pierre-Yves Castagnac

IRIS : La « PirateBox » débarque en France… mais qu'est-ce que c'est ?

Philippe Blanc : Il s'agit, comme son nom l'indique, d'une « boite ». Elle est de petite taille. Elle peut tenir dans le creux d'une main. Elle contient un routeur Wireless, un serveur Linux, une clef USB… et naturellement une batterie. Ce « package » permet de créer réseau wifi portable personnel à courte portée. Objectif : partager des informations à distance sans utiliser le réseau internet officiel. Je tiens d'ailleurs à souligner que le terme de « PirateBox » est abusif car il sous-entend que l'utilisateur se positionne forcement comme un « pirate ». Il serait plus judicieux de parler de « WifiBox » ou selon les endroits et usages d'utilisation, de « bibliothèque-box », de « bar-box », etc. En effet, la technologie n'est ni bonne, ni mauvaise… Il ne s'agit que d'un moyen à la disposition d'un utilisateur. Tout dépend de ce que ce dernier en fait.

IRIS : Comment est né ce concept de réseau wifi indépendant ?

Philippe Blanc : Tout a commencé avec le phénomène des « deaddrops » des romans d'espionnage. Les espions cachaient des petits mots dans le creux d'un mur ou sous la table d'un restaurant… pour qu'un contact le récupère plus tard. Ce concept d'échange à distance a évolué par la suite vers des « deaddrops USB ». Plutôt qu'un morceau de papier, on cimentait une clef USB dans un mur. Seule la tête était visible pour pouvoir se connecter. N'importe qui, averti de l'emplacement, pouvait le faire. Il existe en France une centaine de mur avec une clef USB qui dépasse. De là est né l'idée d'un échange par wifi : la PirateBox ! Il s'agit d'un espace ouvert qui est partagé entre différents utilisateurs. Ces utilisateurs connaissent le lieu mais aussi le nom du réseau wifi. Ils savent donc où se connecter. Sauf que là, à la différence des deaddrops, la PirateBox offre plus de place et garantie un anonyme total.

IRIS : Quels sont les applications pratiques de la PirateBox ?

Philippe blanc : Les applications sont multiples. Elle offre les mêmes avantages qu'un réseau wifi classique. Elle permet un échange de données à distance. Nous pouvons évoquer le cas d'un enseignant qui souhaite partager ses cours avec ses élèves. Chacun amène sa box et copie ce qu'il y a sur celle du voisin. Autre usage : le train. Il n'y a généralement pas de wifi… ce qui peut être gênant. La PirateBox offre à différents voyageurs le moyen d'échanger des fichiers à distance dans un même wagon. Idem, lors des concerts ou des festivals. La PirateBox permet le partage des photos de l'événement. Cependant l'application la plus intéressante réside dans le « mesh ». Une PirateBox isolée n'a qu'un intérêt limité. L'idée est que chaque box puisse se connecter aux autres box situées à portée. Avec le mesh, si le nombre de PirateBox est important, on peut dès lors parler d'un réseau parallèle. Il est non seulement dynamique et décentralisé… mais totalement hors de contrôle ! La mise en « mesh » des PirateBox est un projet en cours de développement. ■■■

IRIS : Peut-on imaginer des applications plus tactiques ?

Philippe Blanc : Oui, tout à fait ! Au-delà, une piratebox peut avoir un rôle à jouer en zone de trouble. Prenons l'exemple d'une manifestation hostile à un gouvernement comme en Tunisie ou en Egypte en 2011. Le réseau Internet officiel avait été coupé. Plus d'échange d'information possible. Avec une PirateBox au contraire, il ne suffit que d'une personne avec sa box pour que les gens autour puissent échanger des informations. La PirateBox permet de créer, si non de recréer, un réseau wifi local. La zone couverte est certes faible… mais elle est suffisante pour couvrir une rue ou une intersection. Ce wifi permet ainsi d'échanger des informations stratégiques à courte distance : où se trouve le prochain barrage ? Où se trouve la police ? Quelle est l'heure du prochain rendez-vous ? Etc. Nous parlons ici que de troubles urbains, mais la PirateBox pourrait avoir les mêmes applications en zone de guerre.

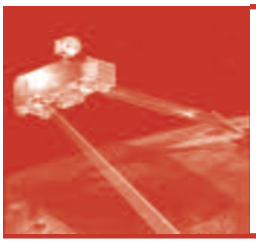
IRIS : Combien coûte une PirateBox ? Et surtout qui peut en fabriquer une ?

Philippe Blanc : Une PirateBox ne coûte pas cher. Il faut compter environ trente-cinq euros. Pour la construire, il est nécessaire d'avoir quelques notions d'informatique et un peu de matériel, mais pas besoin d'être un geek. Vous trouvez toutes les informations nécessaires sur la Toile.

IRIS : Quelles sont les limites de ce système ?

Philippe Blanc : Elles sont tout d'abord géographiques. La portée émettrice d'une PirateBox est limitée. Même si on augmente la puissance, elle reste très locale : une rue, un quartier mais pas plus. Autre point, ce type de réseau est un wifi… avec ses avantages et ses inconvénients. N'importe qui peut capter le signal. On peut le protéger avec un mot de passe et du cryptage, mais cela en limite alors l'utilisation à un réseau d'initiés. A l'inverse, les forces de l'ordre ont également des moyens pour répondre à ce wifi parallèle. Elles peuvent le brouiller ou bien le saturer en créant des dizaines de réseaux wifi similaires et portants le même nom. L'utilisateur ne saura plus sur lequel se brancher. Cette technique peut être efficace, surtout en zone de trouble. Le manifestant risque de perdre un temps précieux pour retrouver le « bon réseau » wifi.

*
* * *
*



Le dilemme chinois du dictateur

par Charles Bwele,
Consultant en technologies de l'information
Auteur du blog Electrosphere

L'Internet chinois est un univers en expansion fulgurante qui bouleverse maintes certitudes et donne des sueurs froides au Parti communiste. En 2012, la langue anglaise occupe la pôle position sur l'Internet avec ses 550 millions d'internautes. Depuis 2008, la Chine s'enrichit chaque année d'une quarantaine de millions d'internautes et en compte déjà plus de 430 millions dont 280 millions de mobinautes. On peut parier sans trop de risques que l'Internet sinophone – souvent appelé « Chinternet » – surpassera l'Internet anglophone à l'horizon 2015.

Le Chinternet mêle diverses caractéristiques qui mettent à mal une approche classique ou linéaire de la liberté d'expression et de la société de la connaissance. Dans ce monde à part, censure et critique semblent presque faire bon ménage.

L'information ouverte et ses ennemis

La Grande Muraille de l'Internet chinois – ou le Great Firewall – est un système sophistiqué de surveillance en ligne combinant procédés techniques et moyens humains. Une énorme liste de sites Internet et d'adresses IP désignés comme « subversifs » (portails et webzines internationaux d'actualités, organisations de défense des droits de l'Homme, blogs de dissidents chinois à l'étranger, sites ayant trait à la cause tibétaine, à la secte Falun Gong, aux événements de Tian'Anmen, aux révoltes arabes, etc) par les autorités chinoises sont inaccessibles depuis la Chine intérieure.

Les pages Web et les messages échangés dans les forums et dans le chat sont également soumis à un filtrage sémantique et affichent parfois des phrases incomplètes. Grâce à une astucieuse reconfiguration des registres DNS, l'internaute chinois qui compose une adresse Web subversive dans son navigateur est aussitôt redirigé vers une adresse plus correcte. Des médias sociaux comme Facebook, Twitter, Youtube et Flickr sont également bannis par les fournisseurs d'accès Internet chinois. Pour couronner le tout, les autorités chinoises délèguent ou externalisent l'essentiel du filtrage aux fournisseurs de contenus grâce à un savant dosage d'incitations et de sanctions. Chaque année, des prix de l'auto-discipline sont décernés aux FAI qui « protègent la Chine des vices et des subversions du réseau mondial » et aux hébergeurs de sites Internet qui « veillent à un développement sain et harmonieux de l'Internet ». Les sociétés jugées contrevenantes ou laxistes se voient retirer leurs licences d'exploitation. Parallèlement, la censure exercée sur le Chinternet et l'inhérente réglementation kafkaïenne dissimulent un protectionnisme « e-conomique » ayant pour but d'offrir de formidables opportunités d'expansion et de positionnement sur le marché national aux firmes technologiques chinoises. Celles-ci seront alors mieux préparées à affronter leurs concurrentes américaines d'envergure planétaire.

La Cité presque interdite

Une frange de « chinternautes » utilisent des applications comme TOR, Privoxy, Ultrareach et Dynaweb afin de contourner la censure via des proxys étrangers régulièrement mis à jour. Toutefois, l'immense majorité des Chinois ne lisent ou ne parlent guère l'anglais ■■■

■■■ et se contentent largement des prolifiques médias numériques en mandarin ou en langues locales.

Youku, Douban, Weibo et Baidu sont de très populaires versions chinoises de Youtube, de Facebook, de Twitter et de Google. Les pages Web de l'infomédiaire QQ – homologue chinois de MSN ou de Yahoo! – fourmillent d'actualités et de débats portant sur des enjeux locaux. Les médias sociaux « made in China » prolifèrent d'autant plus librement qu'ils s'autocensurent au gré des actualités locales ou internationales et des humeurs de l'administration. Les thèmes prohibés ne sont jamais clairement définis et le champ de la censure varie d'une semaine à l'autre.

Après un tragique tremblement de terre qui provoqua la mort de plus de 5000 enfants dans une école de la province du Sichuan à l'été 2008, tout forum critiquant l'intervention des services publics ou tout blog dénonçant certaines normes de construction subissait les foudres de la censure. Quelques mois plus tard, les discussions enflammées sur ces mêmes thèmes reprirent de plus belle...

Au printemps 2012, les autorités chinoises durcirent provisoirement la censure des plateformes de microblogging (dont Weibo qui compte plus de 300 millions d'abonnés) traversées par des rumeurs de révolution de palais ou de coup d'État militaire peu après le limogeage de Bo Xilai, figure charismatique du Parti communiste. Consécutivement, les adeptes du microblogging furent tenus de fournir leurs pièces d'identité, leurs numéros de téléphone mobile et de ne point bloguer avec des noms d'emprunt. Cette disposition lourde, onéreuse et donc difficilement applicable à l'échelle de plusieurs centaines de millions d'internautes relevait surtout de l'intimidation voire d'une incitation ferme à l'autocensure.

Tigres et dragonautes

Dans un pays comptant près d'un demi-milliard d'internautes et où ont lieu chaque année des dizaines de milliers de grèves, d'émeutes et de manifestations violentes ou pacifiques, les médias sociaux prennent nécessairement une tournure volcanique et donnent des sueurs froides au Parti communiste, soit à l'État chinois.

Les ma boke, fameux « blogs de la colère », se chiffrent par dizaines de millions, jouent au chat et à la souris avec les autorités et font feu de tout bois : inflation, crise du logement, pollution, chômage, insécurité, corruption, répression, etc. Ceux interdits sont aussitôt recrées sous d'autres noms, entrainant avec eux leurs furieux essaims de commentateurs pour lesquels la censure vaut littéralement consécration.

Les problèmes intérieurs de la Chine étant à la mesure de sa success story, le Parti communiste se sait étroitement surveillé ou contesté par des médias sociaux dévoilant ses moindres dérives et menaçant perpétuellement de lui « faire perdre la face ».

D'un côté, il étouffe la moindre veilleité de contestation sur la scène intérieure et sur l'Internet; de l'autre, il ne feint plus d'ignorer un magma social en constante fusion. Poussé à l'action, il légifère contre la spéculation immobilière dans les grandes villes, tente de limiter la pollution de certaines rivières, circonscrit tant bien que mal des foyers d'épidémie, s'emploie à réprimer l'exubérante corruption dans les administrations territoriales, subventionne quelques denrées de première nécessité, relaxent des « éléments indisciplinés » appréhendés quelques jours plus tôt...

Pas à pas, l'administration a vite appris à flairer les opinions et à devancer autant que possible les éruptions populaires via les médias sociaux. Elle préfère donc exercer un filtrage malicieux du Chinternet plutôt qu'une implacable et sisyphienne censure. Ainsi, les autorités chinoises ont un oeil averti sur les foules connectées et identifient les esprits les plus retors... qui seront invités à « prendre un thé » au commissariat le plus proche ou recevront la visite d'un inspecteur de police. ■■■

En Chine, ces pratiques connues de tous visent en premier lieu à faire comprendre aux éléments indisciplinés qu'ils sont étroitement surveillés et qu'ils seront arrêtés en cas de récidive.

À pas de chinois !

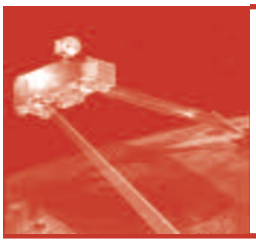
Au milieu des années 1980, George Schultz, économiste et secrétaire d'État de l'administration Reagan, forgea un concept appelé « le dilemme du dictateur » : soit les régimes totalitaires s'ouvrent complètement aux technologies de l'information, sont poussés à des réformes ou à l'effondrement et leurs nations en tirent d'énormes bienfaits sur les plans sociaux, économiques et scientifiques; soit ils se ferment totalement à ces technologies, s'isolent du reste du monde et enfoncent leurs nations dans une stagnation ou dans une régression tous azimuts.

Mikhail Gorbatchev, secrétaire général du Parti communiste soviétique, fut inspiré par ce concept et constata vite que son vaste pays ne pouvait bénéficier des retombées de l'ère informationnelle avec ce régime hermétique et répressif qu'était l'URSS. Par la suite, la glasnost et la perestroïka précipitèrent l'implosion de l'empire soviétique et menèrent à l'effondrement du bloc communiste en Europe centrale et orientale dans les années 1990. Les « régimes durs » et les économies exsangues de Cuba, de la Corée du Nord, de l'Iran et du Zimbabwé illustrent parfaitement ce dilemme du dictateur. Avec un Parti communiste au pouvoir et son économie en pleine expansion – aujourd'hui en deuxième position derrière celle américaine, la Chine fait figure d'étrange exception et, une fois de plus, révèle un paradoxe dont elle a le secret.

Fort d'un plan d'investissement de 120 milliards d'euros par an dans les technologies de l'information, de sa propre architecture DNS et de noms de domaines en caractères chinois, l'Empire du Milieu se dote d'un réseau quasi autonome et distinct de l'Internet mondial. En outre, il exporte ses produits et services technologiques dans le monde entier et sera bientôt la nation la plus connectée.

Par ailleurs, la liberté d'expression n'a certes pas cours légal dans la République populaire mais la parole se libère un peu plus chaque jour et l'innovation scientifique se développe à grande vitesse grâce notamment à l'Internet. Aux yeux et aux oreilles des chinternautes, l'idée de censure n'implique point une critique moribonde ou une créativité au rabais. En effet, les foules connectées s'adaptent rapidement à des règles du jeu aussi changeantes qu'imprécises et les élites économiques et scientifiques, très au fait des techniques anti-censure et des réseaux virtuels privés, ne semblent guère pénalisées dans la conduite des affaires et dans la course à l'innovation. D'une certaine façon, la stratégie chinoise de filtrage de l'Internet consister à « barrer la route aux troupeaux de buffles mais à laisser s'échapper quelques hordes de rats en surveillant ou en orientant leur fuite ». La population chinoise, plutôt fière de sa spectaculaire émergence économique et assez optimiste sur son avenir à moyen ou long terme, serait-elle encline à passer l'éponge sur la politique de censure du Parti Communiste ? Serait-elle persuadée que les jours de cette administration soient comptées et qu'une véritable liberté d'expression s'instaure d'une façon ou d'une autre en Chine ?

Jusqu'ici, le Parti communiste a réussi à embrasser le capitalisme en conservant son ossature socialiste. Aurait-il trouvé la formule magique permettant de sortir le génie de l'Internet en laissant le diable enfermé dans la bouteille ? Survivra-t-il à cette économie de l'information qui émerge sous ses pieds ? La République populaire forgera-t-elle une audacieuse société de la connaissance en muselant l'esprit critique et ouvert supposé fonder celle-ci ? Jusqu'où et quand ira l'État chinois dans sa course-poursuite contre... ou aux côtés de son peuple ? L'histoire nous dira comment la Chine a résolu ou subi son dilemme du dictateur. Mais une chose est sûre : l'envol d'un dragon n'a rien du cours tranquille du Mékong.



OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

La logique de l'épée et du bouclier dans l'univers du cyberespace

par Yannick Harrel,
Spécialiste et chargé de cours en stratégie des pouvoirs et enjeux du cyberespace

Les révolutions 2.0 comme on les a appelé un peu trop hâtivement, ont eu néanmoins le mérite de mettre à l'honneur les réseaux sociaux et leur impact sur les populations comme sur le cours des évènements.

Internet comme courroie des révolutions modernes

Le réseau des réseaux, difficilement lisible dans sa globalité pour une raison fort simple qui est sa perpétuelle évolution, a initié dans son sillage une grappe d'innovations qui ont transformé les communications et même remis en cause les détenteurs de l'information traditionnels.

Les bouleversements géopolitiques récents ont acté une volonté de changement au sein des régimes allant du Maghreb au Machrek, jusqu'aux confins Perses. Ils ne doivent rien au déclenchement de ceux-ci, mais ils n'en ont pas moins amplifié le phénomène. Du reste, l'emploi des outils numériques n'a pas été uniquement un amplificateur interne mais aussi un relais communicationnel vers l'extérieur permettant aux étrangers de suivre les soubresauts parfois en quasi-direct. Ce n'est pas sans raison que les autorités affolées d'Egypte et de Tunisie interrompirent Internet et que, les responsables Iraniens procédèrent en février 2012 à une surveillance accrue du réseau des réseaux en interdisant les protocoles sécurisés.

Pourtant ces tentatives de brider ou bloquer totalement les moyens de communication ne se révèlent pas toujours payantes au prorata des efforts gouvernementaux consentis.

La raison en est simple : l'épée a deux avantages, la mobilité et l'initiative. Le bouclier devient toujours plus résistant mais se meut de plus en plus lentement et se place volens nolens dans une position attentiste. Pis, lorsque le bouclier se pique d'être offensif, il n'emploie qu'une tactique et des moyens souvent inadaptés. Ainsi, lors de la grande coupure d'Internet en Egypte durant la révolution de février 2011, Twitter proposa de passer outre et de continuer à « gazouiller » grâce à l'emploi de la téléphonie retranscrivant le message en un tweet avec le hashtag du pays concerné : le speak-to-tweet était né !

Autre exemple, alors que le gouvernement Chinois admonesta Google en l'enjoignant à se conformer au filtrage en vigueur, la firme de Redmond fulmina quant à ces propositions d'autocensure, boucla son site national dont la page redirigea vers... la version Hong-Kongaise non-censurée. De même, certains réseaux de pair à pair (peer to peer) tel Pirate Bay craignant une vulnérabilité et visibilité trop accentuées, optèrent pour le protocole SSL concernant l'échange des fichiers, compliquant de fait les tentatives d'espionnage des paquets d'informations transitant par les utilisateurs du service.

C'est aussi de cette manière que les sociétés ou individus proposant des services centralisés mutèrent pour aboutir à une forme décentralisée et cryptée des tâches.

Peut-être l'évolution naturelle aurait abouti à la même conclusion, toutefois un événement tiers, généralement menaçant envers une

position, une situation ou un groupe, accélère ou même initie souvent une transformation de l'existant vers une solution adaptée à la nouvelle donne. Ce qui est d'ailleurs paradoxal est que lorsque le bouclier tente de faire cesser un dommage, il robore l'épée qui va s'aiguiser davantage et tenter de trouver une autre faille.

Nul ne peut comprendre cet état de fait s'il n'intègre pas la vision du cyberespace comme un organisme vivant, croissant et mutant en répondant aux attaques qu'il subit. De même que la couche publique n'est que la couche supérieure visible, et que de nombreuses couches demeurent cachées de la vue des utilisateurs lambda du cyberespace. Que l'on songe par exemple aux Darknets.

Les forces qui se font face au sein du cyberespace ne sont pas obligatoirement, et même rarement, de même calibre. Il s'agit souvent d'un rapport de force asymétrique. Il s'ensuit que la problématique est différente pour chaque partie concernée : préservation d'un système et conservation de l'acquis pour le bouclier, fût-ce en y mettant des moyens financiers et humains ; maximisation des atteintes portées à moindre coût en alliant furtivité, inventivité et rapidité pour l'épée.

« Rien n'arrête une idée dont le temps est venu »

C'est par cet axiome que Victor Hugo entendait affirmer que toutes les barrières qui sont érigées pour défendre un régime deviennent caduques ou en passe d'être submergées à partir du moment où le mouvement est par trop puissant et en corollaire irrésistible.

Au final, l'épée est plus mobile. Elle a toujours l'initiative et est animée par une idée conquérante. Elle aura toujours le dessus sur le bouclier, dont l'accumulation de protections le rend plus lourd et forcément moins mobile ainsi que dans l'expectative des prochaines attaques. Bien entendu, un système n'est pas obligé d'être dans une position conflictuelle selon les circonstances : acceptant et s'adaptant à une nouvelle donne, il désamorcera souvent de lui-même une conjecture explosive.

Question : Les réseaux numériques ont-ils réellement les moyens de faire et défaire les gouvernements ?

Charles Bwele : Ce ne sont pas les réseaux numériques à eux seuls qui font ou défont les régimes politiques mais une combinaison de facteurs relevant à fois du politique, du social ou de l'économique, et qui sont probablement amplifiés par quelques effets « boule de neige » inhérent à des foules de plus en plus connectées et informées. L'Internet, la téléphonie mobile et a fortiori l'Internet mobile semblent susciter des hypermimétismes qui se propagent à une vitesse surprenante pour des organisations étatiques souvent enfermées dans leurs habitudes et très peu enclines à des changements rapides et brutaux. Les régimes de Ben Ali en Tunisie et de Moubarak en Egypte ont illustré à merveille cette réalité.

Yannick Harrel : Je m'en tiendrai à ce que j'avais évoqué au moment des Révolutions arabes « 2.0 » : Internet et sa grappe d'innovations est une courroie et non un moteur ! Les outils ne se meuvent aucunement d'eux-mêmes, et une révolution commence déjà par des revendications : les réseaux sociaux ont accentué et amplifié la diffusion de celles-ci mais n'en sont aucunement à l'origine. Il se peut ensuite que certaines stars d'Internet aient une position maîtresse une fois les évènements calmés, comme Slim Amamou en Tunisie, mais les TIC ne sont qu'un vecteur et non un déclencheur. Ce qui ne diminue en rien leur capacité d'action sur le corps social et leur impact sur certains évènements.

IRIS : Les gouvernements non-démocratiques peuvent-ils efficacement contrôler les ré-seaux numériques ? Les

gouvernements démocratiques ne seraient-ils pas tentés par ce même contrôle ?

Charles Bwele : Les réseaux numériques relèvent de structures décentralisées et horizontales et sont rapidement devenus des couches complexes et dynamiques en rhizomes imbriquant étroitement individus, sociétés et économies de par le monde. Nous sommes loin des modèles statiques et centralisés en étoiles d'autrefois. Pour un gouvernement démocratique reposant sur la liberté d'expression et sur une société de l'information ouverte, un contrôle plus ou moins serré se paierait cher sur les plans économiques, scientifiques, culturels, sociaux et donc politiques. Pour un régime dur mené par une élite dirigeante d'abord et surtout soucieuse de sa survie politique et parfois physique, cette question peut sembler moins épineuse. Cependant, les gouvernements de la Chine, de l'Iran et de maintes pétromonarchies arabes sont confrontés à un dilemme du dictateur de plus en plus cornélien depuis qu'ils ont massivement adopté l'Internet et la téléphonie mobile.

Yannick Harrel : Les réseaux numériques sont une problématique nouvelle et sérieuse pour bien des États, et pas uniquement autoritaires ou limite totalitaires. Auparavant le pouvoir central contrôlait les divers moyens de communication : presse écrite, radio, télévision. D'autant plus facilité que ces médias étaient unilatéraux : du producteur au lecteur/auditeur/spectateur. Dorénavant il y a multilatéralité et aussi relativité incidente concernant la croyance dans les médias traditionnels. Contrôler chaque Internaute est illusoire alors les États doivent trouver des solutions annexes plus en amont comme le filtrage et/ou la surveillance à grande échelle et ce avec la coopération des fournisseurs d'accès à Internet. Ont même été envisagés des réseaux nationaux se substituant à Internet (couche 3 du modèle OSI), réalisables techniquement mais butant sur la volonté des résidents d'être connectés avec l'extérieur, et ce par tous moyens. Les États démocratiques ont aussi initié des mesures de contrôle d'Internet : certaines furent trop lourdes financièrement, d'autres invalidées par une instance nationale mais le plus souvent, dépassées techniquement. L'architecture décentralisée comme l'évolution constante des outils liés à Internet sont les principales causes de ces échecs.

IRIS : Que penser de l'affaire Wikileaks et de sa répercussion au niveau mondial ?

Charles Bwele : Avec l'affaire Wikileaks, les gouvernements ont brutalement découvert ce que les industries de la musique et du cinéma ont appris depuis une dizaine d'années : les fichiers numériques peuvent être facilement copiés et rapidement distribués, a fortiori à l'ère des réseaux sociaux et de l'Internet mobile où le partage de données publiques ou confidentielles est devenu une quasi règle d'or auprès des jeunes générations. Le soldat Bradley Manning qui fut la source première des fuites sur la diplomatie américaine côté jardin, est typiquement un « millenial » c'est-à-dire d'un vingtenaire qui a grandi avec l'Internet et la téléphonie mobile. Au-delà du tumulte médiatique, d'autres Wikileaks apparaîtront, la conduite des affaires diplomatiques et militaires continuera son bonhomme de chemin mais il faut vite réinventer un secret-défense propre à l'ère informationnelle car quoiqu'on en dise, l'Etat est un Léviathan qui a besoin de secrets.

Yannick Harrel : L'affaire Wikileaks a été de prime importance, non pas tant pour les révélations (souvent plus proches de confirmations que de révélations) que pour le fait que des États ont été ébranlés par une fuite qui leur a échappé. Fondamentalement il n'est pas évident de déterminer leur importance. L'on a, en certaines occasions prétexté que les Révolutions arabes auraient été provoquées en partie par ces fuites : c'est un peu hâtif, en revanche elles n'ont pas contribué à rasséréner le climat intérieur. D'autant que les forces les plus remuantes sont celles qui ont été connectées avec

l'extérieur et par conséquent agrégatrices de tout élément susceptible de corroborer et renforcer leur lutte. Julian Assange a été neutralisé par une procédure judiciaire à son égard et sous la menace d'une extradition aux États-Unis, seulement qu'adviendra-t-il si de futurs Wikileaks décentralisés apparaissent ? Au fond, il semblerait que ce soient plus les États occidentaux qui ont subi de plein fouet les révélations Wikileaks puisque ce sont chez eux que les réactions les plus virulentes ont été entendues et lues.

IRIS : Le phénomène Anonymous est-il pur effet de mode ou devrait-il persister et même se « radicaliser » dans le futur ? N'a-t-on pas affaire à une forme plus élaborée des petits groupes de hackers d'autrefois ?

Charles Bwele : Anonymous et Lulzsec sont une forme de contestation « en meutes sans leader » typique de générations natives des réseaux numériques, avec son romantisme révolutionnaire orienté vers la transparence des données, la liberté ou la neutralité de l'Internet. Ces mouvances « hacktivistes » doivent énormément leur succès à la réaction des médias et des autorités alors qu'il s'agit simplement de cybermilitantisme agrémenté de vandalisme électronique, loin du cybercrime organisé qui cause silencieusement plus de dégâts à court ou à long terme. D'une certaine façon, le défacement de sites Internet, l'injection SQL massive ou l'attaque DDOS sont des pendants numériques du tract, sitting ou du cocktail Molotov. Qui peut croire un instant que cette « contestation 2.0 » ait quelque impact réel sur l'ordre ou le désordre économique établi ? Paradoxalement, les seules protestations en masse de millions d'internautes de par le monde et de géants du Web tels que Google et Facebook font sérieusement réfléchir les sénateurs américains et le parlement européen à chaque projet peu ou prou liberticide comme l'Acta, le Pipa ou la Sofa...

Yannick Harrel : Le phénomène s'inscrit dans le temps et semble passionner crescendo les médias traditionnels. C'est une nébuleuse difficile à cerner avec un tableau de chasse qui comporte des noms assez prestigieux tels que HBGary Federal ou encore Stratfor. Le danger est suffisamment pris au sérieux par les autorités pour qu'Interpol ait coordonné des poursuites à leur encontre, avec un coup de filet fin février en Espagne et quelques pays d'Amérique du Sud. D'un autre côté, l'hacktivisme ne risque pas d'en être ébranlé pour des raisons simples : coût de mise en oeuvre faible, anonymisation (partielle), approche de nouveaux membres par des réseaux sociaux, outils numériques « clef en main » disponibles, décentralisation des organisations. En outre, leur côté « Robin des Bois » séduit parmi la population, notamment la plus jeune.

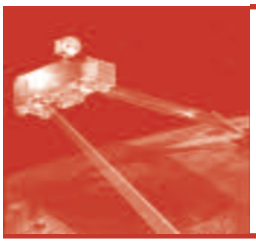
IRIS : La cyberguerre relève-t-elle d'un risque réel ou n'est-ce qu'un épouvantail brandi par certains états pour justifier un contrôle serré de l'Internet ?

Yannick Harrel : Le souci lorsque l'on évoque le terme de cyberguerre c'est l'assimilation aux règles ordinaires d'un conflit conventionnel. C'est là, à mon sens, une grosse difficulté. La question s'était par ailleurs posée en 2007 suite aux cyberattaques envers l'Estonie. Un pays Balte très dépendant des nouvelles technologies de la communication et de l'information, à tel point qu'il se surnomme lui-même E-stonie. Membre de l'Otan depuis 2004, il avait été évoqué l'éventualité de l'application de l'article 5 du Traité de l'Atlantique Nord pour faire intervenir les alliés contre celui que l'on montrait du doigt, la Russie. Il n'en a rien été faute de règles claires de belligérance dans le domaine cyber et surtout de certitude quant à l'origine de ces attaques cybernétiques. Il n'en demeure pas moins qu'un centre de cyberdéfense de l'Otan a vu le jour à Tallinn en mai 2008. Pour l'heure, nous avons affaire à des cyberattaques qui peuvent le cas échéant accentuer les dommages et perturbations causés par une guerre conventionnelle mais nous ne sommes pas encore dans un cadre de

■■■ cyberguerre proprement dit. L'on s'en rapproche cependant du fait de notre dépendance aux nouvelles technologies... Et le cyberespace est clairement déjà devenu un espace conflictuel, du reste l'ancêtre d'Internet n'avait-il pas été prévu pour résister à une attaque nucléaire, le plaçant de plain-pied dans une logique polémologique ? Les États de fait emploient ou emploieront d'autres justifications pour renforcer leur contrôle d'Internet.

Charles Bwele : La récurrence des cyberattaques ne fait pas une cyberguerre, pas plus que l'usage d'armes chimiques lors d'un conflit conventionnel en fait une guerre chimique. À ce jour, la cyberguerre relève d'une probabilité ou de la prospective. Par ailleurs, les enjeux de sécurité sont très souvent liés à des enjeux de contrôle, et ceci est d'autant plus vrai dans le cyberespace en général, et sur l'Internet en particulier. À mesure que les sociétés, les économies, les infrastructures et les vies personnelles et professionnelles s'étendront dans les réseaux numériques, la sécurité et le contrôle de l'Internet deviendront des enjeux cruciaux sur les plans techniques, économiques, stratégiques et politiques. Toutefois, le cyberespace, qui ne se réduit guère à l'Internet, est un environnement immatériel en évolution constante, crée et recrée chaque jour par les hommes, et donc radicalement différent de l'environnement terrestre, maritime, aérien ou spatial. Selon l'analyste technologique Larry Downes, le cyberespace nous soumet aux lois de la disruption qui, en résumé, stipulent que « les technologies évoluent exponentiellement tandis que les mentalités et les réglementations évoluent par incrémentations ». D'où cette difficulté proprement sisyphienne qu'éprouvent les politiques, les stratèges, les juristes et les techniciens à penser la sécurité et la réglementation de l'Internet. Ce n'est qu'un début. ■

*
* * *
*



OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

IRIS
INSTITUT DE RELATIONS INTERNATIONALES ET STRATÉGIQUES

Technologies « de libération » : quelle réalité ?

par François-Bernard Huyghe,
Directeur de recherche à l'IRIS

Les technologies de libération – d'après une définition du Journal of Democracy (une des nombreuses organisations qui veut les rendre accessibles aux citoyens du monde entier) – sont « toute forme de technologie de l'information et de la communication (TIC) qui peut étendre la liberté économique, sociale et politique. À l'époque contemporaine, ce sont essentiellement les formes modernes, interconnectées de TIC numériques, l'ordinateur, Internet, le téléphone mobile et une multitude d'applications inventives dont les nouveaux médias comme Facebook et Twitter ». Une vision qui correspond assez bien à celle d'Hillary Clinton et d'un « droit de l'homme » de se connecter. Mais que l'on aurait pu appliquer à la machine à écrire. Il est vrai que des États totalitaires ont interdit la possession de machines à écrire !

Quant aux technologies de censure, de contrôle ou de surveillance, ce serait tout celles qui permettent d'intercepter, de filtrer, d'attribuer à une personne réelle (donc que l'on peut éventuellement arrêter), de falsifier, de submerger sous une propagande inverse... des propos politiquement subversifs ou des contenus illicites.

Technologie vs technologie

Ce vocabulaire suscitera des critiques. Les uns diront que l'on ne qualifie pas le fusil de technologie « de liberté » ou d'oppression suivant qu'il est au service d'une cause juste ou injuste. Ou, plus finement, que l'imprimerie n'a pas été en soi une technologie « de rationalité » ou la télévision une technologie « de massification », même s'il est impossible de comprendre la montée des Lumières sans la force de l'imprimé ou la sociologie des masses au XX^{e} siècle en faisant l'impasse sur le plus important des mass media.

D'où des objections sémantiques et politiques : parler de technologie « de libération », n'est-ce pas faire un choix idéologique en amont et mythifier la technique en lui confiant un rôle presque messianique ? Ou des objections techniques plus fines. Ainsi : les principes ne sont-ils pas les mêmes utilisés de façon différente ? Un outil de cryptologie peut aussi bien servir à une transaction commerciale qu'à un groupe d'opposants et créer des relais en cas de coupure d'Internet, il ne sert pas forcément des groupes de résistants ou de démocrates.

Mais dans l'esprit de leurs commanditaires ou de leurs utilisateurs, la fonction de certains dispositifs est bien claire. Il existe des technologies qui, dès leur conception, tendent à visent un usage par une communauté pouvant protester ou se soulever, ou, à l'inverse, par ceux qui s'efforcent de repérer ou de museler ladite communauté. Tout est dans l'intention. Facebook a été conçu pour un usage ultra-élitiste dans une des universités les plus snobs du monde, puis est devenu le lieu d'une nouvelle forme de convivialité planétaire qui va bientôt relier un milliard d'homme. Désormais, des défenseurs des droits de l'homme, un dictateur ou un groupe djihadiste peuvent faire avancer leur cause en multipliant les « friends » sur leur « mur d'amis ». Facebook n'est donc pas en soi une technologie de libération ou de répression. Au même titre que des techniques commerciales servant à l'identification des contenus ou des auteurs, la plate-forme se prête à des usages politiques. ■■■

Innovation technique, lutte politique

En revanche, quand quelqu'un fabrique un appareil pour se connecter à Internet de relais en relais, même si les autorités veulent en couper l'accès, lorsqu'il conçoit un système de surveillance des élections truquées par les internautes ou lorsqu'il imagine une méthode de chiffrement destinée à tout citoyen, la démarche est différente. De même – mais en sens inverse – lorsqu'il produit un logiciel de surveillance et d'interception des communications électroniques.

En somme, des appareils et des applications sont conçus pour lutter contre d'autres appareils et applications (et pour contrer leur capacité de connexion, de dissimulation, de repérage...). La phrase souvent répétée selon laquelle la technologie est neutre et que seul son usage la met au service de la libération ou de l'oppression trouve ici ses limites. Un système technique (outil, logiciel…) pensé « stratégiquement » pour surmonter une volonté et une intelligence adverses.

Des industriels fabriquent des matériaux ou des logiciels destinés à contourner la censure. Et d'autres laboratoires ou compagnies des moyens de repérage de contenus (politiquement suspects ou violant le droit de propriété intellectuelle) et vendent ces technologies à des gouvernements qui ne sont pas forcément très sympathiques.

L'inventeur et le stratège

Très logiquement, les inventeurs et fabriquants sont sollicités par les gouvernements soit pour leur donner des moyens de contrôle (chez eux) soit pour aider (chez les autres) des opposants à se connecter contre le gré des autorités. Tandis que des groupes militent pour la neutralité d'Internet, en soi, c'est-à-dire en pratique pour que chacun ait les moyens d'accéder aux données qu'il veut et d'exprimer ce qu'il désire, sans risque d'être empêché ou identifié. Et ceci indépendamment de la "cause" qu'il défend ou du lieu où il est.

Les trois étages – technique (matérielle, logicielle), économique, politique – se déterminent donc mutuellement. Pour former un jeu de pouvoir dont la somme est tout sauf nulle et que l'on ne peut comprendre sans commencer par la base technologique. ■

*
* * *
*

Glossaire

Anonymiseur : serveur qui permet de devenir anonyme sur la toile en supprimant les données personnelles de l'utilisateur (adresse IP, navigateur…). On ne peut donc pas identifier la personne physique qui a effectué cette navigation.

Bambuser : site suédois de diffusion de vidéo en streaming pour téléphone portable

Commotion : nom de code d'un projet de logiciel libre. Objectif : créer un réseau sans fil à haut débit totalement autonome. Il fonctionnerait sur les fréquences Wifi sans s'appuyer sur un relais existant comme le téléphone, le câble ou le satellite.

Couche 3 du modèle OSI : dite aussi couche réseau est une zone tampon entre les adresses physiques (cartes réseau) et les adresses logiques (IP). Son importance est due à sa fonction de routage des données.

Darknet : réseau social virtuel privé généralement de petite taille et non répertorié par les moteurs de recherche usuels. Il permet de partager des fichiers mais aussi de communiquer. Pour détruire un Darknet, il est nécessaire de détruire l'ensemble des nœuds qui le compose.

Deep Packet Inspection : activité qui consiste à analyser le contenu d'un paquet réseau soit pour en tirer des statistiques, soit pour filtrer le contenu soit pour remonter la source d'intrusions.

Défacement : anglicisme désignant la modification non sollicitée de la présentation d'un site web à la suite du piratage de ce site. Il s'agit d'une forme de détournement d'un site par un hacker.

Distributed denial-of-service (DDOS) : attaque visant le dysfonctionnement d'un serveur en le submergeant de trafic inutile par un nombre de sollicitations massif en simultané ou en un temps très court.

Hashtag : mot ou phrase précédés par le symbole « # ». Ils sont utilisés par les réseaux sociaux pour renvoyer vers le mot ou phrases clefs.

Hacktiviste : contraction entre hacker et activiste. Informaticien qui infiltre des réseaux et qui déjoue les sécurités pour diffuser un message politique.

Lutz Security ou Lulzec : groupe de hackers responsables de plusieurs intrusions informatiques. Il a obtenu une couverture médiatique importante en raison des victimes notables et des messages sarcastiques qu'il diffusait suite à ses attaques. Le 25 juin 2011, le groupe annonce la fin de ses activités. L'ensemble des membres du groupe aurait été arrêté le 6 mars 2012.

Peekabooty : système de navigation en peer-to-peer (P2P) qui permet à un ordinateur situé dans une région où la censure existe de lancer une recherche via un ordinateur situé dans une zone non-censurée.

Peer to peer : modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi le serveur. Il peut être centralisé ou décentralisé. Parfois francisé sous la dénomination de Pair à Pair.

PirateBox : plate-forme Wifi portable qui permet de partager des fichiers dans un anonymat totale. Il est composé d'un routeur wireless, d'une batterie, d'un serveur Linux et d'un disque dur USB.

Pretty Good Privacy (PGP) : logiciel de chiffrement et déchiffrement hybride. Il garantit la confidentialité des messages mais aussi l'authentification des données.

Proxy : logiciel servant d'intermédiaire entre deux ordinateurs ou logiciels. Il s'agit d'une sorte d'interphase pour que les deux structures se comprennent et puissent communiquer.

Psiphon : logiciel qui permet de créer un réseau privé virtuel (VPN). Psiphon permet de contourner les politiques de filtrage et de censure existante dans certains pays.

Secure Sockets Layer ou SSL: protocole de sécurisation des échanges sur Internet.

The Onion Router (TOR) : logiciel libre sous licence BSD révisée qui permet de créer un réseau décentralisé de routeurs sur le modèle des couches d'un oignon. Un anonymat partiel est garanti sur la toile.

Tweecrypt : logiciel de chiffrement à la volée. Il permet de créer un disque virtuel chiffré contenu dans un fichier et de le monter comme un disque physique réel. TrueCrypt permet ainsi de chiffrer une disquette ou une clé USB.

Tweet : message bref envoyé via Twitter. Il contient maximum 140 caractères.

Ushaidi : plates-formes en open source qui permettent le crowdsourcing et la géolocalisation instantanée. Il est très utilisé par les activistes. Il permet de suivre en direct une série d'événement via plusieurs contributeurs.

Virtual Private Network (VPN) : protocole de tunnelisation qui permet de sécuriser un système informatique. Il interconnecte plusieurs systèmes… tout en les protégeant du monde extérieur.

Wikileaks : site web lanceur d'alerte spécialisé dans la diffusion massive d'informations classées « confidentiel », « secret » et « secret-défense ». Il base son existence sur la fuite d'informations.

*
* * *
*

L'Observatoire Géostratégique de l'Information

Sous la direction de François-Bernard Huyghe, cet observatoire a pour but d'analyser l'impact de l'information mondialisée sur les relations internationales. Comprendre le développement des médias et de l'importance stratégique de la maîtrise de l'information. Il analyse, par exemple les rapports de force entre puissances politiques et économiques et les firmes qui contrôlent le flux des informations dans le Monde.

IRIS - Institut de Relations Internationales et Stratégiques
2 bis, rue Mercoeur
75011 Paris - France
iris@iris-france.org

www.iris-france.org
www.affaires-strategiques.info

Secrétariat de rédaction : Pierre-Yves Castagnac