

# Groupe de travail sur le pourriel

## Propositions concernant le Centre canadien de lutte contre le pourriel

mai 2005

## **Contexte**

Le Groupe de travail canadien sur le pourriel a adopté une approche de type « boîte à outils » pour lutter contre le pourriel. Cette stratégie multiple comprend l'examen des mesures législatives, l'application plus efficace des lois actuelles, des solutions technologiques, l'éducation et la sensibilisation du public ainsi que la collaboration internationale. Elle préconise une démarche hautement synchronisée et coordonnée en matière de prévention et d'application de la loi. Le Groupe de travail a constaté qu'une communication et une collaboration plus étroites s'imposaient particulièrement dans le domaine de l'application de la loi, car un grand nombre d'organismes d'application et de réglementation partagent la responsabilité de la lutte anti-pourriel.

Les travaux du Groupe de travail ont permis de définir les défis importants suivants :

- l'existence de compétences multiples lors des enquêtes sur le pourriel;
- la disponibilité de l'expertise technique pour la tenue des enquêtes;
- le besoin de ressources adéquates pour lutter contre le pourriel;
- la capacité des exploitants de réseaux et opérateurs techniques de partager l'information;
- la nécessité de disposer de mesures valables pour décrire le problème du pourriel;
- le besoin, pour les Canadiens, de renseignements fiables et exacts afin de se protéger contre le pourriel;
- le besoin, pour les Canadiens, d'un point central et d'un processus simple pour le dépôt des plaintes;
- le besoin de coordination et de collaboration à l'échelle nationale et internationale.

## **Centre canadien de lutte contre le pourriel**

Les points précédents soulèvent la nécessité d'établir un organisme central ou un centre de responsabilité qui coordonnerait la lutte anti-pourriel au Canada. Ce document propose donc l'établissement du Centre canadien de lutte contre le pourriel (CCLP).

Ce centre deviendrait l'instrument principal afin de superviser et de coordonner de façon plus efficace les politiques et de fournir un appui accru aux organismes d'application de la loi.

Pour mener la lutte contre le pourriel, le Centre superviserait et coordonnerait les politiques, notamment :

- en formulant des approches stratégiques concernant le problème du pourriel et les menaces connexes, y compris la supervision et l'analyse des dossiers et la consultation régulière des principaux intervenants;

- en recueillant et en compilant des renseignements et des données statistiques pour mesurer et évaluer l'ampleur du problème du pourriel ainsi que l'efficacité des mesures anti-pourriel, et faire rapport au public, le cas échéant;
- en fournissant au public canadien les renseignements et autres ressources, ainsi que les services de soutien et d'acheminement, dont il a besoin pour se protéger contre le pourriel;
- en encourageant les secteurs public, privé et universitaire à collaborer à la lutte anti-pourriel à l'échelle nationale et internationale.

Le CCLP appuierait également l'application des lois :

- en recevant et en analysant les soumissions et plaintes du public concernant le pourriel et les activités connexes et en aiguillonnant les cas aux organismes d'application de la loi ou de réglementation appropriés;
- en fournissant une expertise technique à l'appui des enquêtes futures et en cours.

Cette proposition présente un concept qui a déjà été formulé ou est en voie d'élaboration dans d'autres pays. Par exemple, l'Association of the German Internet Economy e. V. a coordonné un groupe de travail anti-pourriel en Allemagne, qui a mené à la création du projet pilote Spotsam.

## **Fonction I : Supervision et coordination des politiques**

### **Promouvoir la coordination nationale de la lutte anti-pourriel**

À l'heure actuelle, les ressources nécessaires pour lutter contre le pourriel sont réparties entre plusieurs organismes ayant des mandats divers non strictement associés à la lutte anti-pourriel. Ces divers organismes doivent affecter leurs ressources en fonction de leurs priorités concurrentielles et, comme dans l'état actuel des choses la lutte contre le pourriel n'est pas toujours une priorité, son financement est souvent inadéquat et fragmentaire.

Le CCLP travaillerait étroitement avec tous les organismes gouvernementaux engagés dans des activités anti-pourriel. Il serait en mesure de gérer et de coordonner les ressources affectées à ces initiatives et d'en accroître l'efficacité, en éliminant le double emploi par exemple.

### **Assurer l'éducation et la sensibilisation du public**

L'éducation et la sensibilisation du public figurent parmi les principaux outils de la lutte anti-pourriel. Les Canadiens ont besoin de renseignements exacts pour se protéger contre le pourriel et les activités connexes (comme l'hameçonnage). L'information sur le sujet ne manque pas, particulièrement sur Internet, mais elle est peu cohérente et parfois contradictoire.

Le CCLP occuperait une position unique comme organisme chargé de regrouper l'information sur le pourriel et les activités connexes afin de fournir au public des renseignements et des programmes éducatifs à l'avant garde, exacts et fiables sur le sujet. Ses fonctions en matière

d'éducation et de sensibilisation incluraient des campagnes proactives pour empêcher les Canadiens d'être victimes du pourriel et des activités qui y sont liées. L'approche unique de PhoneBusters à l'égard des communications pourrait servir de modèle pour le CCLP.

## **Promouvoir la collaboration internationale dans la lutte anti-pourriel**

Diverses composantes du pourriel transcendent les frontières. Une collaboration internationale est essentielle pour répondre à ce problème.

Le CCLP jouerait le rôle de centre national de coordination et collaborerait aux enquêtes internationales sur le pourriel. Il établirait également des relations et renforcerait la collaboration générale avec les partenaires internationaux, en participant notamment à des accords internationaux qui encourage la collaboration dans la lutte anti-pourriel, accords engageant des pays et des organismes multilatéraux tels que l'Organisation de coopération et de développement économiques et l'Union internationale des télécommunications.

## **Fonction II : Appui aux organismes de réglementation et d'application de la loi**

### **Recevoir les plaintes**

Divers organismes traitent présentement les plaintes relatives au pourriel. En conséquence, le public et les organismes canadiens ne savent pas précisément où déposer une plainte, certains ignorent qu'ils peuvent le faire, et d'autres présentent leur plainte au mauvais endroit.

Le CCLP serait préparé à recevoir toutes les plaintes. Il pourrait donc mesurer l'ampleur du problème en se basant sur le nombre de plaintes reçues et affecter les ressources analytiques nécessaires, suivant le cas, pour les traiter. Le Canada serait donc doté d'un processus précis pour le dépôt et le traitement des plaintes. Après une analyse correcte (voir la discussion qui suit), ces plaintes seraient acheminées à l'organisme d'application de la loi approprié, au besoin.

### **Maintenir une base de données canadienne sur les pourriels (le « congélateur à pourriels »)**

La Base de données canadienne sur les pourriels servirait d'archivage de copies des pourriels reçus dans les boîtes aux lettres électroniques. Le CCLP inventorierait ces messages et les conserverait pour une période de temps donnée.

Cette base de données canadienne sur les pourriels serait semblable à celles de la Federal Trade Commission et du Anti-Phishing Working Group (APWG) des États-Unis et à la base de données sur les plaintes concernant le télémarketing de PhoneBusters.

La Base de données canadienne sur les pourriels recevrait et emmagasinerait systématiquement les pourriels volontairement soumis par les Canadiens. Elle offrirait aux victimes canadiennes un

mécanisme de déclaration fiable et efficace qui faciliterait l'application des lois canadiennes appropriées aux infractions liées au pourriel et au multipostage abusif.

La Base de données servirait également de ressource aux organismes chargés de prévenir les effets du pourriel, de poursuivre les responsables ou d'obtenir des réparations appropriées pour les torts causés par le pourriel et autres types d'abus du courriel connexes au pourriel. Cette ressource serait mise à la disposition des organismes d'application de la loi, des fournisseurs de service Internet, des organismes de recherche et autres organismes pertinents, notamment d'Industrie Canada. Les renseignements sur le pourriel affectant les Canadiens, envoyé par les Canadiens ou générant des bénéfices pour les Canadiens pourraient servir de preuve à des fins de poursuite légale, d'analyse statistique et d'élaboration des politiques gouvernementales.

### **Fournir une expertise en matière technique, analytique et d'enquête**

À l'heure actuelle, il faut posséder une expertise judiciaire technique solide pour enquêter sur une plainte grave relative au pourriel. La responsabilité des enquêtes sur ce genre de plainte peut relever de divers organismes, notamment le Bureau de la concurrence, le Commissariat à la protection de la vie privée du Canada, la Gendarmerie royale du Canada (GRC) ou même les autorités policières locales. Or, il est devenu évident que certains de ces organismes ne possèdent pas l'expertise technique et spécialisée requise pour mener les enquêtes.

Le CCLP emploierait des experts techniques capables de composer avec la nature complexe des plaintes et des enquêtes liées au pourriel. Ainsi, le problème du manque d'expertise technique serait réglé, et il ne serait pas nécessaire d'assurer la présence d'experts au sein de tous les organismes concernés, ce qui réduirait considérablement les coûts.

Le Centre contribuerait aux enquêtes en recevant les plaintes et en emmagasinant les éléments de preuve, tel que décrit. Ses experts techniques internes mèneraient des enquêtes préliminaires et achemineraient les plaintes, accompagnées de leurs analyses préliminaires, aux organismes d'application de la loi appropriés.

Le CCLP pourrait également fournir des données en temps réel sur les tendances courantes du pourriel, afin d'appuyer les démarches en temps réel visant à contrer les menaces sérieuses, telles les attaques par hameçonnage.

### **Faciliter le partage de renseignements sur le multipostage abusif**

Les renseignements exacts et en temps voulu sont essentiels à la lutte anti-pourriel. Il importe donc que les principaux intervenants communiquent ensemble et, en particulier, que les exploitants de réseaux recueillent et partagent leurs données sur les polluposteurs qui encombrant leurs réseaux.

Le CCLP servirait de centre d'échange de renseignements entre les représentants du secteur privé, notamment les exploitants de réseaux et autres intervenants pertinents. Cet échange pourrait empêcher la prolifération des polluposteurs sur les réseaux canadiens.

## Organisation du Centre

Il y a différentes options pour l'organisation du CCLP. On pourrait créer un nouvel organisme, mais un centre relevant d'un organisme existant présenterait plusieurs avantages, notamment des coûts moins élevés.

Une première option consisterait à créer un nouveau partenariat public-privé ou à conférer les responsabilités à un organisme privé tierce partie. PhoneBusters est un exemple de ce modèle. Un tel partenariat risquerait toutefois de ne pas répondre à toutes les exigences du double mandat du CCLP, à savoir la supervision et la coordination des politiques et la fourniture d'un appui aux organismes d'application de la loi – en particulier la première partie du mandat.

Une deuxième option consisterait à affecter les responsabilités du Centre à un organisme de réglementation existant. Le Bureau de la concurrence, par exemple, joue un rôle significatif dans la lutte anti-pourriel. Toutefois, il s'occupe uniquement de certaines variétés d'infractions liées au pourriel, particulièrement celles portant sur le contenu fallacieux, et n'a pas le mandat de poursuivre les polluposteurs qui portent atteinte à la vie privée. Le Commissariat à la protection de la vie privée du Canada et le Conseil de la radiodiffusion et des télécommunications canadiennes sont d'autres organismes à envisager. Le choix d'un organisme réglementaire existant est compliqué, car il y a un grand nombre d'organismes d'application de la loi et de réglementation qui partagent la responsabilité de la lutte anti-pourriel.

Une troisième option consisterait à établir le Centre au sein d'un ministère du gouvernement fédéral. À cet égard, Industrie Canada serait un centre décisionnel idéal pour la lutte anti-pourriel au Canada.

# Appendice

## Sommaire des modèles existants

### PhoneBusters

Établi en janvier 1993, PhoneBusters est un centre d'appel anti-fraude national exploité conjointement par la Police provinciale de l'Ontario, la GRC et le Bureau de la concurrence. PhoneBusters joue un rôle important de sensibilisation du public aux techniques précises de la fraude par télémarketing. De plus, il recueille et diffuse les déclarations des victimes, les statistiques, la documentation et les enregistrements sur cassette, qui sont mis à la disposition des autres organismes d'application de la loi.

À l'origine, PhoneBusters avait pour mandat de poursuivre les individus engagés dans la fraude par télémarketing, au Québec et en Ontario, en vertu du *Code criminel* du Canada. Son mandat a été élargi, et il facilite maintenant les poursuites des organismes américains au moyen de l'extradition, et du Bureau de la concurrence en vertu de la *Loi sur la concurrence*.

PhoneBusters est l'organisme central canadien chargé de recueillir les renseignements sur le télémarketing, les lettres de fraude exigeant des frais à l'avance (lettres de fraude de l'Afrique de l'Ouest) et les plaintes concernant l'usurpation d'identité. Une de ses fonctions principales consiste à recueillir et à analyser les renseignements et les éléments probants, puis à les remettre aux organismes d'application de la loi aux fins d'enquête. Les données recueillies par l'organisme permettent d'évaluer les retombées des divers types de fraude pour le public. Elles contribuent également à la prévention d'actes criminels semblables. Une des priorités de PhoneBusters, qui reçoit un financement partiel du secteur privé, est d'éduquer et de sensibiliser le public.

### Centre national de coordination contre l'exploitation des enfants

Le Centre national de coordination contre l'exploitation des enfants (CNCEE), faisant partie des services nationaux de police, a été créé pour protéger les enfants contre l'exploitation sexuelle en ligne.

Le CNCEE est un centre d'information et de coordination national qui accueille les demandes d'enquête en provenance de l'étranger sur l'exploitation sexuelle des enfants dans Internet. Il fournit un soutien aux agents de la paix, en particulier aux enquêteurs mis à contribution dans les dossiers portant sur l'exploitation sexuelle des enfants dans Internet. Il établit des relations et collabore avec des partenaires nationaux et internationaux afin de sensibiliser le public aux activités criminelles visant à cibler, à exploiter et à abuser des enfants. De plus, il contribue à l'élaboration de normes et de lignes directrices au Canada et offre divers niveaux de soutien aux enquêteurs de police affectés aux dossiers portant sur l'exploitation sexuelle des enfants sur Internet.

### Cyberaide.ca

Cyberaide.ca est le site national de dénonciation de l'exploitation sexuelle des enfants sur Internet. Il s'agit d'un portail Web centralisé qui reçoit et achemine les rapports du public concernant les cas de pornographie infantile, de leurre, de tourisme sexuel mettant en cause des

enfants et d'exploitation des enfants au moyen de la prostitution infantile. Cyberaide.ca fournit également aux Canadiens des renseignements, des services d'acheminement et autres ressources pour les aider à assurer la sécurité de leurs enfants sur Internet.

En tant que site national canadien de dénonciation, Cyberaide.ca a pour mandat de protéger les enfants contre l'exploitation sexuelle sur Internet. Il s'acquitte de son mandat en recevant et en analysant les renseignements du public sur le matériel et les activités potentiellement illicites se rapportant à l'exploitation sexuelle des enfants sur Internet, et en acheminant les renseignements aux organismes d'application de la loi appropriés. En outre, il fournit au public des renseignements et d'autres ressources, ainsi que des services de soutien et d'acheminement, pour aider les Canadiens à assurer leur sécurité et celle de leur famille sur Internet.

### **Signalement en direct des délits économiques**

Le Signalement en direct des délits économiques (Centre RECOL) est une initiative qui fait appel à un partenariat intégré entre des organismes d'application de la loi internationaux, fédéraux et provinciaux ainsi qu'à des organismes de réglementation et à des organisations commerciales privées qui s'intéressent de façon légitime aux enquêtes en recevant une copie des plaintes relatives à des délits économiques.

Le consentement contrôlé par l'utilisateur est requis pour acheminer les plaintes relatives à des fraudes vers les organismes de réglementation et les services de police appropriés. Le Centre RECOL recommande des enquêtes possibles aux organismes d'application de la loi et de réglementation ou aux organisations commerciales privées.

Le Centre RECOL fournit des données en temps réel sur les tendances actuelles en matière de fraude. Il soutient également l'éducation, la prévention et la sensibilisation relatives à la délinquance économique.

La confidentialité de toutes les données entrées par un utilisateur est protégée, et les données ne peuvent être contrôlées que par l'utilisateur qui les a entrées en déposant une première plainte. Tous les membres qui participent à l'initiative du Centre RECOL assureront une supervision afin de garantir qu'on protège la confidentialité du contenu et qu'on utilise les renseignements uniquement pour faciliter les enquêtes sur des plaintes relatives à des délits économiques.

Ce service est administré par le Centre national des crimes économiques du Canada et bénéficie du soutien de la GRC et d'autres organismes participants.

### **Operation Slam Spam aux États-Unis**

Operation Slam Spam est le fruit d'une collaboration entre la Direct Marketing Association (DMA) et le Federal Bureau of Investigation (FBI). La DMA affecte des fonds et des services de renseignements pour aider le FBI à identifier les polluposteurs et à les poursuivre au criminel.

Operation Slam Spam a permis d'identifier plus de 100 polluposteurs importants. En outre, l'initiative a :

- ciblé 50 polluposteurs comme centres d'intérêt pour le projet;
- préparé 10 paquets de données sur les principaux sujets aux fins d'acheminement aux organismes d'application de la loi;
- relié 3 groupes de sujets à des entreprises éventuellement liées au crime organisé;
- recommandé 5 vastes enquêtes sur des polluposteurs;
- cerné plus de 350 ressources compromises, y compris 50 sites gouvernementaux;
- embauché des enquêteurs criminels militaires pour l'aider à identifier les actes criminels associés aux sites gouvernementaux compromis;
- établi un catalogue des techniques utilisées par les polluposteurs, notamment la collecte d'adresses de courriel, l'utilisation des virus et l'usage des outils « clés en main » (*turnkey*) servant à contourner les filtres.

### **Anti-Phishing Working Group aux États-Unis**

L'APWG est un organisme américain voué à l'élimination de l'escroquerie et de la fraude sur Internet.

Les attaques par hameçonnage recourent à l'ingénierie sociale et à des subterfuges techniques pour usurper les données personnelles et les justificatifs des comptes financiers des consommateurs. Les stratagèmes fondés sur l'ingénierie sociale utilisent le courriel trompeur pour diriger les consommateurs à des sites Web contrefaits conçus pour les inciter à divulguer des données personnelles et financières, notamment les numéros de cartes de crédit, les noms d'utilisateur de compte, les mots de passe et les numéros d'assurance sociale.

Usurpant les noms de marque des banques, des commerçants électroniques et des compagnies de cartes de crédit, les hameçonneurs arrivent souvent à convaincre les destinataires de répondre. Les stratagèmes techniques consistent à insérer des logiciels criminels dans les ordinateurs personnels afin de voler les justificatifs directement. On utilise souvent le logiciel de supervision des touches Trojan (*Trojan keylogger spyware*) à cette fin. Les logiciels criminels de réorientation (*pharming crimeware*) acheminent les utilisateurs vers des sites frauduleux ou des serveurs mandataires en ayant recours au détournement ou à l'empoisonnement de DNS.

Le public peut signaler les courriels hameçons, les sites de réorientation et les logiciels espions malveillants au site Web de l'APWG afin de freiner ces menaces aux systèmes de paiement et à l'infrastructure du commerce électronique. Le site Web donne également accès aux ressources anti-hameçonnage, notamment aux conseils des consommateurs sur l'hameçonnage.