CHRONIQUE ÉCONOMIQUE DES TIC

Bulletin d'information, vol. 1, no. 1, Juin 2012
ISSN 2292-2288

DANS CE NUMÉRO

RÉSUMÉ ANALYTIQUE

Dans le contexte de la mise en oeuvre du programme d'expansion du nombre de gTLD approuvé par ICANN et de la renégociation du contrat de l'IANA liant ICANN et la NTIA américaine, 2012 marque la réouverture des RTI après 24 ans de libéralisation du secteur des télécommunications. Une négociation politique globale sur les enjeux de dénationalisation et de gouvernance multipartite des réseaux de télécommunications s'organise et les acteurs signalent leurs positions et mobilisent leurs appuis sur de nombreux axes politiques conflictuels.

Malgré l'existence de programmes para-légaux de partage de données entre fournisseurs de services Internet et agences policières et de renseignements, les États-Unis et le Canada envisagent d'enchâsser ces pratiques dans de récentes initiatives législatives concernant la cybersécurité. Des deux côtés de la frontière, la définition de « cyber-menace » y est problématique.

CHRONIQUE ÉCONOMIQUE DES TIC

Bulletin d'information, vol. 1, no. 1, Juin 2012

Gouvernance globale d'Internet

Gouvernance Internet : BRIC contre États-Unis, putsch onusien à l'horizon ?

Aux dires de certains, Internet serait en danger, et la menace viendrait en fait de l'ONU. Au cours des dernières semaines, plusieurs commentateurs ont effectué des sorties publiques dans les médias pour denoncer une potentielle prise de contrôle d'Internet émanant des pays du BRIC (Brésil, Russie, Inde, Chine) qui, laissent-ils présager, seraient tentés de confier des responsabilités de gestion technique jusqu'alors reservées a des ONG privées, dénationalisées et présumement plus neutres (l'ICANN notamment) à des fonctionnaires et bureaucrates de l'ONU. Si les propos de certains essayistes et commentateurs semblent exagérés, il n'en reste pas moins que les négociations qui ont présentement cours en vue de préparer le terrain pour la Conférence mondiale des télécommunications internationales (CMTI-12 - « *World Conference on International Communications* ») qui se tiendra en décembre et au cours de laquelle les fondements politiques du Net seront vraisemblablement appelés a être revus suscitent de vives inquiétudes. L'absence relative d'acteurs en provenance de la société civile et du milieu technique privé au sein des forums supranationaux proposés souleve de vives questions en termes de légitimité. Bien que l'histoire politique d'Internet témoigne de plusieurs autres tentatives de supra-nationalisation par le passé, l'échec de ces dernières ne présume pas pour autant que celles qui auraient actuellement cours vont subir le même sort.

Des mises en garde

Le Net tel qu'on le connaît serait menacé, et l'adversaire ne serait nul autre que l'ONU. Robert McDowell, commissaire au FCC (« *Federal Communications Commission* ») n'y est pas allé de main morte dans une lettre ouverte au Wall Street Journal en février dernier pour défendre les vertus du modèle actuel de gestion du Net. Autrefois domaine réservé des informaticiens, ingénieurs et scientifiques, Internet aurait prospéré et perduré, dit-il, parce qu'il échappait justement à la main lourde de l'autorité étatique. Or, le modèle de gouvernance multipartite (« *multi-stakeholder model* ») prédominant actuellement (qui s'est developpé de manière complètement indépendante de la règlementation internationale en vigueur a l'époque) a su s'établir dans le vide politique créé par la libéralisation du secteur via, entre autres, la ratification du Règlement des télécommunications internationales (RTI – « *International Telecommunication Regulations* »), traité indépendant, signé en 1988 au sein de l'UIT (« Union Internationale des

LE RTI ET LA CMTI-2012

Le Règlement des télécommunications internationales (RTI) est un outil de l'UIT ayant force obligatoire et la portée d'un traité. Il met en place des principes généraux et des dispositions régissant les services de télécommunications à l'échelle internationale. Le RTI et le Règlement des radiocommunications (RR) constituent les règlements administratifs de l'UIT et sont complémentaires à la Constitution et à la Convention de l'UIT. Le RTI a été adopté dans le cadre de la Conférence administrative télégraphique et téléphonique internationale de 1988 (CAMTT-88), qui s'est déroulée à Melbourne, en Australie. Aucune modification n'a été apportée au RTI depuis son entrée en vigueur le 1er juillet 1990. L'UIT organisera une conférence mondiale sur les technologies de l'information (CMTI) en vue d'examiner et de mettre à jour le RTI. L'événement se déroulera à Dubaï, aux Émirats arabes unis, en décembre 2012, immédiatement après l'Assemblée mondiale de normalisation des télécommunications (AMNT) de l'UIT.

Source : Industrie Canada (http://www.ic.gc.ca/eic/site/smt-gst.nsf/fra/sf10026.html)

Télécommunications »). En conséquence de diverses raisons techniques, économiques et politiques[1], les rouages techniques fondamentaux du réseau des réseaux ne sont non pas gérés par des gouvernements nationaux ou une quelconque instance internationale, mais à travers une panoplie d'ONG (comme l'ICANN, l'IETF ou le W3C[2]) favorables aux valeurs libérales de respect des libertés individuelles et de libre-circulation de l'information. Le sommet de 2012 pour le renouvellement du RTI de 1988 peut donc être vu comme une tentative internationale de rétablissement des fondements légaux d'un modèle de gouvernance inter-étatique qui fut en vigueur pendant de nombreuses décennies sur le secteur des télécommunications traditionnelles.

Or, soulève-t-il, ce même modèle pourrait être instrumentalisé par certains pays (principalement la Russie, l'Inde et la Chine) qui chercheraient à profiter des discussions entourant la révision du RTI pour reprendre le contrôle des flux d'information sur leur territoire. Répression, atteintes à la vie privée des citoyens et des internautes, tarification du trafic numérique transfrontalier au profit des fournisseurs d'accès et gouvernements nationaux (comme dans le cas des appels téléphoniques par exemple); le cri de ralliement du commissaire a été repris par plusieurs autres commentateurs au

[1] Dont certaines sont abondamment développées dans Mueller (2004) et Drake (2000)

[2] Voir, entre autres, Russell (2006) pour une présentation du détail de la période de concurrence entre standards techniques et modèles d'organisation et de développement technologique que vécurent, par exemple, l'IETF et l'UIT.

cours des derniers mois. Plus récemment, lors de la conférence Freedom to Connect, Vinton Cerf, un des pères fondateurs d'Internet devenu depuis « évangéliste en chef » chez Google vint lui aussi prévenir d'une potentielle prise de contrôle par une UIT désireuse de s'ériger en tant que « gendarme global de Internet ». Michael Joseph Gross opine, lui, que les discussions au sein du SMSI s'inscrivent même dans le cadre plus large d'une « Guerre mondiale 3.0 » ou s'affronte un éventail d'axes idéologiques à divers degrés d'opposition mutuels. Exagération ou pas, de part et d'autre les acteurs fourbissent leurs armes et mobilisent leurs appuis en vue du sommet de Dubaï ou se tiendront en décembre prochain les discussions entourant la révision du RTI.

Menace réelle ou épouvantail ?

Vu le manque d'informations actuellement disponibles, difficile d'évaluer l'exactitude des propos de McDowell. Néanmoins, plusieurs initiatives récentes publiquement disponibles temoignent d'un réel désir chez certains pays de redéfinir les termes fondamentaux de l'organisation politique d'Internet.

L'essentiel de la menace articulée par McDowell fait référence à une proposition de « code de conduite » déposée le 12 septembre dernier par la Russie, la Chine, le Tadjikistan et l'Ouzbekistan (Ministère des affaires étrangeres chinois). Invoquant un besoin de sécurisation de l'information et du cyberespace, le document visait a réaffirmer la souveraineté des États en la matière tout en jetant les bases d'une administration multilatérale et stato-centrée des rouages techniques fondamentaux d'Internet (notamment en termes d'adressage). Vladimir Poutine a déjà déclaré publiquement son appui a l'UIT lors d'un entretien avec son secrétaire général, Hamadoun Touré, en juin dernier et plusieurs autres estiment, comme lui, que l'UIT serait favorablement positionnée pour hériter des responsabilités qui incombent actuellement à l'ICANN.

L'Inde, elle, fit précédemment valoir sa position à travers une proposition (texte complet) soumise a l'Assemblee générale de l'ONU le 26 octobre dernier prônant la création d'un nouveau forum, le CIRP (« *Committee on Internet Related Policies* »). Appuyée par l'Afrique du Sud et le Brésil (qui s'en est subséquemment dissocié), cette nouvelle organisation composée de quelque cinquante individus mandatés par les pays membres se rassemblerait une fois par année et serait depourvue de tout pouvoir coercitif. Outre la défense des droits humains, le forum viserait à faciliter la résolution des disputes, faciliter la négociation de traités et de conventions, assurer la

coordination des divers acteurs face aux enjeux globaux liés a Internet et créer un espace pour traiter des enjeux liés aux questions de développement. La proposition, réitérée par les representants indiens le 18 mai dernier, fait néanmoins face à de vives critiques, même à l'interne (India Today). Pawan Duggal, analyste indien en cyber-législation, rappelle que les craintes associées aux soulèvements populaires du « printemps arabe » ne devraient pas pour autant pousser la plus grande démocratie du monde à s'associer à des pays qui, comme la Russie ou la Chine, affichent de piètres feuilles de route en matière de respect des droits humains…

Les États-Unis et l'Internet « minimaliste »

La posture américaine fait écho aux préoccupations soulevées par McDowell. La « *cyberweek* » du 28 mai comportera non seulement un vote sur le fortement contesté CISPA (voir ci-bas), mais aussi une audience du sous-comité sur les communications et la technologie de la Chambre des représentants visant justement à examiner les diverses propositions concernant la régulation d'Internet. McDowell y sera lui-même, et défendra une position analogue à celle presentée dans son éditorial de février dernier. L'Administration Obama réfère, quant à elle, aux orientations édictees dans sa « stratégie internationale pour le cyberespace » pour réitérer les bienfaits du caractère émergent, participatif et communautaire d'Internet (Blogue - Office of Science and Energy Policy - Maison Blanche) et ajoute, elle aussi, qu'une mainmise étatique viendrait selon elle éroder l'esprit d'entreprise et d'innovation que l'on y trouve.

CMTI-12 : Une nouvelle étape dans le débat sur la gouvernance Internet ?

Bien que la dernière rencontre du SMSI du 14-18 mai dernier ait été qualifiée de succès lors de sa cérémonie de clôture par le secrétaire general de l'UIT, Monika Ermert rapporte toutefois que les discussions y ont creusé des divisions encore saillantes (IP-Watch.org). Le forum lui-même, qui a le bénéfice d'être chapeauté et financé par diverses instances onusiennes (UIT, ECOSOC, UNESCO, CNUCED), s'inscrit en competition désormais directe avec l'IGF, un autre forum à vocation similaire mais appuyé par voie de donations volontaires. Déplorant l'opacité du processus, un collectif d'ONG a par ailleurs publié une lettre ouverte (Texte complet - Center for Democracy and Technology) en appelant aux États membres et au secrétaire général d'autoriser la libre-circulation des divers documents préparatoires et propositions préliminaires ainsi qu'à favoriser la participation d'acteurs provenant de la société civile, tel que stipulé dans les principes mêmes du

SMSI, adoptés lors du Sommet de Tunis en 2005, prônant la création d'une société de l'information ouverte et inclusive et la participation d'une pluralité d'acteurs, particulièrement en provenance des pays en voie de développement.

Malgré tout, le manque de transparence du processus jusqu'à présent pousse à une relative prudence analytique. D'un côté, l'article et la position de McDowell lui-même contredit un mémo diplomatique daté du 23 janvier dernier (Texte complet) et distribué au sein de cercles restreints dans lesquels les négociateurs américains affirment que les négociations découlant du CMTI-11 peuvent être qualifiées de succès et que personne n'ait véritablement semblé vouloir doter l'UIT de responsabilités en matière d'adressage (notant par le fait même que les questions d'ordre plus pratique, comme la lutte à la fraude et l'accès en itinerance (« *roaming access* ») dominaient les échanges). Ils y notent toutefois que plusieurs pays émergents pourraient être tentés de profiter de la prochaine ronde de négociations, soit CMTI-12, pour contrecarrer l'agenda « minimaliste » américain et amender le RTI pour des questions de politiques commerciales. Joel Hruska (ExtremeTech) rappelle d'ailleurs que l'ordre minimaliste prôné par McDowell permet entre autres aux fournisseurs d'accàs Internet (FAI) américains de facturer d'importants frais d'accès à leurs homologues étrangers et que cette « balkanisation » tant crainte par le commissaire de la FCC aurait probablement aussi pour effet de rétablir un rapport de force qui soit nettement moins favorable aux intérêts nationaux et privés américains.

« Guerre Mondiale 3.0 » ou simple feu de paille ? La complexité des enjeux, la diversité des intérêts en place et l'abondance d'alternatives politiquement envisageables ont pour effet de laisser plusieurs questions en suspens. D'un côté, comme le rappelle Milton Mueller (Internet Governance Project), c'est loin d'être la première fois que l'on assiste à des frictions sur ce plan. Certains pays, notamment la Russie, tentent depuis plusieurs années de doter l'UIT des pouvoirs réservés a l'ICANN, et, faute d' appuis suffisants, ceux-ci n'ont essuyé que des échecs jusqu'à présent. L'Internet « minimaliste » - tel qu'érigé dans sa mouture actuelle - concorde à plusieurs égards avec certains des intérêts américains déclarés, et ces derniers n'en sont pas à leur premier tour au bâton. L'ICANN elle-même est née dans le cadre d'une autre lutte politique impliquant les États- Unis, des puissances européennes et asiatiques, l'UIT et plusieurs acteurs des communautés civiles et informatiques.

Recherche et rédaction :
Olivier Dagenais

Pour en savoir plus :

Who'sWhoLegal, The 2012 World Conference on International Telecommunications : Another Brewing Storm Over Potential UN Regulation of the Internet, 28/11/2011, en ligne: http://www.whoswholegal.com/news/features/article/29378/the-2012-world-conferenceinternationaltelecommunications-brewing-storm-potential-un-regulation-internet/

Internet Governance Project, *Threat Analysis of ITU's WCIT (Part 1) : Historical Context*, 24/05/2012, en ligne : http://www.internetgovernance.org/2012/05/24/threat-analysis-of-itus-wcit-part-1-historical-context/

Drake, W.J., 2000. "The rise and decline of the international telecommunications regime". In C. T. Marsden, ed. *Regulating the global information society*. Londres, pp. 124–177.

Mueller, M., 2004. Ruling the root: Internet governance and the taming of cyberspace, Cambridge, Mass.: MIT Press.

Russell, A., 2006. "Rough Consensus and Running Code"and the Internet-OSI Standards War. *IEEE Annals of the History of Computing*, 28(3), pp.48–61.

CHRONIQUE ÉCONOMIQUE DES TIC
Bulletin d'information, vol. 1, no. 1, Juin 2012

Cybersécurité et libertés fondamentales

Internet et cybersécurité à la frontière canado-américaine
Après l'échec des projets de loi SOPA et PIPA, la loi CISPA

Les États-Unis poursuivent leur guerre contre les produits numériques piratés et les attaques informatiques. Après l'échec des projets *Protect IP Act* (PIPA) et *Stop Online Piracy Act* (SOPA), dont l'objectif principal était de contingenter l'accès outre-mer à des sites Internet délivrant du contenu « piraté », la Chambre des Représentants (CR) vient d'adopter la *Cyber Intelligence Sharing & Protection Act* (CISPA), introduite en Chambre le 30 novembre dernier par Michael Rogers (R-MI) et Dutch Ruppersberger (D-MD). Largement bipartisan, celui-ci mobiliserait, s'il est entériné, les fournisseurs de services Internet (FSI) américains afin de mettre en place un régime volontaire de partage d'informations entre ces entreprises et le gouvernement. La « cybersécurité » étant au coeur du débat, cette loi reçoit davantage d'appui de la part d'entreprises comme Facebook qui avaient protesté, conjointement avec la société civile, contre les projets PIPA et SOPA. Cependant, le Président Barack Obama pourrait apposer son véto au projet, car il estime que la loi ne propose aucun mécanisme dissociant les informations recueillies de leurs usagés, mettant ainsi à risque la vie privée des citoyens. Selon l'administration Obama, le projet n'arrive pas à sécuriser l'infrastructure numérique du pays, tout en n'offrant aucune garantie que les FSI utiliseront les données à bon escient.

Un problème de définition : la notion de menace informatique

La CISPA fait partie de la stratégie américaine portant sur la « cybersécurité » visant à déployer des mesures afin de combattre les menaces informatiques. Comme le font remarquer certains auteurs et plusieurs groupes de pression tels que l'*Electronic Frontier Foundation* (EFF), la notion de menace y serait définie de manière trop expansive : « toute action pouvant résulter en un accès non-autorisé à, manipulation de, ou atteinte à l'intégrité, confidentialité, ou disponibilité d'un système d'information ou d'informations conserver sur, traité par, ou encore transitant sur un système informatique »[3]. Cette définition a des répercussions pour le consommateur puisque la CISPA permettra entre autres aux FSI d'accéder aux données personnellement identifiables de leurs usagés, comprenant l'ensemble des communications de

[3] Traduction libre.

ceux-ci (courriels, adresse IP, conversations vocales, etc.). Ces entreprises pourront donc collecter les informations privées de leurs utilisateurs et les transmettre aux agences gouvernementales américaines qui, à leur tour, pourront les communiquer à d'autres entreprises.

L'immunité pour les FSI

Par ailleurs, la stratégie américaine pour contrer les cyber-menaces donnera assez de latitude aux FSI pour qu'elles installent des systèmes de surveillance dans leurs réseaux. Il est difficile d'imaginer quelles seront les mesures que prendront les FSI, mais il est certain qu'elles pourront bloquer des sites spécifiques ou des individus et utiliser différents systèmes de filtrage. Une des problématiques soulevées par la notion trop large de menace informatique est justement que celle-ci pourrait affecter la neutralité des réseaux (*net neutrality*[4]). Plusieurs soulignent que cette crainte fait écho aux revendications des FSI qui cherchaient à « limiter leur service » de bande passante (*downstream*) face à des applications de *streaming*[5], de *peer-to-peer*[6] ou encore de services concurrents.

En vertu de la CISPA, les FSI auront un rôle central dans l'archivage des informations et de leur distribution aux agences gouvernementales américaines. C'est pourquoi la CISPA protégerait ces firmes contre des poursuites civiles ou criminelles aussi longtemps que leurs activités seraient faites de « bonne foi ». Par ailleurs, les dispositions prévues dans le texte quant à d'éventuelles poursuites de consommateurs face aux FSI qui transmettraient de l'information sont favorables pour ces entreprises, ce qui rendrait difficile pour les consommateurs de faire valoir leurs droits devant une cour de justice.

Ce projet reste controversé alors qu'il vient affecter la vie privée des citoyens américains, sans réellement régler la question de la « cybersécurité ». Le Républicain Mac Thornberry de la CR souligne en effet que l'approche

[4] Les tenants de ce concept défendent, entre autres, qu'Internet ne doit pas être « contrôlé » par les FSI. Sur la question, voir Faulhaber, 2011; Powell, 2009; Wu, 2007 et Sidak, 2006.

[5] L'Office québécois de la langue française propose « lecture en transit » comme traduction. Cela signifie la lecture d'un flux vidéo ou audio « à la carte » ou à mesure que celui-ci est diffusé (*live streaming*) sur Internet (traduction libre)

[6] Une telle approche permettrait aussi à ces derniers d'opérer une discrimination à l'encontre de certains protocoles Internet, particulièrement ceux permettant le partage de fichiers en mode pair-à-pair (peer-to-peer) souvent employé à des fins de piratage.

développée dans cette loi se concentre seulement sur l'échange de données, mais considère que c'est tout de même « un pas dans la bonne direction ». Or, cette loi ne résoudra pas les problèmes d'infrastructures qui relèvent de l'ensemble de la communauté informatique plutôt que du gouvernement américain, comme le mentionnent les auteurs du rapport « *Cyber Attack : A Risk Management Primer for CEOs and Directors* » du British-North American Committee.

La CISPA et ses impacts sur les consommateurs canadiens

Malgré le fait qu'Internet soit un médium « sans » frontières, il existe toujours des enjeux de régulation nationale. En Amérique du Nord, le Canada et les États-Unis ont uni leurs efforts afin de traiter la question des menaces informatiques comme étant un sujet de sécurité transfrontalière. « Par-delà la frontière » est un document ciblant les initiatives communes pour sécuriser la frontière canado-américaine et une ébauche d'un projet de coopération plus large entre les deux pays. Concernant la sécurité informatique, ils

> *[…] « feront rapport de l'impact de la mise en commun des pratiques les plus efficaces en cybersécurité, du nombre de contacts pris avec des pays tiers et des progrès réalisés vers la réalisation des objectifs canadiens et américains dans le dossier du cyberespace au sein des instances internationales grâce à ces efforts »*
>
> *(**Source :** Par-delà la frontière, p.32.)*

La crainte est de voir les États-Unis faire pression pour que le Canada adopte des règles similaires à la CISPA, si celle-ci est adoptée. Parallèlement, il convient de noter que le Canada est en voie d'adopter deux lois qui affecteraient la vie privée de ses citoyens. Le projet de loi C-12[7] modifiant la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) redéfinit la notion d'autorité légitime actuellement limitée à l'État pour l'étendre au FSI et propose d'élargir les paramètres permettant aux FSI de transmettre de l'information sans le consentement de leurs clients. Par ailleurs, les FSI n'auront pas besoin de vérifier si le requérant a les autorisations légales avant de transmettre les informations privées de leurs clients.

[7] *Loi édictant la Loi sur la protection des renseignements personnels et des documents électroniques.*

Le projet de loi C-30[8], quant à lui, permettrait aux FSI de collecter les informations privées et de transmettre ces informations, grâce à une immunité incluse dans le projet. Selon Michael Geist, C-30 autoriserait, en outre, une instance gouvernementale à réclamer ces informations, incluant les courriels et les habitudes de navigation Internet, toujours sans détenir de mandat. Cette mesure donnerait davantage de liberté aux FSI, qui seront plus confortables de se plier aux demandes du gouvernement.

Bien que les projets C-12 et C-30 n'aillent pas aussi loin que la CISPA, il importe de se questionner sur l'utilisation qui sera faite des données personnelles des utilisateurs d'Internet, autant aux États-Unis qu'au Canada. La CISPA n'autorisant pas les consommateurs à connaître les informations collectées à leur insu, elle soulève un débat important. Il faudra suivre les développements entourant de la sécurité des réseaux tout en gardant en tête les enjeux liés aux questions de liberté et de vie privée. Si, au Canada, les projets de loi semblent se diriger vers une adoption certaine, rien n'est assuré aux États-Unis et le véto de M. Obama pourrait bien aider les législateurs à préciser la stratégie américaine en matière de sécurité informatique.

Sources :

Canada. Affaires étrangères et Commerce international Canada. 2011. « Par-delà la frontière : une vision commune de la sécurité du périmètre et de la compétitivité économique ». Ottawa : Imprimeur de la Reine.

Canada. Lithwick, Dara. Division des affaires juridiques et législatives. Résumé législatif. Services d'information et de recherche parlementaires. Projet de loi C-12 : Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques. 41-1-C-12F. Ottawa : Bibliothèque du Parlement.

Faulhaber, Gerald R. 2011. « Economics of net neutrality: A review ». In *Communications & Convergence Review*, Vol. 3, No. 1, pp. 53-64.

Rodriguez, Katitza. Openmedia. What CISPA could mean for Canadian privacy. En ligne. http://openmedia.ca/blog/eff-what-cispa-could-mean-canadian-privacy. Page consultée le 18 avril 2012.

Le partage d'informations; d'hier à aujourd'hui, une pratique courante aux États-Unis

Pour comprendre la *Cyber Intelligence Sharing & Protection Act* (CISPA), il est nécessaire de mettre en perspective les pratiques déjà en place aux États-Unis

[8] Loi édictant la Loi sur les enquêtes visant les communications électroniques criminelles et leur prévention et modifiant le Code criminel et d'autres lois.

pour contrer certaines formes d'attaques informatiques. Kashmir Hill, souligne que la CISPA ne créerait pas un précédent puisqu'un mécanisme est déjà en place pour assurer la liaison entre des entreprises de tous les domaines et le gouvernement. Effectivement, des entreprises ont le loisir de transférer de l'information sensible découverte sur leurs réseaux au *Federal Bureau of Investigation* (FBI) via la *National Cyber Forensics and Training Alliance* (NCFTA). Cet organisme à but non lucratif, créé par un ancien agent du FBI, Dan Larking, fonctionne déjà comme un conduit entre le FBI et les entreprises.

Depuis 1997 la NCFTA possède une entente légale avec le gouvernement américain afin de lui permettre de recevoir de l'information donnée par les entreprises pour ensuite la communiquer au FBI. L'organisme coopère aussi avec le *Department of Justice's Computer Crime and Intellectual Property Section* (CCIPS), en plus de travailler de concert avec des universités et les forces de l'ordre de différents paliers gouvernementaux. En pratique, la NCFTA travaille avec la *Cyber Initiative and Resource Fusion Unit* (CIRFU), une unité spécialisée du FBI présente dans les bureaux de la NCFTA, afin d'analyser les informations à transmettre par la suite au FBI. Cette entente assure la transmission d'informations sensibles puisque la NCFTA est protégée par son statut légal. En effet, celle-ci est un OBNL selon l'article 501(c)6 de l'*Internal Revenue Code*, ce qui lui permet de transiger avec les compagnies qui autrement, ne le feraient pas par précaution légale. Par ailleurs,

> *[i]n light of the PATRIOT Act's mandate to enhance cyber-forensic capabilities, the Alliance is poised to play a critical role in bridging the gap between law enforcement cyber-forensics and private-industry efforts to prevent, detect, and investigate computerrelated crime and terrorist activity"*
>
> *(Rush et Paglia, p.22)*

Selon son directeur Ron Plesco, pour y arriver, la NCFTA récupère les informations provenant d'adresses IP suspectes et des serveurs s'adonnant au « harponnage de données courriel » (*phishing*), pour ensuite les analyser, les agréger et finalement les transmettre au FBI. Le rôle de l'organisation s'arrête à fournir des informations générales telles que les adresses IP, aucun nom ni adresse postale ne peut-être transmis et il revient au FBI de monter un dossier et de faire enquête. Il reste que cette tactique déployée par le FBI lui donne un avantage certain : l'organisme fédéral n'a pas besoin de se procurer un mandat pour récupérer des données personnelles de citoyen, en plus de ne pas avoir à craindre de poursuite.

Repousser les limites actuelles; fournir davantage d'informations

Alors qu'avant la création de la NCFTA les entreprises pouvaient mettre des mois à fournir des bribes d'information au FBI, elles les partagent aujourd'hui rapidement, devenant de réelles partenaires du gouvernement qui, à son tour, peut partager des éléments d'enquêtes en cours avec elles. Kashmir Hill recense un cas précis de partage d'information entre le FBI et les entreprises en guise d'exemple. Alors qu'un groupe de serveur suspect provenant de l'Estonie s'apprêtait à être fermé par le FBI, celui-ci s'est rendu compte qu'une telle action couperait le service Internet de milliers d'utilisateurs Internet aux États-Unis. Pour remédier à cette problématique, le FBI a délégué à une entreprise la gestion du « système des noms de domaines » (DNS) de ces consommateurs. L'Internet Systems Consortium inc. de Paul Vixie a été l'OBNL retenu pour assurer la gestion DNS pendant la période d'inoculation massive des utilisateurs infectés par le DNS Changer[9].

Cet exemple met en exergue que l'échange de données, et parfois de données personnelles[10], est une procédure ayant cours entre le FBI et certaines entreprises depuis longtemps pour des raisons de sécurité. Qui plus est, la CISPA propose un cadre dans lequel la NCFTA s'inscrit déjà, soulevant la question de la nécessité de cette loi, bien qu'elle soit plus mordante.

L'Alliance nationale d'intervention judiciaire et de formation contre la cybercriminalité

Le pendant de la NCFTA au Canada est l'Alliance nationale d'intervention judiciaire et de formation contre la cybercriminalité (ANIJFC), dont les objectifs poursuivis sont les mêmes que son voisin du Sud. Peu d'information est disponible sur cette alliance canadienne, mais on sait qu'elle travaille avec différentes universités pour développer des systèmes d'identification pour débusquer les concepteurs de « *spam* ».

Pour conclure, il est difficile de prévoir quels seront les impacts de la CISPA aux États-Unis et des projets C-12 et C-30 au Canada sur les informations déjà transmises à la NCFTA et à l'Alliance. Plusieurs questions

[9] Le DNS Changer est le nom du virus. Il fonctionnait comme un miroir et redirige les internautes faisant des recherches sur les sites dont les propriétaires payaient pour la publicité. Il est important de mentionner que les consommateurs ont été avertis que leurs données étaient accessibles.

[10] Comme nous l'avons mentionné, les données personnelles sont regroupées en paquet.

sont soulevées cependant alors que ces projets de loi tentent d'aller plus loin que le partage actuel d'information et cherchent à encadrer légalement une activité qui semble être pratique courante.

Recherche et rédaction :
Victor Alexandre Reyes Bruneau

Sources :

Hill, Kashmir. Forbes. 2012. The FBI Workaround For Private Companies To Share Information With Law Enforcement Without CISPA. En ligne. http://www.forbes.com/sites/kashmirhill/2012/04/26/the-fbiworkaround-for-private-companies-to-share-information-with-law-enforcement-without-cispa/. Page consultée le 26 avril 2012.

Rush, Mark A. et Paglia, Lucas G. 2002. « Balancing Privacy, Public Safety, and Network Security Concerns after September 11 ». *Information Systems Security*, vol 11, no 2, pp. 15-24.

Pour en savoir plus :

Nakashima, Ellen. The Washington Post. Obama threatens to veto CISPA cybersecurity bill, citing privacy concerns. En ligne. http://www.washingtonpost.com/politics/obama-threatens-to-veto-cispa-cybersecurity-bill-citing-privacy-concerns/2012/04/25/gIQAkS3khT_story.html. Page consultée le 25 avril 2012.

Powell Alison. 2009. « Lessons from the Net Neutrality lobby: Balancing openness and control in a networked society ». En ligne. http://journal.webscience.org/130/1/websci09_submission_32.pdf. Page consultée le 21 avril 2012.

Sidak J. Gregory. 2006. « A consumer-welfare approach to Network neutrality regulation of the internet ». *Journal of Competition Law and Economics*, 2(3), pp. 349–474.

Wu Tim. 2007. A Brief History of American Telecommunications Regulation. En ligne. http://ssrn.com/abstract=965860. Page consultée le 21 avril 2012.

Actualités connexes

IPv6 arrive – qu'est-ce que ça veut dire pour vous ?

Il y a plus de 10 ans que IETF (Internet Engineering Task force) a développé le protocole IPv6 permettant d'augmenter exponentiellement le nombre d'adresses IPv4 ("Internet Protocol" version 4) datant de 1981 et prévoyant au plus quelque 4 milliards d'adresses. Malgré le fait longuement anticipé de l'éventuel épuisement des adresses IPv4, plusieurs entreprises de services Internet ou d'équipements informatiques et de réseaux n'ont pas activé les paramètres IPv6 sur leurs différents produits. IPv6 fournit quant à lui une banque de quelque 34 (1036) adresses IP (340, suivi de 36 zéros!), présumément suffisamment pour couvrir les besoins actuels et futurs du nombre croissant d'usagers, de terminaux et de fonctions usant du protocole Internet. Dans ce qui constituera le jour mondial du lancement d'IPv6, plusieurs entreprises activeront de concert, le 6 juin, les paramètres IPv6 de leurs produits. L'ISOC (Internet Society) a préparé un petit guide explicatif pour vous, citoyens et citoyennes, administrateurs et administratrices de la société de l'information dans laquelle nous vivons. Google propose aussi une page permettant de suivre l'adoption du nouveau protocole au niveau mondial à l'aide d'un diagramme et d'une carte interactive mise à jour en temps réel.

Après Stuxnet, voici Flame

Stuxnet, déployé en juin 2010, fut considéré par plusieurs comme étant le virus le plus avancé et ambitieux de l'Histoire numérique (voir un vidéo de la télé australienne sur la question). Crédité pour avoir forcé l'arrêt temporaire du programme iranien d'enrichissement d'uranium et la mise hors-service de cascades entières de centrifugeuses, le fameux ver informatique, que plusieurs associent à des intérêts israéliens, semble avoir fait des émules. Eugene Kaspersky, président du fabricant russe de logiciels antivirus, a annoncé le 28 mai dernier avoir découvert un autre programme malveillant, baptisé Flame (ou *Worm.Win32.Flame* pour les intimes), au cours d'une enquête commandée par l'UIT. Contrairement à Stuxnet toutefois, les analyses préliminaires semblent indiquer que Flame ne visait pas spécifiquement les systèmes SCADA (« *Supervisory Control and Data Acquisition* ») des PLC (« *Programmable Logic Controller* ») à vocation industrielle ou critique, mais plutôt la collecte d'informations non-ciblées, régulièrement relayées par canal crypté à un centre de contrôle distant (SecureList).

Iran, Google et le mystère du Golfe disparu

Si l'on s'en remet a Google Maps, le Golfe Persique n'existe pas, ou, du moins, son nom ne semble pas s'y afficher correctement (voir ici - page consultee le 29 mai 2012). L'evenement, emanant potentiellement d'une simple erreur technique, s'est transforme en bourde diplomatique des lors que le gouvernement iranien a menacé de traîner le geant de la recherche en cour et de le forcer a restaurer le nom, faute de quoi le geant americain de la recherche s' exposerait a de "lourdes consequences". Fait a noter, plusieurs pays du monde arabo-musulman preconisentsoit le nom de Golfe Arabe, soit celui de Golfe Arabo-Persique.

Iran et ailleurs, la censure va bon train

L'Internet iranien se referme de plus en plus sur lui-même. Le ministre iranien des télécommunications a annoncé récemment que les universités, les banques de même que les firmes d'assurances et de télécommunications (entre autres) ne pourront désormais plus transiger avec des clients faisant usage d'adresses de courriel offertes par des fournisseurs étrangers (comme Gmail ou Yahoo! Par exemple) et devront plutôt se rabattre sur des fournisseurs locaux et le Iran Mail ID (dont la phase d'enregistrement vient justement de commencer et qui exige la divulgation d'informations personnelles véridiques chez l'usager, devant légalement concorder avec celles dont dispose le gouvernement). Plusieurs estiment que le geste s'inscrit dans une initiative plus large visant la mise sur pied d'un Intranet national « Halal » (ou conforme à la Loi Islamique) sur lequel le gouvernement pourrait plus facilement exercer son influence. Les autorités iraniennes, elles, présentent un discours contradictoire sur la question. Rappelons que le régime a récemment bloqué le recours aux connexions sécurisées (HTTPS) sur son territoire, et que le blocage de sites étrangers ou jugés « immoraux » est croissant

Chronique économique des TIC

Bulletin réalisé par le Centre d'Études sur l'intégration et la mondialisation dans le cadre du projet d'études sur les technologies de l'information et des communications (ETIC)

Direction scientifique : Nicolas Adam, Michèle Rioux
Recherche et rédaction : Olivier Dagenais, Victor Alexandre Reyes Bruneau

Pour nous joindre : +1 (514) 978-3000 #3910
Sur le web : http://www.ceim.uqam.ca – ceim@uqam.ca

Abonnez-vous à la liste de diffusion et au fil RSS du bulletin!