COLLABORER POUR ÉLIMINER LES POURRIELS ET LES COMMUNICATIONS INDÉSIRABLES

IIC 2016 – SEMAINE DES POLITIQUES ET DE LA RÉGLEMENTATION EN MATIÈRE DE COMMUNICATIONS

LE 11 OCTOBRE 2016, BANGKOK (THAÏLANDE)

Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

Canada

Nº de cat. : BC92-94/2017F-PDF

ISSN : 978-0-660-08311-7

Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)
Ottawa (Ontario)
Canada
K1A ON2

Tél: 819-997-0313
Ligne sans frais : 1-877-249-2782 (au Canada seulement)

https://services.crtc.gc.ca/pub/submissionmu/bibliotheque-library.aspx

Photos: © ThinkStock.com, 2017

Also available in English

TABLE DES MATIÈRES

REMERCIEMENTS

Le CRTC souhaite remercier tous les participants à l'atelier, sans qui le présent rapport n'aurait pu être rédigé. Il souhaite particulièrement remercier les spécialistes suivants, qui ont contribué à titre de conférenciers et de modérateurs, stimulant une discussion approfondie et interactive.

- **Richard Bean**, président intérimaire, Autorité australienne des communications et des médias, Australie
- **Chris Chapman**, président, Institut international des communications
- **Stephen Eckersley**, chef de l'application de la loi, Commissariat à l'information, R.-U.
- **Adriana Labardini Inzunza**, commissaire, Instituto Federal de Telecomunicaciones, Mexico
- **Travis LeBlanc**, chef, Bureau de l'application de la loi, Federal Communications Commission, É. U.
- **Toni Li**, directeur adjoint (soutient), Bureau de l'autorité des communications, Hong Kong (région administrative spéciale)
- **Peter Merrigan**, enquêteur principal, Unité de la conformité des messages électroniques, ministère des Affaires intérieures, Nouvelle-Zélande
- **Christine Runnegar**, directrice, Politiques en matière de sécurité et de protection des renseignements personnels, Internet Society
- **Steve Unger**, dirigeant principal de la technologie et directeur du groupe de la stratégie, de l'international, des technologies et de l'économie et membre du conseil d'administration, Bureau des communications, (R.-U.)
- **Viola Veiderpass**, agente des crimes numériques, Direction des cybercrimes, Complexe mondial INTERPOL pour l'innovation

Le CRTC souhaite également remercier l'Institut international des communications pour son appui et son partenariat stratégique à l'atelier. Merci tout particulièrement à **Andrea Millwood-Hargrave**, directrice générale, et à **Amanda Crabbe**, directrice des programmes, pour leur orientation, leur leadership et leurs contributions inestimables à l'activité.

À titre de responsables de la réglementation, nous devons avoir une capacité d'adaptation, être ouverts à la collaboration et faire preuve d'innovation et de débrouillardise. En travaillant ensemble et en échangeant des idées durant des activités telles que celle-ci, nous améliorons notre efficacité à cet égard...

Jean-Pierre Blais, président et premier dirigeant, CRTC
Bangkok (Thaïlande)

CONTEXTE

Le 11 octobre 2016, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), en partenariat avec l'Institut international des communications (IIC), a tenu un atelier sur la lutte aux pourriels et autres formes de communications indésirables. L'activité d'une demi-journée était organisée dans le cadre de la semaine annuelle des politiques et de la réglementation en matière de communication, à Bangkok, en Thaïlande.

Comme beaucoup d'organismes de réglementation des communications, le CRTC est déterminé à garantir que les citoyens de son pays aient accès à un système de communication de calibre mondial qui est sécuritaire et fiable. Dans le cadre de son mandat, le CRTC est responsable de promouvoir le respect des cadres politiques canadiens sur les communications non sollicitées et de veiller à leur application. De plus, le CRTC travaille continuellement à l'amélioration de sa capacité de collaborer avec des partenaires clés (le secteur privé, les partenaires de gouvernements au Canada et les gouvernements étrangers) afin de réduire les préjudices aux consommateurs causés par la nature abusive des communications non sollicitées. En raison de la nature mondiale des réseaux de communication, et de l'abus dont font l'objet ces réseaux, la collaboration entre les administrations est essentielle à la réussite.

En établissant un partenariat avec l'IIC, le CRTC a voulu faire progresser la coopération internationale à l'égard de cette question importante. L'IIC a fourni le forum idéal pour favoriser la discussion, puisqu'il a offert une plateforme indépendante, internationale et reconnue où discuter des incidences importantes et évolutives des pourriels et des communications indésirables sur les citoyens et les entreprises à l'échelle mondiale. L'IIC a également offert l'accès à un réseau mondial de stratèges de haut niveau occupant des postes de direction, d'autorités réglementaires, d'organismes d'exécution, d'universitaires et d'autres experts. L'atelier a présenté l'IIC au milieu de l'application de la loi concernant les communications non sollicitées et a élargi la discussion sur les questions relatives aux politiques sur les communications. Finalement, l'IIC a offert un environnement ouvert et équilibré propice à la présentation de nouvelles idées.

OBJECTIFS DE L'ATELIER

L'atelier comportait trois objectifs. Le premier était de réunir des experts des milieux des politiques et de la mise en application de partout au monde afin de leur permettre d'échanger des points de vue et des expériences en matière de politiques, de règlements et d'application de la loi relativement aux pourriels et aux communications indésirables. Ces divers milieux sont engagés activement dans un dialogue et des travaux productifs pour lutter contre les pourriels et les autres communications non sollicitées. Par contre, ces conversations sont trop souvent tenues de manière isolée, principalement au sein d'un même milieu. Par conséquent, les politiques peuvent être élaborées sans que les besoins en matière d'application soient suffisamment pris en compte, et les décideurs n'obtiennent pas toujours la rétroaction des enquêteurs, ce qui donne lieu à des obstacles législatifs qui nuisent aux activités d'application. Les participants à l'atelier devaient également réfléchir à la façon de faire progresser les efforts relatifs à la collaboration transfrontalière. Les discussions visaient à mobiliser les responsables de la réglementation des pays émergents et de leur présenter les travaux de réseaux, de milieux et d'organisations bien établies dans le secteur. Tel qu'il a été mentionné, la nature mondiale de ces questions entraîne des défis uniques. Bien que des considérations importantes pour les efforts de lutte contre les pourriels puissent s'appliquer à la fois aux initiatives nationales et internationales, le présent rapport est axé sur les perspectives internationales et les approches de collaboration entre les juridictions.

L'assistance à l'atelier incluait 45 participants représentant des organismes de réglementation de toutes les régions du monde, des représentants de l'industrie, des universitaires et d'autres experts en communications. L'atelier a commencé par une présentation liminaire sur les principaux thèmes de discussion, les incidences des communications non sollicitées sur les gouvernements et les citoyens et le contexte actuel dans lequel les organismes de réglementation et d'application de la loi évoluent. Au cours de cette présentation, on a également informé les participants de l'existence du réseau d'application des lois en matière de communications non sollicitées (UCENet), un réseau spécialisé d'organisations coopérant à l'échelle internationale pour lutter contre les pourriels.

Le premier groupe de discussion, formé de spécialistes et d'agents responsables de l'application de la loi, a examiné trois études de cas, détaillant la nature internationale et inter-juridictionnelle des défis liés à la mise en application des règles sur les pourriels et les communications non sollicitées. Le groupe a ensuite discuté des défis et des occasions associés aux activités d'application transfrontalières. Il a notamment identifié le besoin de tenir un dialogue continu afin de garantir des stratégies optimales de mise en application et de conformité entre les pays. Le deuxième groupe, formé de spécialistes des politiques et de spécialistes techniques, a cerné les lacunes au chapitre de la capacité et les façons d'augmenter l'harmonisation des politiques et activités d'application transfrontalières. Il a notamment parlé des occasions et des défis propres aux économies émergentes. Pour conclure l'atelier, les cadres des organismes de réglementation ont tenu une discussion durant laquelle ils ont récapitulé les points importants soulevés par les deux groupes et ont incité tous les participants à l'atelier à définir les prochaines étapes. Une copie de l'ordre du jour de l'atelier figure à l'**annexe A**. Toutes les discussions durant l'atelier se sont déroulées sous la règle Chatham House.

Le présent rapport résume les discussions qui ont eu lieu durant l'atelier. Les sujets présentés durant l'après-midi se sont fréquemment chevauchés, ce qui témoigne des liens entre les défis liés aux politiques, à la technologie et la mise en application. Les liens entre les défis et les secteurs d'expertise ont été mis en évidence tout au long des discussions de groupe de l'atelier. Ainsi, le rapport reflètr ces thèmes, qui sont pertinents tant pour les pays ayant de solides dispositions législatives et politiques sur les pourriels que pour ceux qui veulent rapidement augmenter leur capacité et profiter des leçons apprises.

FAITS SAILLANTS

Le rapport est divisé en trois sections selon l'information partagée par les participants à l'atelier. La première partie explique pourquoi, à l'échelle internationale, il y a un besoin de poursuivre la collaboration transfrontalière sur les questions relatives aux pourriels et aux communications non sollicitées. Les communications non sollicitées représentent une grave menace pour la prospérité sociale et économique de l'économie numérique. La vente ou le vol des renseignements personnels des citoyens, qui figurent parmi les principaux motifs de l'envoi de pourriels, est devenu une activité lucrative sur le marché noir. Les secteurs public et privé ont la responsabilité partagée de protéger et d'informer les citoyens relativement à cette question.

La deuxième partie cerne les défis interdépendants liés aux activités d'application de la loi. Les communications non sollicitées, qu'elles proviennent de parties légitimes ou non, traversent souvent les frontières, provenant d'une juridiction, mais ciblant les citoyens d'une autre juridiction. Cette situation peut entraîner des défis juridiques, tandis que les avancées technologiques, qui permettent notamment d'envoyer des pourriels de manière anonyme, compliquent davantage les enquêtes. Également, les juridictions n'ont pas toutes les mêmes ressources et la même expertise, ce qui peut contribuer ou nuire à l'amélioration des capacités relatives aux activités d'application de la loi.

La troisième partie résume le consensus établi par les participants relativement à la voie à suivre. Précisément, les participants ont convenu que les parties intéressées (c.-à-d. les organismes de réglementation et d'application de la loi et les tierces parties telles que des représentants de l'industrie ou des universitaires) devraient :

- Tenir des discussions continues et régulières sur les politiques;
- Mettre à profit les partenariats avec le secteur public et le secteur privé;
- Participer activement au réseau UCENet.

Aucune organisation ne peut faire progresser les choses seule. Les décideurs politiques et les organismes d'application de la loi doivent collaborer à l'échelle internationale tout en établissant des cadres solides à l'interne. L'atelier représentait une première étape ambitieuse pour commencer ces travaux.

Pour une introduction aux rudiments des pourriels et des communications non sollicitées, les lecteurs peuvent consulter la trousse anti-pourriels (en anglais seulement) de la Internet Society et le rapport sur les pratiques exemplaires pour lutter contre les menaces faites en ligne, par téléphone cellulaire ou par téléphone filaire (en anglais seulement) préparé par le Messaging, Malware and Mobile Anti-Abuse Working Group (en anglais seulement).

01

POURQUOI AGIR MAINTENANT?

IL S'AGIT D'UNE RESPONSABILITÉ PARTAGÉE

La lutte aux communications non sollicitées – qu'il s'agisse d'appels indésirables, de pourriels, de maliciel[1] ou une infection par un réseau de zombies[2] – est une priorité pour plusieurs gouvernements qui sont déterminés à favoriser la croissance et l'innovation dans une économie numérique. Les menaces en ligne et mobiles représentent un risque important pour toutes les administrations souhaitant profiter de la prospérité économique et sociale créée par l'économie numérique. Dans sa plus récente édition de *Perspectives de l'économie numérique*, l'Organisation de coopération et de développement économiques (OCDE) explique ce qui suit :

> *L'économie numérique est indissociable d'innombrables aspects de l'économie mondiale. Son influence se fait sentir dans des secteurs aussi divers que la banque, le commerce de détail, l'énergie, les transports, l'éducation, l'édition, les médias ou la santé. Les technologies de l'information et des communications transforment les modalités de l'interaction sociale et des relations personnelles, tandis que la convergence des réseaux de téléphonie fixe et mobile, et de radiodiffusion, ainsi que l'interconnexion constante des appareils et des objets donnent forme à l'internet des objets*[3].

Internet et les technologies mobiles ont en effet révolutionné la façon dont le commerce est mené à l'échelle mondiale ainsi que la façon dont les gouvernements exercent leurs activités et offrent des services à leurs citoyens. Cependant, au fur et à mesure que l'utilisation d'Internet augmente chez les commerçants et les citoyens, de nouvelles avenues sont disponibles pour les acteurs malveillants en ce qui a trait à l'hameçonnage[4], le vol de données et d'autres actions nuisibles pour les consommateurs. Les courriels non désirés, les appels automatisés[5] et les messages texte non sollicités causent à tout le moins de la frustration chez les destinataires et dérangent ceux-ci. Mais ils peuvent également entraîner la fraude, les atteintes à la vie privée et des pertes financières importantes.

L'enjeu est grand pour les gouvernements et le secteur privé dans la lutte contre les communications non sollicitées : les effets dommageables et trompeurs des communications non sollicitées peuvent au bout du compte miner la confiance des citoyens dans les réseaux de communication et, généralement, dans l'économie numérique. Les polluposteurs les plus mal intentionnés sont habiles et rapides, et font preuve d'un mépris flagrant à l'égard de la loi. L'obtention de renseignements personnels par la tromperie ou ou carrément le vol est une activité lucrative sur le marché noir actuel. Dans plusieurs cas, les acteurs malveillants comptent sur leurs capacités de i) cacher leur identité, ii) d'abuser des vides juridiques et iii) d'exploiter de multiples juridictions à la fois. Dans un tel contexte, ils peuvent commencer et mettre fin à leurs activités rapidement, ce qui fait qu'il est extrêmement difficile de faire appliquer la loi.

[1] Les maliciels sont créés ou utilisés par les criminels pour perturber les opérations informatiques (voir https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf (en anglais seulement)

[2] Les réseaux de zombies sont des groupes d'ordinateurs infectés par un maliciel qui, en communiquant entre eux (souvent par un réseau complexe d'ordinateurs infectés), coordonnent leur activité pour collecter les renseignements que les maliciels subtilisent (voir https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf [en anglais seulement]).

[3] OCDE, Perspectives de l'économie numérique de l'OCDE 2015, éditions OCDE, Paris (voir http://www.oecd-ilibrary.org/fr/science-and-technology/perspectives-de-l-economie-numerique-de-l-ocde_9789264243767-fr).

[4] L'hameçonnage désigne les techniques utilisées par des personnes malveillantes pour piéger une victime et obtenir des renseignements personnels, organisationnels ou financiers de nature délicate (voir https://www.m3aawg.org/sites/default/files/M3AAWG_LAP-79652_IC_Operation-Safety-Net_2-BPs2015-06.pdf [en anglais seulement]).

[5] Les appels automatisés sont des appels de télémarketing non sollicités préenregistrés effectués à des lignes téléphoniques résidentielles. Il peut également s'agir d'appels automatisés ou préenregistrés ou de messages textes envoyés à des numéros de téléphone cellulaire, à des numéros de services d'urgence et à des chambres de patients dans des installations de soins de santé (voir https://www.fcc.gov/stop-unwanted-calls [en anglais seulement]).

De plus, la réglementation et l'application de la loi relatives aux communications non sollicitées relèvent du droit civil et du droit pénal, mobilisent divers organismes d'application de la loi et déclenchent divers cadres juridiques. La nature technique de la question implique également des opérateurs de réseau ainsi que des fournisseurs de services Internet et de courriels, tandis que les ministères gouvernementaux et les organismes de réglementation des communications gèrent souvent le volet des politiques et le volet législatif. La participation de ces milieux, qui ont chacun leurs objectifs et leur mandat, complique davantage l'établissement d'une approche d'application unifiée.

Tel qu'il a été souligné durant l'atelier, la lutte aux communications non sollicitées n'est pas un problème unique, mais plutôt une série de problèmes nécessitant un éventail de solutions. Les efforts de lutte contre les pourriels sont donc une responsabilité partagée par plusieurs milieux qui doivent harmoniser leurs efforts pour traiter la question : les gouvernements et législateurs, les responsables de la réglementation, les organismes d'application de la loi, les organisations non gouvernementales, le secteur privé et les spécialistes techniques. Les perspectives de la lutte contre les communications non sollicitées semblent peut-être peu prometteuses, mais les nouvelles ne sont pas toutes mauvaises. Bon nombre de pays ont réalisé d'importants progrès, notamment pour ce qui est d'établir des lois sur les pourriels et les communications non sollicitées, de promouvoir la conformité à la loi et d'établir des ententes de coopération nationale et des partenariats internationaux entre divers milieux.

COMMUNAUTÉS ET PARTENAIRES POUR LA LUTTE CONTRE LES POURRIELS

02

POURQUOI EST-CE UNE QUESTION COMPLEXE?

LES DÉFIS, QUI SONT D'ORDRE MONDIAL, NE CESSENT D'ÉVOLUER ET EXIGENT LA COOPÉRATION DE NOMBREUX PARTENAIRES

Les communications non sollicitées constituent un problème d'envergure mondiale. Partout, les citoyens sont vulnérables aux dérangements et aux attaques, quel que soit le cadre juridique en place dans le pays. Les défis que pose la lutte contre les communications non sollicitées découlent en partie de la nature pluridimentionnelle du problème, laquelle touche notamment les politiques, la technologie et le renforcement des capacités. Les sections qui suivent montreront en quoi ces défis sont interreliés.

INCOHÉRENCES DANS LES POLITIQUES ET LES LOIS

Rédiger des lois et des politiques en vue de lutter contre les communications non sollicitées est, en soi, une tâche complexe. Les communications peuvent autant provenir d'entreprises légitimes que d'entreprises illégitimes, et les violations peuvent être de nature civile ou de nature criminelle. Dans le cas des entreprises légitimes, un cadre civil clair conjugué à des mesures de sensibilisation efficaces peut fortement inciter à comprendre les règles et à les respecter. Si de tels outils sont en place, la plupart des entreprises légitimes se conformont à la loi et, de ce fait, protégeront les citoyens contre les pourriels et les formes de communications non sollicitées. Bien que les cadres de conformité prévoient souvent des mesures correctives, comme des pénalités ou des amendes, les participants à l'atelier conviennent qu'il est plus facile de faire respecter les règles lorsque les organismes de réglementation et les organismes d'application de la loi mobilisent les entreprises légitimes et les appuient en leur communiquant de l'information, en leur faisant part des pratiques exemplaires en matière de conformité et en menant d'autres activités de sensibilisation.

En revanche, dans le cas des entreprises illégitimes, on observe un lien de plus en plus étroit entre les communications non sollicitées et les activités criminelles. Par exemple, une entreprise illégitime peut effectuer des appels automatisés ou envoyer des pourriels pour vendre des produits et services frauduleux ou soutirer des renseignements personnels en faisant croire qu'elle se livre à des pratiques commerciales légitimes. Les réseaux de zombies peuvent aussi être utilisés pour envoyer des pourriels qui contiennent un maliciel ou qui en permettent le téléchargement à partir de liens menant à des sites Web infectés. Dans ces cas, l'existence d'un cadre de conformité assorti de pénalités ne contribue guère à limiter l'abus du système de communications. De plus, en raison de la nature trompeuse et frauduleuse de ces activités, d'autres organismes d'application de loi (p. ex. les services de police) et d'autres exigences législatives (p. ex. les cadres de justice pénale) peuvent souvent entrer en jeu, et ce, dans l'ensemble du pays.

Dans bon nombre de cas, l'envoi de pourriels est un acte qui relève d'un régime d'exécution en matière civile. Par contre, toute activité frauduleuse ou ajout d'un virus dans le message peut constituer une infraction criminelle. Dans de telles situations, les organismes de réglementation et d'application de la loi doivent collaborer et partager l'information avec d'autres organismes d'application de la loi, qui ont le mandat d'intenter des poursuites au criminel. Une telle démarche peut se révéler difficile à l'échelle nationale, et encore plus difficile à l'échelle internationale. Implliquer dans les discussions les partenaires d'autres pays, dont les perspectives au chapitre de la loi, des politiques, des structures organisationnelles et de la culture sont différentes, peut compliquer davantage le processus.

Lorsque les organismes d'application de la loi constatent l'existence d'une activité dommageable, il importe qu'ils en informent les consommateurs pour réduire les risques de fraude et qu'ils collaborent avec toute entreprise légitime qui en a été victime. Par exemple, lorsqu'un organisme d'application de la loi, qui a participé à l'atelier, a constaté l'existence d'une manœuvre frauduleuse par appels automatisés offrant des aubaines de voyage ou des forfaits de vacances en utilisant des marques maison bien connues, l'agence a collaboré avec les entreprises légitimes touchées afin d'afficher simultanément des alertes sur leurs sites Web respectifs, prévenant ainsi les citoyens de cette activité et empêchant du coup que la situation empire.

Peu importe que les communications non sollicitées proviennent d'une source légitime ou non, la technologie a permis que les violations transcendent les frontières en plus grand nombre, plus rapidement et, surtout, plus facilement. Il n'est donc pas étonnant que les types de communications non sollicitées les plus malveillantes proviennent souvent d'un pays autre que celui des destinataires ciblés. Or cette réalité peut se traduire par des obstacles juridiques, car il peut se révéler difficile d'intenter des poursuites dans des affaires transfrontalières sans disposer du pouvoir nécessaire aux termes de la loi ou, à tout le moins, de mécanismes permettant la mise en commun de renseignements, comme les protocoles d'entente.

Ces obstacles s'expliquent par le fait que les lois varient beaucoup entre les pays. En effet, s'il existe des incohérences ou des lacunes dans les cadres législatifs entre différents pays, il peut être difficile d'échanger des renseignements, de prendre des mesures d'exécution efficaces et de réclamer des mesures correctives. Par exemple, plusieurs pays hébergent des bases de données de renseignements sur les pourriels, qui collectent un grand volume de courriels infectés par maliciel et qui proviennent d'ailleurs. Il serait possible d'intensifier les efforts de lutte contre les pourriels et de prendre des mesures d'exécution plus efficaces si les pays mettaient ces données en commun. Toutefois, ces données contiennent souvent des renseignements personnels et les exigences nationales en matière de confidentialité peuvent limiter la capacité d'échanger ces renseignements (p.ex. des ententes supplémentaires et un pouvoir conféré par la loi pourrait être requis). Qui plus est, l'expérience pratique démontre qu'il peut être difficile d'exercer des pouvoirs d'application de la loi au-delà des frontières du pays. Comme l'a souligné un participant à l'atelier, lorsqu'un organisme mène une enquête sur une cible qui est établie à l'étranger, il lui est inutile de lui imposer une amende s'il n'est pas habilité à la faire appliquer. Il est tout de même possible de progresser lorsque les pays travaillent ensemble d'établir des partenariats de confiance.

Étude de cas : mise en commun de renseignements

Un participant a fait état des difficultés auxquelles il s'est heurté pour obtenir d'une compagnie établie à l'étranger les renseignements confidentiels dont il avait besoin pour poursuivre une enquête. La compagnie prétendait ne pas être tenue de communiquer les renseignements parce qu'elle n'exerçait pas ses activités dans le pays du participant, et ce, même si elle permettait une activité illégale dans ce pays. Heureusement, le pays du participant jouissait d'une relation de longue date avec l'organisme d'exécution du pays où était située la compagnie. Ensemble, ils ont pu invoquer leurs lois respectives pour produire et échanger les renseignements de façon légale aux fins de la prise de mesures d'exécution.

LA TECHNOLOGIE ET L'ANONYMAT

La technologie continue d'évoluer, et la complexification des communications non sollicitées également. Les avancées technologiques ont permis d'abaisser les coûts, d'éliminer les obstacles liés aux frontières, de fournir aux polluposteurs un accès facile à divers outils servant à tromper les consommateurs et à leur causer du tort. Non seulement les polluposteurs peuvent rejoindre un vaste public à une vitesse incroyable, ils peuvent aussi cacher facielement leur identité. Comme l'a expliqué un participant lors de l'atelier, il est possible d'envoyer des pourriels de façon anonyme à partir d'à-peu-près n'importe où dans le monde en utilisant des applications de contournement (p. ex. Whatsapp).

Certaines applications de contournement sont dotées de fonctions qui, en soi, facilitent le pollupostage. Par exemple, une application de clavardage qui ne demande pas de consentement additionnel de la part des utilisateurs avant de les ajouter à des forums de clavardage susceptibles de générer du pollupostage. Bien que de telles fonctions soient souvent involontaires, leurs répercussions peuvent causer divers types de dommages aux consommateurs, notamment le vol d'identité.

Il est facile de garder l'anonymat, même pour un polluposteur peu expérimenté. Comme l'a expliqué un participant à l'atelier, le polluposteur peut se servir d'une carte SIM (module d'identité d'abonné) prépayée pour obtenir un numéro de téléphone, seule exigence à remplir pour s'abonner à certaines applis de messagerie par contournement. Dans bien des pays, il est possible d'acheter une carte SIM sans abonnement ou inscription, de telle sorte que retrouver le polluposteur est pratiquement impossible.

Comme l'a souligné un autre participant, les répercussions des avancées technologiques ont affecté les communications non sollicitées non seulement sur les nouvelles plateformes, mais également sur les plateformes traditionnelles, dont la téléphonie. À titre d'exemple, chaque jour, des millions de citoyens reçoivent des appels automatisés. Un participant a indiqué que dans son pays, au moins 21 % des appels effectués sont des appels automatisés (c.-à-d. 1 sur 5). Les facteurs technologiques ont fait chuter les coûts de l'équipement et des services, ce qui a contribué au volume élevé de ces appels. Autrefois, il fallait de l'équipement spécialisé pour effectuer des appels automatisés; aujourd'hui, il suffit d'un logiciel sur un ordinateur ou un téléphone mobile.

Les appels automatisés sont également devenus un problème d'envergure internationale. Comme l'utilisation des applis de messagerie ou au courriel pour les pourriels, la majorité des auteurs d'appels automatisés misent sur le fait qu'ils peuvent cacher leur identité. Comme l'a expliqué un participant à l'atelier, les numéros de téléphone ne sont plus associés à une seule adresse physique. Et grâce aux progrès technologiques, il est plus facile d'obtenir de multiples numéros de téléphone et de mystifier[6] un numéro.

Étude de cas : pourriels par contournement

Les applications de contournement permettent aux polluposteurs d'ajouter des utilisateurs à des groupes de clavardage sans obtenir aucune forme de consentement. Le polluposteur peut ensuite créer un groupe de clavardage à partir d'un bloc de numéros de téléphone séquentiels et lui envoyer des polluposts en prétendant faussement faire la promotion d'une entreprise précise. L'entreprise en question peut être une entreprise légitime qui n'a ni envoyé le message ni autorisé son envoi. Dans un tel cas, l'entreprise légitime ne peut être blâmée juridement, mais remonter à la véritable source du pollupostage demeure un problème.

[6] La mystification de l'identité des appelants a lieu lorsque des télévendeurs illégitimes qui changent l'information qui apparaît sur l'afficheur d'identité de l'appelant pour se faire passer pour quelqu'un d'autre et amener le destinataire à répondre à l'appel (voir http://www.crtc.gc.ca/fra/phone/telemarketing/identit.htm).

En outre, avec l'arrivée de la technologie de commnunication vocale sur protocole Internet (VoIP), le coût des appels internationaux n'empêche plus de cibler une vaste zone géographique, ce qui veut dire qu'il peut être avantageux de faire les appels automatisés depuis l'étranger.

En plus de grandement faciliter l'envoi et la réception des communications non sollicitées, les avancées technologiques ont aussi permis aux polluposteurs de tirer profit des consommateurs, surtout d'obtenir frauduleusement des fonds. Sous l'angle de l'application de la loi, s'il est impossible de retrouver le polluposteur, il faut alors suivre la piste de l'argent. Par exemple, lorsque des renseignements personnels sont volés pour être revendus (p.ex. pour des demandes de cartes de crédit ou d'emprunts), retracer chaque transaction monétaire peut aider à remonter jusqu'au fraudeur.

La technologie permet désormais, et facilement, les paiements directs entre les polluposteurs et les victimes. Autrefois, le processus à suivre pour transférer des devises d'un pays à un autre était lourd et impliquait au moins une tierce autorité (p. ex. un caissier de banque). Cette tierce autorité aurait probablement davantage examiné une telle transaction. Aujourd'hui, il est extrêmement facile de transférer de l'argent d'une personne à une autre, que ce soit au moyen de cartes cadeaux, de devises virtuelles, de virements électroniques entre comptes bancaires, ou d'autres systèmes de paiement en ligne. Les occasions d'intercepter les transactions se faisant plus rares, les polluposteurs ont le temps d'encaisser les fonds obtenus frauduleusement et de se volatiliser avant qu'une victime constate qu'elle s'est fait escroquer.

RENFORCEMENT DES CAPACITÉS DANS LES PAYS ÉMERGENTS

En ce qui concerne les communications non sollicitées, tous les pays font face à des problèmes, mais ceux auxquels se heurtent les pays émergents sont bien différents. Comme indiqué dans les sections précédentes, les communications non sollicitées ont évolué et ne se limitent plus au courriel indésirable occasionnel. Ainsi, le contexte de la menace est nettement différent aujourd'hui de ce qu'il était lorsqu'Internet a fait son apparition. Qui plus est, dans de nombreux pays développés, l'infrastructure des télécommunications – et l'utilisation à mauvais escient qui y est associée – a évolué pendant près d'un demi-siècle, alors que les pays émergents sont passés directement aux technologies de communications mobiles sans avoir connu les technologies filaires. Par conséquent, comme l'a expliqué un participant, les pays émergents risquent de faire face à des polluposteurs avertis alors qu'ils n'ont pas eu l'occasion d'établir leurs compétences et leurs ressources lorsque la menace était plus simple.

Le participant a poussé son explication, indiquant que l'on observe souvent une croissance rapide et exponentielle du nombre d'utilisateurs du service Internet local lorsque la large bande devient abordable dans un pays. De nombreux pays émergents deviennent rapidement des économies principalement axées sur le commerce mobile, ce qui risque d'épuiser les ressources des gouvernements tout comme celles des nouveaux opérateurs de réseau, qui ne connaissent peut-être pas les regroupements qui luttent contre les pourriels ou les ressources connexes. S'ils ne disposent pas d'une loi antipourriel ou de cadres de réglementation, ou s'ils ne participent pas à des réseaux de coopération, les pays émergents sont plus vulnérables aux attaques de polluposteurs et risquent de servir de terreau fertile pour ces derniers.

Un autre participant a abordé certains des défis que pose l'établissement de partenariats avec des pays dont l'expérience en matière d'exécution de la loi n'est pas la même. À titre d'exemple, il a indiqué qu'un appel automatisé qui serait considéré comme une violation de la loi antipourriel dans un pays donné pourrait, dans un autre pays, être considéré comme une pratique commerciale dérangeante, mais tout de même inoffensive et légitime. Si une partie ne considère pas l'acte visé par l'enquête comme étant inapproprié, il sera vraisemblablement plus difficile d'obtenir une volonté de coopération et d'établir un sentiment de confiance.

03

PROCHAINE ÉTAPE?

SOLUTIONS MONDIALES EN RÉPONSE À DES PROBLÈMES MONDIAUX

Les communications non sollicitées et les communications indésirables défient les frontières tandis que les milieux des politiques et de l'application de la loi sont confrontés à des obstacles tels que les incohérences dans la loi, la technologie qui permet l'anonymat et les besoins précis des pays dont l'expérience en matière de politiques et d'exécution de la loi varient. À l'atelier, les participants ont tous convenu que la solution pour surmonter ces problèmes ne résidait pas uniquement dans les lois et les politiques antipourriel, ni dans une démarche axée uniquement sur l'application de la loi ou la technologie. En fait, comme l'a affirmé l'un d'entre eux, un ensemble d'efforts et de solutions progressives donne vraisemblablement de meilleurs résultats qu'un seul plan ambitieux. Par conséquent, les participants ont discuté d'activités possibles pour faire avancer ce travail. Ils ont convenu que les prochaines étapes requièrent la participation active et la coopération de tous les intervenants, y compris les organismes de réglementation, les organismes d'application de la loi, le secteur privé et les tierces parties intéressées, comme les universitaires et les organismes sans but lucratif. Les prochaines étapes sont les suivantes.

1. TENIR DES DISCUSSIONS CONTINUES ET RÉGULIÈRES SUR LES POLITIQUES

Les organismes de réglementation et les organismes d'application de la loi doivent s'appliquer à établir des règles, des politiques et des pratiques qui sont souples et efficaces. Sinon ils risquent de compromettre les avantages concurrentiels qu'offre l'économie numérique. Comme l'a décrit un participant, une démarche réglementaire efficace doit présenter un juste équilibre entre la nécessité de créer un milieu hostile pour les compagnies qui ciblent délibérément les membres vulnérables de la société et celle de créer un milieu de mobilisation et de soutien pour les compagnies qui font de leur mieux pour respecter la loi.

Un autre participant a fait remarquer qu'il est essentiel d'avoir une collaboration internationale concertée pour cibler les pourriels et les communications indésirables, non seulement lorsqu'ils sont envoyés, mais avant même que l'activité n'ait lieu. Très souvent, la coopération internationale en matière de politiques publiques exige temps, connaissances juridiques et ententes écrites officielles. En revanche, les menaces que présentent les communications non sollicitées sont souvent imminentes. Il est difficile d'établir une coopération internationale sans d'abord établir à l'échelle du pays des politiques, des cadres juridiques et une coordination entre les secteurs.

Les participants à l'atelier ont admis que les incohérences entre les pays (p. ex. les différences dans les lois et l'absence de cadre de réglementation) peuvent limiter la capacité d'obtenir et de mettre en commun les renseignements nécessaires à la poursuite de certaines enquêtes. Ainsi, les participants ont convenu que les pays, quel que soit leur niveau d'expérience, devraient tenir régulièrement des discussions sur les politiques pour mettre en commun leurs expertises et leurs pratiques exemplaires en vue d'adopter des lois ou de revoir les lois existantes. Ces discussions contribueront aussi à nourrir les relations qui permettraient un meilleur échange des renseignements et une meilleure collaboration.

Tel que l'a souligné un participant, l'expérience révèle qu'un système en évolution rapide, comme Internet, est mieux servi lorsque l'approche à l'égard des politiques repose sur l'ouverture, le consensus et la participation. Cette approche impliquerait de multiples parties prenantes et tiendrait compte de la grande variété d'intérêts des personnes dont les droits et les responsabilités se recoupent d'un secteur à l'autre, et d'un pays à l'autre.

Par conséquent, les participants à l'atelier ont convenu qu'un forum international – nouveau ou existant – permettrait de poursuivre les discussions sur diverses questions de politique précises, dont les suivantes :

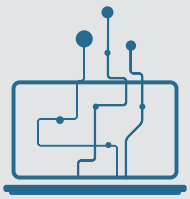
- Quelles sont les « leçons apprises » à prendre en considération pour l'élaboration de politiques et de lois antipourriel? Quel est le meilleur moyen de garantir que les dispositions soient souples et permettent la communication rapide des renseignements d'un pays à l'autre?
- Comment faire pour garantir que les dispositions des politiques et des lois soient suffisamment souples pour évoluer au fil du temps et s'adapter à la technologie, aux nouvelles plateformes et aux nouveaux protocoles?
- En quoi peut-on améliorer, ou rendre plus efficaces, les ententes entre les pays et les ententes au sein des pays?
- Quel est le rôle du citoyen dans l'acquisition des connaissances de base? Quel est le juste équilibre entre la prise de mesures pour assurer la sécurité et la confidentialité, et la sensibilisation et l'éducation afin d'habiliter et informer les citoyens?

2. MISER SUR LES PARTENARIATS ENTRE LE SECTEUR PUBLIC ET LE SECTEUR PRIVÉ

Les participants à l'atelier ont convenu que les cadres juridiques et les réseaux d'application de la loi, tant à l'échelle nationale qu'internationale, ont besoin d'avis et de support des intervenants du secteur privé. De façon précise, le secteur privé peut fournir des technologies et des incitatifs commerciaux à titre de compléments aux outils classiques d'application de la loi. Les opérateurs de réseau, les entreprises de télécommunication et les fournisseurs de services Internet (FSI) à l'échelle du monde disposent, en raison de leur rôle dans la construction et l'exploitation des infrastructures de communication, d'une grande influence pour contrôler l'envoi et la réception des pourriels.

Tout au long de l'atelier, les participants ont souligné des démarches novatrices de lutte contre les pourriels nécessitant des partenariats avec le secteur privé, telle que les suivantes :

INITIATIVES POUR LA LUTTE CONTRE LES POURRIELS ET LES COMMUNICATIONS INDÉSIRABLES

	MÉCANISME	EXEMPLE	DESCRIPTION
	Base de données de renseignements sur les pourriels	Intelligence Hub (ICO) (en anglais seulement)	Outil à partir duquel les citoyens peuvent signaler les pourriels et autres menaces électroniques aux organismes gouvernementaux. L'industrie peut aussi alimenter les bases de données de renseignements sur les pourriels, fournissant ainsi des renseignements supplémentaires pour justifier les mesures d'exécution.
	Signalement par composition abrégée	#7726 ou #Spam	Lorsque la personne reçoit un message non sollicité, elle peut composer le 7726, ou « spam », et la plainte est automatiquement acheminée à une base de données utilisée par les organismes d'application de la loi.

	Projets de coalition de l'industrie appuyés par le gouvernement	Robocall Strikeforce (FCC) (en anglais seulement)	Des compagnies de technologie et de communications s'unissent pour mettre en commun des renseignements, travailler avec les organismes de réglementation et les consommateurs, et lutter contre les communications abusives de façon efficace.
	Recherche et rapports	Rapport national sur la cybercriminalité (INTERPOL) Operation Safety Net (M3AAWG) (en anglais seulement)	Les organismes d'application de la loi, les partenaires du secteur privé et d'autres groupes obtiennent et partagent des renseignements sur ce problème qui évolue rapidement. Ces rapports incluent des analyses des cadres juridiques et techniques, cernent les lacunes en matière de cybercapacité et présentent les pratiques exemplaires pour les gouvernements, les organismes de réglementation et le secteur privé.

Par conséquent, les participants à l'atelier ont convenu qu'il est essentiel, pour l'élaboration de protocoles d'exécution multidimensionnelle, d'établir un dialogue et des partenariats avec les intervenants du secteur privé. Lorsque l'on détecte la présence d'une activité illégale sur les réseaux de fournisseurs de services de télécommunication ou de FSI, il est à l'avantage de tous les intervenants que les renseignements soient mis en commun.

Dans bon nombre de pays, les organismes d'application de la loi travaillent souvent avec diligence pour intervenir de manière proactive afin de prévenir les menaces à l'intérieur du pays et au-delà des frontières. Néanmoins, une grande partie des activités d'exécution se fait de manière réactive, une fois le dommage causé. Or le secteur privé, en tant qu'opérateurs de réseau et d'experts en technologie, peut fournir de précieux renseignements sur les menaces en temps réel. Par exemple, si un FSI est alerté qu'une infection se propage sur le réseau, il peut, sur-le-champ, arrêter le trafic malveillant qui surcharge le système.

Un des principaux facteurs de réussite consiste à disposer de processus et de protocoles normalisés qui sont mis en commun avec les intervenants concernés, tant à l'échelle nationale qu'internationale. Par exemple, il est essentiel que le secteur public et le secteur privé entretiennent un dialogue continu pour créer des protocoles de notification bidirectionnels pouvant être déployés rapidement en cas de brèche de sécurité. De plus, grâce à son expertise en cybersécurité, le secteur privé peut déceler des activités nuisibles (p. ex. une commande connue et une activité de contrôle de serveur[7] exécutée sur le serveur d'un partenaire privé) de façon plus rapide et plus efficace. Il peut ensuite communiquer le renseignement à l'organisme d'application de la loi, qui à son tour peut recourir aux outils que lui confère la loi, notamment des pouvoirs de perquisition et d'injonction, pour interrompre l'activité et recueillir les renseignements nécessaires afin de prendre des mesures d'exécution.

Les intervenants du secteur privé collaborent déjà à l'échelle de la planète pour traiter ces questions. À titre d'exemple, le Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG [en anglais seulement]), un regroupement mondial dirigé par l'industrie qui, dans un cadre confidentiel, se penche exclusivement sur les problèmes opérationnels que cause l'utilisation abusive d'Internet. Ce groupe publie activement des articles sur les pratiques exemplaires, des énoncés de position, des vidéos de formation et d'information et autres document. De plus, il prodigue des conseils d'ordre technique et opérationnel aux gouvernements et aux organismes de politique publique qui élaborent de nouvelles politiques et de nouvelles lois[8] relatives à Internet.

D'autres importants collaborateurs incluent divers types d'équipes d'interventions en cas d'indicent lié à la sécurité informatique (ERIS) et d'organismes à but non lucratif tel que Spamhaus. Les ERIS ont la responsabilité de coordonner et d'appuyer l'intervention à un énévement ou un incident lié à la sécurité informatique au sein d'un organisme (p.ex. le gouvernement, des organismes commerciaux ou des organismes à but non lucratif). Leur objectif est de minimiser et de contrôler le dommage créé par ces incidents, de fournir des conseils efficaces concernant les activités d'intervention et de récupération, et de travailler pour prévenir d'éventuels incidents[9]. Le projet Spamhaus est un organisme international à but non lucratif qui retrace les pourriels et les menaces cybernétiques et fournit les renseignements en temps réel aux réseaux Internet principaux, aux entreprises en ligne ainsi qu'aux fournisseurs de sécurité Internet. Spamhaus travaille également avec les organismes d'application de la loi afin d'identifier et suivre les sources de pourriels et de maliciels à l'échelle internationale[10].

Étude de cas : détection de la menace

Un participant à l'atelier a fait état d'un protocole de notification qui a porté des fruits. Dans le cadre de ce protocole, l'organisme d'application de la loi assurait le suivi d'un maliciel et d'autres menaces électroniques et se servait des renseignements ainsi recueillis pour alerter les parties intéressées. Ces dernières étaient alors en mesure de bloquer les menaces ou de les contrer. Il aurait été possible d'intervenir après coup, mais cette démarche a permis de stopper l'activité illégitime pendant qu'elle avait lieu, atténuant encore plus les dommages aux consommateurs.

[7] Serveurs de contrôle qui sont utilisés pour envoyer à distance des commandes souvent malveillantes à un réseau de zombies, ou réseau d'ordinateurs compromis : http://www.trendmicro.com/vinfo/us/security/definition/command-and-control-(c-c)-server

[8] Voir https://www.m3aawg.org

[9] Voir https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

[10] Voir https://www.spamhaus.org/organization/

3. S'INVESTIR ACTIVEMENT DANS LE UCENET

Il existe une autre ressource vitale pour promouvoir la coopération dans le domaine de l'application transfrontalière de la loi est le Unsolicited Communications Enforcement Network (en anglais seulement [UCENet]), anciennement appelé le Plan d'action de Londres (the London Action Plan). Établi depuis longtemps, ce réseau a pour but de favoriser la coopération internationale au chapitre de l'application de la loi en ce qui concerne les pourriels et la téléphonie. Il vise aussi à traiter les problèmes qui se rattachent aux communications indésirables, comme la fraude et l'escroquerie en ligne ou par téléphone, l'hameçonnage et la propagation de virus.

Les participants à l'atelier ont convenu qu'il faut absolument s'investir dans le UCENet pour établir un partenariat transfrontalier dans les domaines de l'application de la loi, du renseignement, des communications et de la formation. Cette communauté d'organismes d'exécution reconnaît depuis longtemps que les activités en ligne et le télémarketing ne sont pas liés aux limites géographiques et juridictionnelles. Étant donné que de nombreux organismes gouvernementaux fonctionnent à l'aide de ressources limitées, UCENet favorise la collaboration par ensembles de compétences et domaines d'expertise, réduisant ainsi le dédoublement d'efforts pour l'atteinte d'objectifs communs. Parmi ses membres, on compte des agences de 27 pays, des ministères, des parties intéressées provenant du secteur privé, d'organismes à but non lucratif et des universitaires. Du point de vue de l'application de la loi, le réseau permet à ses membres d'apprendre l'un de l'autre de leurs expériences. Les participants à l'atelier recommandaient que d'autres gouvernements et organismes intéressés deviennent membres du UCENet pour que le réseau ait une plus grande portée et qu'il procure plus d'avantages.

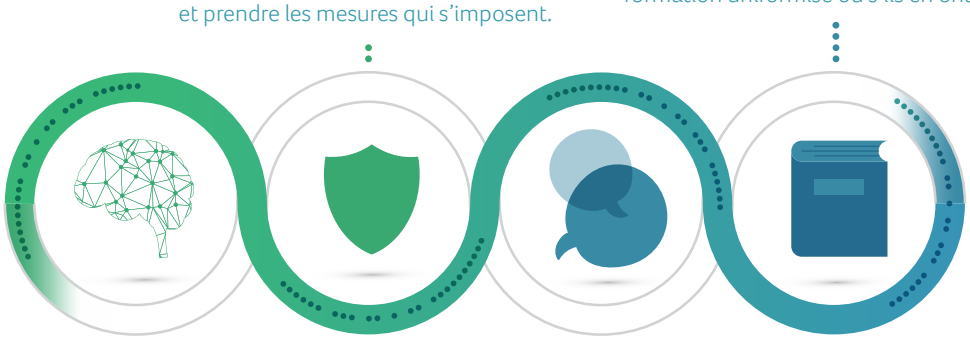
Les membres du UCENet profitent en outre de nombreux efforts coordonnés qui touchent l'échange d'information, le renseignement et les techniques d'enquête. Par exemple, les membres du réseau travaillent ensemble à analyser et à communiquer les renseignements et les données pertinents pour améliorer en temps opportun les activités de coordination et de conformité/d'exécution entre eux. Lorsqu'ils peuvent compter sur des voies de communication ouvertes et dignes de confiance, les organismes d'application de la loi sont capables d'intervenir rapidement pour cerner les risques et trouver des façons de s'attaquer aux problèmes qui existent à la fois au pays et à l'étranger.

Les membres actifs actuels du UCENet peuvent, eux aussi, y gagner à s'investir dans le réseau. En effet, diverses occasions s'offriront à eux, qu'il s'agisse de formation continue, de contributions à des projets de recherche, de possibilités de faire preuve de leadership en transmettant des pratiques exemplaires et des leçons apprises à des membres qui commencent tout juste à instaurer des mesures d'exécution.

PILIERS ET PRIORITÉS DE UCENET

APPLICATION DE LA LOI
Maximier notre pouvoir collectif et notre portée pour protéger les citoyens, surtout les plus vulnérables. Se servir des renseignements et des éléments de preuve recueillis pour déceler, contrer et prévenir les infractions criminelles et civiles à la loi, et prendre les mesures qui s'imposent.

FORMATION
Offrir une formation valable aux enquêteurs et aux praticiens lors de l'assemblée annuelle. Vérifier si les membres du UCENet aimeraient avoir accès à un programme de formation uniformisé ou s'ils en ont besoin.



RENSEIGNEMENT
Recueillir, analyser et communiquer les renseignements ou données pertinentes pour permettre d'améliorer les activités de coordination et de conformité/d'exécution. Intervenir rapidement pour cerner les risques et les occasions d'agir, et collaborer pour traiter les défis et les problèmes communs.

3. COMMUNICATIONS
Favoriser et fournir une méthode fiable, sûre et efficace pour la mise en commun de l'information et des renseignements entre les membres et les partenaires du UCENet, notamment aux termes du protocole d'entente du UCENet, afin de permettre l'exécution du plan opérationnel. Publiciser et promouvoir nos activités de conformité et d'exécution. Dans le but de renforcer la coopération et la coordination, mettre en valeur les avantages que procure l'adhésion au UCENet et veiller à ce que les membres comprennent le différent contexte de chaque pays.

Source : www.ucenet.org

CONCLUSION

Qu'il s'agisse de désagrément ou carrément d'abus, les communications non sollicitées ont des répercussions très variées sur les citoyens. Le pollupostage n'est plus un problème qui se limite au courriel. En effet, le pollupostage est devenu un véhicule pour la fraude et a envahi une foule de plateformes électroniques que les citoyens de partout au monde utilisent pour exploiter leurs entreprises, faire leur travail, accéder aux services gouvernementaux, interagir socialement et entretenir des relations. Les acteurs malveillants sont continuellement à l'affût de nouvelles victimes, que ce soit pour leur faire télécharger un maliciel à leur insu ou leur voler des données personnelles. Heureusement, de nombreux gouvernements voient l'urgence d'agir, et des efforts pour lutter contre le pourriel s'organisent à l'échelle de la planète.

Il est crucial que les gouvernements, les organismes de réglementation et d'application de la loi, ainsi que le secteur privé sachent que ces efforts sont déployés et qu'ils y contribuent par leurs connaissances et expertises afin de renforcer les capacités à l'échelle mondiale. Ces milieux doivent miser sur leurs relations entre eux et solliciter de l'aide lorsqu'ils en ont besoin, enrichissant ainsi leurs propres compétences et leur expérience qu'elles pourront, à leur tour, transmettre à d'autres.

Même si chaque milieu a des priorités et des ressources différentes, il faut, pour réussir, continuer à travailler de front sur les plans des politiques, de l'application de la loi, de la technologie et du développement international. Il faut aussi continuer à solliciter la participation des utilisateurs finaux et de la société civile au nom de la prospérité économique et sociale. Échanger l'information, collaborer avec des partenaires, et cultiver un réseau d'alliés et d'homologues, voilà quelques éléments clés pour faire progresser la lutte contre le pourriel à l'échelle du monde.

Les prochaines étapes présentées dans ce rapport se veulent une démarche collective importante afin de renforcer la capacité d'exécution et d'énoncer des politiques souples et rigoureuses pour lutter contre les communications non sollicitées. La participation du secteur privé et la mobilisation des ressources internationales comme UCENet constituent également des piliers pour l'avancement de notre programme commun.

Réunir un groupe d'experts de différents milieux pour discuter pendant un après-midi était un bon point de départ. S'attaquer fondamentalement au problème, aux défis associés aux pourriels et aux communications non sollicitées requiert tout d'abord un dialogue, mais également plus de travail. Les organismes de réglementation, les décideurs politiques, les fournisseurs de services et les organismes d'application de la loi doivent i) améliorer leur capacité à échanger les renseignements, ii) apprendre les uns des autres, et iii) cibler l'objectif commun, qui est de réduire les menaces qui pèsent contre notre système de communications mondial. Le CRTC est impatient de poursuivre ce dialogue avec tous ses partenaires.

ANNEXE A – ORDRE DU JOUR DE L'ATELIER

IIC 2016 – SEMAINE DES POLITIQUES ET DE LA RÉGLEMENTATION EN MATIÈRE DE COMMUNICATIONS

SÉCURITÉ DES COMMUNICATIONS : COLLABORER POUR ÉLIMINER LES POURRIELS ET LES COMMUNICATIONS INDÉSIRABLES

Mot de bienvenue

- **Jean-Pierre Blais**, président et premier dirigeant, CRTC

Allocution d'ouverture : *Comprendre le contexte actuel*

- **Stephen Eckersley**, chef de l'application de la loi, Commissariat à l'information, R.-U.

Panel : *Études de cas transfrontaliers*

Modérateur :
- **Chris Chapman**, président, IIC

Conférenciers :
- **Travis Leblanc**, chef, Bureau de l'application de la loi, Federal Communications Commission, É.-U.
- **Toni Li**, directeur adjoint (soutien), Bureau de l'autorité des communications, Hong Kong (région administrative spéciale)
- **Peter Merrigan**, enquêteur principal, Unité de la conformité des messages électroniques, ministère des Affaires intérieures, Nouvelle Zélande

Pause

Panel : *Combler le vide entre les responsables des politiques et les organismes d'application de la loi*

Modérateur :
- **Steve Unger**, dirigeant principal de la technologie et directeur du groupe de la stratégie, de l'international, des technologies et de l'économie et membre du conseil d'administration, Bureau des communications, R.-U.

Conférenciers :
- **Christine Runnegar**, directrice, Politiques en matière de sécurité et de protection des renseignements personnels, Internet Society
- **Viola Veiderpass**, agente des crimes numériques, Direction des cybercrimes, Complexe mondial INTERPOL pour l'innovation

Mot de la fin : *La voie à suivre?*

- **Jean-Pierre Blais**, président et premier dirigeant, CRTC
- **Adriana Labardini Inzunza**, commissaire, Instituto Federal de Telecomunicaciones, Mexico
- **Richard Bean**, président par intérim, Autorité australienne des communications et des médias

CRTC.GC.CA