Criminologie

La régulation du cybercrime comme alternative à la judiciarisation

Le cas des botnets

Benoît Dupont

Volume 47, Number 2, Fall 2014

Criminalité et police transnationales : une perspective critique

URI: https://id.erudit.org/iderudit/1026733ar
DOI: https://doi.org/10.7202/1026733ar

See table of contents

Publisher(s)

Les Presses de l'Université de Montréal

ISSN

0316-0041 (print)
1492-1367 (digital)

Explore this journal

Cite this article

Dupont, B. (2014). La régulation du cybercrime comme alternative à la judiciarisation : le cas des botnets. *Criminologie*, *47*(2), 179–201. https://doi.org/10.7202/1026733ar

Article abstract

Botnets, which are computers controlled by malicious hackers, currently represent the most serious threat to the digital ecosystem, providing the infrastructure to commit bank fraud, distributed denial of service attacks (DDoS), or click fraud. During the past few years, two main approaches have been used to fight botnets : First, police organizations have arrested high profile hackers and dismantled their command and control systems. Second, some countries, more precisely Japan, South Korea, Australia, the Netherlands and Germany have encouraged public-private partnerships involving Internet service providers and anti-virus companies. Inspired by regulatory principles, these initiatives seek to identify infected computers, notify their owners and help them clean their machines. This article compares these two approaches (criminalization vs. regulation) by trying to establish their respective effectiveness with respect to securing the digital ecosystem.

La régulation du cybercrime comme alternative à la judiciarisation

Le cas des botnets

Benoît Dupont[1, 2]
Directeur
Centre international de criminologie comparée (CICC)
Université de Montréal
benoit.dupont@umontreal.ca

RÉSUMÉ • *Les botnets, ou réseaux d'ordinateurs compromis par des pirates informatiques, représentent à l'heure actuelle la menace criminelle la plus sérieuse, servant de support à la fraude bancaire, aux attaques distribuées par déni de service (DDoS), ou encore à la fraude au clic. Au cours des dernières années, deux approches distinctes ont été privilégiées pour combattre ces botnets : d'une part, les services de police ont procédé à l'arrestation fortement médiatisée de quelques pirates de haut vol et au démantèlement de leurs infrastructures de commandement et de contrôle. D'autre part, dans certains pays, et notamment au Japon, en Corée du Sud, en Australie, mais aussi en Hollande ou en Allemagne, les gouvernements ont favorisé l'émergence de partenariats public-privé impliquant des fournisseurs d'accès et des entreprises de sécurité informatique. Dans une démarche régulatoire, ces initiatives visent à identifier les ordinateurs infectés, à notifier leurs propriétaires et à aider ces derniers à nettoyer leur machine. Cet article a donc pour objectif de comparer les deux approches (judiciarisation vs régulation), en essayant notamment d'évaluer les effets produits par chacune d'elles sur le niveau général de sécurité de l'écosystème numérique.*

MOTS-CLÉS • *Cybercrime, botnets, judiciarisation, régulation, prévention.*

---

1. Université de Montréal, École de criminologie, Pavillon Lionel-Groulx, C. P. 6128, succursale Centre-ville, Montréal (Québec), Canada, H3C 3J7.

2. L'auteur désire particulièrement remercier Sécurité publique Canada, dont la subvention n° 7181358 a rendu cette étude possible, ainsi que Bruce Matthews, de l'Australian Communication and Media Authority, pour ses précieux commentaires sur une version antérieure de cet article.

Introduction

Des formes de délinquance se déployant à l'échelle transnationale, la cybercriminalité représente certainement le mode de soustraction le plus abouti aux contraintes imposées par les frontières administratives des États. En effet, Internet repose sur une infrastructure technologique décentralisée et mondialisée qui permet de délocaliser les activités illégales vers les juridictions où les contrôles policiers sont moins contraignants, voire totalement défaillants, tout en conservant un accès privilégié à un réservoir potentiellement illimité de victimes ou de consommateurs de produits ou de services illicites. Cette difficulté à contrôler les activités délinquantes menées sur Internet n'empêche pas la mise en œuvre de capacités de surveillance extrêmement sophistiquées, comme les récentes révélations d'Edward Snowden durant l'été 2013 l'ont amplement démontré[3], mais ces investissements massifs sont pour l'instant réservés aux agences de renseignement et restent hors de portée des organisations policières.

Pourtant, la cybercriminalité a connu ces dernières années une croissance vertigineuse, à contre-courant des réductions de la délinquance observées dans la plupart des sociétés occidentales (Aebi & Linde, 2010 ; Farrell, Tseloni, Mailley & Tilley, 2011 ; Ouimet, 2002). Les estimations les plus délirantes concernant l'ampleur des coûts associés à celle-ci, ainsi que des profits accumulés par ceux qui s'y livrent, évoquent fréquemment des montants proches de 1000 milliards de dollars (Maass & Rajagopalan, 2012) ou établissent des parallèles invérifiables avec les profits générés par le trafic de stupéfiants (Symantec, 2009). Plus récemment, une équipe multidisciplinaire de chercheurs anglais a proposé avec beaucoup de circonspection le chiffre plus réaliste de 67,5 milliards de dollars, extrapolé de manière conservatrice à partir de données nationales et internationales et en tenant compte des coûts directs et indirects, comme l'acquisition de systèmes de protection (Anderson *et al.*, 2012). Au Canada, l'analyse des résultats de la dernière enquête de victimisation, menée en 2009, laisse penser que la cybercriminalité représente environ 29,5 % des crimes contre la propriété (Perreault, 2011 ; Perreault & Brennan, 2010). La majorité de ces incidents n'est jamais déclarée à la police, qui ne dispose de toute

3. Pour une compilation des révélations faites par le *Guardian* sur le sujet, voir www.theguardian.com/world/the-nsa-files

manière que de ressources spécialisées fort limitées pour faire face à cette délinquance technologique transnationale.

Pourtant, cette pénurie de moyens n'empêche pas les organisations policières de mener avec succès des enquêtes qui laissent entrevoir de manière anecdotique la dimension transnationale inhérente à la cybercriminalité. Ainsi, un réseau de dix pirates informatiques démantelé en février 2008 par la Sûreté du Québec avait réussi à prendre le contrôle de plus de 630 000 ordinateurs localisés dans plus de 70 pays (Décary-Hétu & Dupont, 2012 ; Dupont, 2013a). La même année, le *Secret Service* américain arrêtait Albert Gonzalez et quatre complices, responsables du vol de plus de 170 millions de numéros de carte de crédit revendus en ligne sur des forums clandestins, établissant des liens avec des pirates et des fraudeurs notoirement connus établis en Allemagne, en Biélorussie, en Chine et en Estonie (Dupont, 2010). La plupart de ces affaires fortement médiatisées impliquent la création, la gestion ou l'utilisation de « botnets » par les individus arrêtés. Un botnet est un ensemble de machines informatiques contrôlées à l'insu de leur propriétaire légitime par un pirate informatique qui les utilise de manière coordonnée. Les botnets représentent actuellement l'infrastructure privilégiée permettant à la cybercriminalité de se développer à grande échelle et d'industrialiser ses processus.

Mais relativement à l'approche judiciaire traditionnelle qui consiste à identifier, neutraliser et punir quelques pirates trop téméraires, une seconde stratégie reposant sur des modes de régulation polycentriques ou nodaux (Drahos, Shearing & Burris, 2005 ; Shearing & Wood, 2003) semble se dessiner dans un certain nombre de pays dont l'écosystème numérique florissant est menacé par les botnets. Par contraste avec l'approche punitive d'un système judiciaire mal adapté à cette forme complexe de délinquance transnationale, l'approche régulatoire repose sur des partenariats entre acteurs publics et privés destinés à renforcer la résilience de l'écosystème et à aider les victimes infectées à restaurer l'intégrité de leur équipement informatique. Ce mode de gestion atypique de la délinquance transnationale apporte une réponse originale aux méga-crimes non violents (Leman-Langlois, 2003), dont les caractéristiques (fort volume mais faible impact) sont incompatibles avec un système de justice pénale conçu pour traiter un faible volume de crimes à fort impact comme les atteintes à l'intégrité physique des personnes.

Après avoir présenté de manière plus détaillée les caractéristiques et utilisations possibles des botnets dans une première section, on se penchera ensuite sur l'efficacité toute relative des interventions policières pour combattre cette forme de délinquance transnationale. La troisième partie de cet article sera consacrée à l'analyse de six initiatives nationales de lutte anti-botnet, avant d'introduire dans une quatrième et dernière section une discussion sur la place susceptible d'être occupée par les institutions policières dans ces réseaux transnationaux de sécurité.

Les botnets : nouvelle infrastructure du cybercrime

Les botnets sont habituellement définis comme des réseaux constitués d'ordinateurs infectés par un logiciel malveillant (les « bots », abréviation de robots) permettant à un délinquant, aussi connu sous le nom de « botmaster », de contrôler simultanément plusieurs milliers, voire millions de machines (Abu Rajab, Zarfoss, Monrose & Terzis, 2006, p. 42). L'architecture des botnets a été caractérisée comme un « service militaire obligatoire auquel seraient assujetis les ordinateurs Windows » (Stromberg cité dans Zarfoss, 2007, p. 11), même si de nombreux botnets exploitant les systèmes Mac OS d'Apple (tels que PintSized ou Flashback) et Android de Google (par exemple MisoSMS ou Sandroid) ont été découverts depuis.

La construction d'un botnet se décompose en cinq phases principales. Le botmaster doit dans un premier temps élaborer un logiciel malveillant qui disposera de fonctions permettant des communications furtives (c'est-à-dire indétectables à l'œil nu par un utilisateur lambda) avec les machines infectées. Ces communications devront être bidirectionnelles, afin de transmettre à ses « zombies » (un autre terme utilisé pour désigner les bots) des instructions variées, mais aussi pour que ces derniers puissent rendre compte en retour de leur état de fonctionnement. Il devra également intégrer à ce logiciel la capacité d'extraire les informations variées détenues par les machines infectées, qu'il s'agisse de documents, de courriels, ou de mots de passe utilisés par leurs propriétaires pour accéder à des comptes bancaires ou à d'autres services en ligne. Si le botmaster ne dispose pas des compétences suffisantes en programmation, il pourra se procurer sur les forums clandestins consacrés au piratage et à la fraude une application déjà fonctionnelle, dont le tarif variera en fonction des performances et du soutien technique

offert par ses concepteurs. Ainsi, l'application malveillante ZeuS, spécifiquement conçue afin d'élaborer des botnets ciblant en priorité les informations financières se détaillait en mars 2010 entre 3 000 et 19 000 $, selon les options sélectionnées par l'acheteur (Stevens & Jackson, 2010). L'une de ces options consiste en un module capable de désinstaller des machines infectées des logiciels malveillants concurrents détectés par ZeuS, afin que le pirate dispose d'un monopole sur leur contrôle et puisse ainsi mieux rentabiliser l'exploitation de ces ordinateurs.

À la deuxième étape, le pirate doit injecter le logiciel malveillant dans un nombre aussi élevé que possible de machines. Plusieurs stratégies s'offrent à lui : il peut procéder à une campagne plus ou moins large d'hameçonnage (ou *phishing*), expédiant des millions de courriels invitant leurs destinataires à cliquer sur un lien sous de faux prétextes (comme modifier le mot de passe de divers comptes en ligne) généralement associés à un sentiment d'urgence. Il peut également placer son code malveillant sur des sites Internet légitimes mais mal protégés qui infecteront à leur insu leurs usagers, comme ce fut le cas de la page en ligne du New York Times en septembre 2009. Dans la logique de crime par sous-traitance déjà esquissée plus haut, il pourra enfin confier à des courtiers spécialisés le mandat d'installer son application sur des machines déjà compromises ou vierges, rémunérant ces intermédiaires selon le volume d'infections réalisées et la distribution géographique des ordinateurs contaminés (Goncharov, 2012). La troisième étape est celle de la prise de contrôle des machines infectées et leur intégration à l'infrastructure de commandement du pirate. En effet, en raison de la taille des botnets, qui réunissent souvent plusieurs dizaines de milliers d'ordinateurs – voire plus –, des protocoles spécifiques de communication permettant une coordination et une distribution des tâches doivent être mis en œuvre, les pirates ne pouvant se permettre une gestion individualisée des machines de leurs victimes. Les botmasters transmettent leurs instructions aux zombies par le biais de serveurs dédiés connus sous le nom de serveurs C&C (pour commandement et contrôle) ou par le biais de canaux de clavardage en ligne auxquels les bots se connectent à intervalles réguliers. À ce stade, le défi pour les botmasters consiste à réussir la prise de contrôle sans se faire détecter par les victimes ou leurs fournisseurs d'accès à Internet (les FAI), ce qui entraînerait la mise en œuvre de mesures correctrices et la perte d'une machine potentiellement profitable. Afin de maintenir la furtivité des

communications avec leurs bots, les botmasters les plus avancés techniquement mettent en œuvre des solutions de chiffrement.

La quatrième étape est celle de l'exploitation, où tous les efforts consentis par les pirates portent leurs fruits et se traduisent par l'extraction d'un profit financier ou d'avantages sous une autre forme, comme la neutralisation d'un adversaire. Il existe cinq principales modalités de monétisation des botnets (Namestnikov, 2009), mais cette classification n'est probablement pas exhaustive, la créativité des pirates informatiques étant virtuellement sans limites. Les botnets représentent ainsi des outils particulièrement bien adaptés aux attaques par déni de service distribué (les DDoS), à l'envoi de pourriels (ou *spams*), à la fraude bancaire, à la fraude au clic et à la commercialisation de services de proxy clandestins. Les attaques par déni de service distribué exploitent la taille considérable des botnets pour saturer les serveurs des organisations ciblées de demandes et rendre ces derniers indisponibles aux utilisateurs légitimes. Ces attaques peuvent être commanditées pour des raisons idéologiques, mais aussi pour perturber les activités commerciales de concurrents ou exercer un chantage contre des entreprises dont la profitabilité est immédiatement érodée par ce type d'action, comme les casinos en ligne par exemple. En 2012, la location auprès de pirates russes d'un botnet dédié aux DDoS coûtait de 30 à 70 dollars par heure, avec des tarifs dégressifs pouvant aller jusqu'à des rabais de 1 700 % pour une location d'un mois (Goncharov, 2012, p. 8). L'envoi massif de pourriels constitue la deuxième source de profit potentielle pour les botmasters. Le recours aux botnets permet de multiplier les sources légitimes de courriels indésirables et de déjouer ainsi les filtres et les listes d'exclusion mis en place par les administrateurs de réseaux. À titre d'illustration, le botnet Grum, qui fut démantelé en juillet 2012, expédiait chaque jour 18 milliards de pourriels depuis 120 000 ordinateurs infectés (Krebs, 2012a), ce qui procura à son botmaster (qui se faisait appeler GeRa) 2,7 millions de dollars de commissions sur la vente de 80.000 produits pharmaceutiques contrefaits sur une période de trois ans (Krebs, 2012b). Une autre étude menée la même année sur l'économie du pourriel identifiait des profits similaires (1,9 million de dollars annuels en commissions) pour les trois opérateurs du botnet Rustock (McCoy *et al.,* 2012, p. 12). Les procédés liés à la fraude bancaire exploitent quant à eux la dimension furtive des botnets pour s'emparer des informations personnelles (identifiants et mots de passe) stockées sur les disques durs des machines compromises, permettant aux pirates

de les exploiter directement en vidant les comptes de leurs victimes par le biais de transferts non autorisés ou en revendant ces informations sur des forums spécialisés. Certains botnets spécialisés dans ce type de fraude (comme ZeuS ou SpyEye) peuvent également injecter des informations trompeuses dans les pages Internet des banques consultées par les victimes afin de pousser ces dernières à communiquer des informations financières additionnelles, comme leur numéro de carte de crédit et le code secret de celle-ci (Trusteer, 2009, p. 2). La fraude au clic, bien que moins connue que la fraude bancaire, n'en est pas moins tout aussi lucrative. Cette forme de fraude exploite le modèle publicitaire dominant sur Internet, par lequel les annonceurs rémunèrent les sites qui diffusent leurs messages chaque fois qu'un internaute clique sur leur bannière, par opposition au modèle classique de la presse écrite ou des médias audiovisuels où les tarifs sont fixés en fonction d'une audience globale. Le marché de la publicité en ligne représentait en 2012 des dépenses 94,2 milliards de dollars (GO-Gulf, 2012). Les fraudeurs utilisent ici les botnets pour cliquer de manière automatisée et répétée sur des liens publicitaires placés sur des sites complices, qui recevront ainsi des revenus publicitaires indus versés par les annonceurs via les régies spécialisées gérées par Google, Yahoo ou Microsoft (Vratonjic, Manshaei, Raya & Hubaux, 2010). Le botnet ZeroAccess, qui contrôlerait environ un million de machines infectées, générerait ainsi par la fraude au clic des revenus mensuels de plus de 2,7 millions de dollars, en prenant comme élément de référence une rémunération de 1 cent par clic (Wyke, 2012, p. 45). Finalement, les pirates peuvent commercialiser l'accès aux machines sous leur contrôle en les louant à des utilisateurs qui cherchent à dissimuler leurs activités ou des contenus illégaux comme des images de pornographie juvénile. Ces services de proxy illégaux utilisent les ordinateurs des victimes comme moyen d'éluder la surveillance policière (Choo, 2007).

La cinquième et dernière phase peut se définir comme le maintien de l'emprise du botmaster sur son réseau de machines. Cela implique pour ce dernier une veille constante afin de s'assurer que son code malveillant reste indétectable par les principaux logiciels d'antivirus disponibles sur le marché, que les procédures mises en place pour désactiver ces logiciels ou empêcher leur mise à jour régulière demeurent efficaces, ou encore que les serveurs C&C n'aient pas été publiquement répertoriés par des chercheurs en sécurité (à l'instar des informations

disponibles sur le site zeustracker.abuse.ch par exemple), ce qui éroderait l'efficacité de son botnet et, conséquemment, ses profits.

Il demeure excessivement difficile d'obtenir des chiffres fiables sur la prévalence et les préjudices causés par les botnets à l'échelle nationale ou internationale. Toutefois, dans une étude réalisée en Hollande, van Eeten et ses collaborateurs (2011) évaluent le taux d'infection par botnet dans les pays développés à une fourchette comprise entre cinq et dix pour cent du parc informatique, ce qui permet à Anderson et ses collègues (2012, p. 24) d'évaluer le montant des coûts mondiaux associés à la prévention de cette forme de délinquance à 24,8 milliards de dollars, dont la majeure partie (20 milliards) sert à désinfecter ou protéger les machines menacées.

L'insuffisance de la réponse judiciaire : le syndrome de Sisyphe

Dans la mythologie grecque, Sisyphe symbolise l'absurdité d'un travail inutile et sans espoir (Camus, 1942, p. 162). Fils d'Éole réputé pour sa ruse et sa duplicité, Sisyphe s'attira la foudre des dieux par son refus de mourir et ses multiples manœuvres pour retourner dans le monde des vivants. La punition que lui imposa Zeus (le dieu, pas le botnet) fut alors de pousser éternellement jusqu'en haut d'une montagne un lourd rocher dont le poids l'écrasait avant d'atteindre le sommet, l'obligeant à reprendre sans fin ses efforts depuis la base de l'escarpement (Homère, 1766 : chant 11). Même si Camus est convaincu que la futilité de son destin n'empêche pas Sisyphe d'être heureux, cette parabole sur l'impuissance, qu'aucun effort ne permet de surmonter, reflète assez bien l'état actuel de la répression policière contre les botmasters.

Les organisations policières peuvent sans aucun doute se prévaloir ces dernières années de quelques opérations fortement médiatisées de démantèlement de botnets, aussi bien au Canada qu'aux États-Unis ou en Europe. Outre l'opération Basique, déjà mentionnée dans l'introduction, on peut citer l'arrestation par le FBI en décembre 2012 de dix individus suspectés d'être à l'origine du botnet Butterfly, qui aurait réussi à infecter plus de onze millions de machines (Federal Bureau of Investigation [FBI], 2012), celle d'un citoyen russe par la police arménienne en octobre 2010, à la demande de la police hollandaise, cette dernière ayant saisi quelques jours plut tôt les 143 serveurs C&C du botnet Bredolab, qui aurait asservi 30 millions d'ordinateurs (de Graaf,

Shosha & Gladyshev, 2012), ou l'opération massive menée par 19 pays à la demande de la justice américaine en mai 2014 et ayant conduit à l'arrestation de plus de 90 personnes (dont 26 en France) impliquées dans la conception ou l'utilisation du logiciel malveillant Blackshades (Eudes & Seelow, 2014). Dans les deux derniers cas, le conditionnel est utilisé en raison des difficultés inhérentes associées à la mesure de la taille des botnets (Abu Rajab, Zarfoss, Monrose & Terzis, 2007 ; van Eeten *et al.*, 2011), ce qui conduit parfois les enquêteurs à surévaluer l'importance de leurs interventions.

Mais si le pirate qui contrôlait Bredolab fut ultimement condamné par la police arménienne à quatre années de prison (Cluley, 2012), c'est la pérennité des effets obtenus qui doit être interrogée. En effet, deux jours seulement après la saisie des serveurs, Bredolab reprenait ses activités de distribution de pourriels et de contenus malveillants à partir de serveurs basés en Russie, et semblait particulièrement cibler des victimes espagnoles (Vicario, 2010). Cette résilience du botnet s'explique notamment par le fait que son infrastructure de base (les millions de machines infectées) a été laissée intacte par la police, et qu'il suffit de quelques heures à des pirates opportunistes pour en reprendre le contrôle une fois son concepteur placé derrière les barreaux. Par ailleurs, la propension des pirates à établir des serveurs C&C redondants dans une multitude de pays complique considérablement la tâche des enquêteurs, puisque la survie d'un seul d'entre eux suffit à maintenir le contrôle sur l'ensemble du botnet. Ainsi, dans le cas de l'opération Butterfly, le FBI collabora avec les polices bosniaque, croate, macédonienne, néo-zélandaise, péruvienne et britannique, ce qui impliqua des efforts de coordination importants de la part des enquêteurs et des ressources hors de portée de la plupart des services de police occidentaux – et *a fortiori* de leurs homologues des pays émergents, pour qui les botnets sont loin d'être une priorité.

Outre la résilience des botnets face aux interventions policières, la mise en œuvre par les botmasters les plus sophistiqués des techniques de camouflage décrites plus haut, comme le chiffrement des communications ou la modification constante des signatures laissées par leur code informatique afin d'échapper à la détection des logiciels antivirus, implique pour certains observateurs qu'à de rares exceptions près, ce sont probablement des pirates informatiques débutants ou de niveau intermédiaire qui se retrouvent devant les tribunaux (Maurushat, 2012). Ce constat a été partiellement confirmé dans le cas de l'affaire Basique,

où en dépit du préjudice technique bien réel résultant d'un nombre élevé d'infections, seul un des dix accusés semblait disposer de compétences techniques avancées et aucun d'entre eux ne fut en mesure de profiter financièrement de ses bots (Dupont, 2013a). De surcroît, les peines prononcées par les tribunaux dans ce type d'affaires restent en règle générale relativement clémentes, ce qui se justifie par la jeunesse des accusés, le fait qu'il s'agit souvent pour eux d'une première infraction, qu'ils n'ont pas eu recours à la violence et que leur potentiel de réinsertion professionnelle et sociale est élevé dans l'économie numérique contemporaine (Smith, Grabosky & Urbas, 2004). Enfin, et c'est là un point déterminant, le système pénal semble bien mal équipé pour requérir la mise en œuvre de stratégies de notification et de désinfection concernant les milliers, voire les millions, d'ordinateurs affectés à l'échelle mondiale. Si les responsables sont donc parfois sanctionnés, leurs victimes restent quant à elles vulnérables du fait de l'incapacité des institutions policières et judiciaires à adapter leurs modalités d'intervention à des crimes dont le volume est extrêmement élevé, mais dont l'impact pour chaque incident reste limité (par comparaison avec des crimes contre la personne par exemple).

Si la judiciarisation – et son regard tourné vers le passé – s'avère assez mal adaptée aux propriétés de cette délinquance numérique, la régulation, qui s'attache plutôt à changer le futur en modifiant les paramètres économiques et sociaux de son émergence, semble plus prometteuse. Plus fréquemment mobilisée par les juristes, les économistes, les politologues, voire les sociologues, la régulation (en tant qu'activité ou instrument et non comme domaine d'étude) se définit comme « toute tentative prolongée et ciblée d'altérer les comportements selon des critères et des objectifs définis et afin de produire les résultats espérés, impliquant le recours à des mécanismes d'établissement des normes, de collecte de l'information et de modification des comportements » (Black, 2002, p. 27). Loin d'être restreinte aux modalités contraignantes par lesquelles l'État fait appliquer ses décisions, la notion de régulation porte au contraire en elle l'ambition d'analyser la multiplicité des mécanismes et des institutions qui permettent de contrôler de manière indirecte certains secteurs de l'activité humaine (Baldwin, Cave & Lodge, 2010 ; Grabosky, 2012). Elle relève en ce sens plus de la persuasion que de la dissuasion, même si la légitimité et la nécessité d'une escalade vers des mesures punitives en cas d'échec des

approches partenariales restent au cœur de ses préoccupations (Ayres & Braithwaite, 1992).

La régulation en réseau des botnets : six initiatives nationales

Six pays se sont dotés au cours des dix dernières années de stratégies anti-botnets reposant sur une approche régulatoire : l'Australie, la Corée du Sud, le Japon, l'Allemagne, la Hollande et les États-Unis. Ces six pays placent au cœur de leur stratégie les fournisseurs d'accès à Internet (ou FAI) plutôt que la police (ce qui n'empêche pas cette dernière de continuer à enquêter). Les FAI occupent une place particulière dans l'écosystème numérique, puisque ces acteurs privés détiennent un monopole virtuel sur la circulation des flux de données qui irriguent le réseau des réseaux. À ce titre, l'ensemble des communications entre ordinateurs infectés et botmasters transite par leurs infrastructures, et cette propriété, ainsi que l'inspection plus ou moins approfondie des données à laquelle ils se livrent afin de maintenir les performances de leurs réseaux, en font des intermédiaires déterminants dans la lutte contre les botnets. Ils constituent à ce titre des « acteurs pivots » dont les actions se répercutent directement et indirectement sur l'ensemble de l'écosystème. À titre d'illustration, van Eeten, Bauer, Asghari, Tabatabaie et Rand (2010, p. 9) ont déterminé que plus de la moitié des pourriels diffusés dans le monde émanaient d'ordinateurs compromis reliés à Internet par cinquante grands FAI, ce qui implique que ce petit nombre d'entreprises facilite de manière involontaire les activités florissantes d'une proportion considérable des botnets en activité. Une modification des pratiques des FAI en matière de détection et de prévention des botnets pourrait donc rapidement provoquer des effets en cascade susceptibles d'améliorer durablement la sécurité des internautes.

Les FAI sont évidemment bien conscients du problème que constituent les botnets pour leurs usagers, et on peut distinguer trois grands types de réponses en matière de sécurité : interne, externe ou hybride (Rowe, Wood, Reeves & Braun, 2011). Les mesures internes couvrent les pratiques par lesquelles les FAI identifient les botnets et en perturbent les activités sans que leurs usagers en soient conscients, par exemple en bloquant certains ports (ou canaux) de communication. Les mesures externes concernent les conseils de sécurité prodigués par les FAI à leurs clients, ainsi que les rabais consentis en partenariat avec

les entreprises de sécurité sur les logiciels antivirus. Finalement, les initiatives hybrides concernent l'imposition de politiques contraignant les usagers à jouer un rôle dans la prévention du trafic informatique indésirable. L'un des obstacles majeurs à la mise en œuvre harmonisée de ces trois types d'interventions découle du manque d'incitatifs financiers directs, qui conduit certains FAI à ne consentir que des efforts minimaux, dans la mesure où les botnets ne nuisent en aucune manière à leur profitabilité. Les six initiatives de régulation décrites ici viennent ainsi structurer de manière plus homogène les mesures de sécurité prises par les FAI.

L'Australie et la Corée du Sud furent les premières à promouvoir des initiatives de régulation anti-botnet en 2005, suivies de près par le Japon l'année suivante. Les caractéristiques détaillées de chacun de ces six programmes sont présentées ailleurs par Dupont (2013b), et le tableau 1 récapitule les éléments qui nous paraissent les plus pertinents.

TABLEAU 1

Caractéristiques des six initiatives anti-botnets

	Australie	Japon	Corée du Sud	Allemagne	Hollande	É.-U.
Lancement	2005	2006	2005	2010	2010	2012
Volontaire	Oui	Oui	Oui	Oui	Oui	Oui
Financements publics	Oui	Oui	Oui	Oui	Oui (à partir de 2013)	Oui (partiel)
Surveillance	Centrale	Centrale	Centrale	FAI	Centrale (à partir de 2013)	FAI
Altération du trafic	Non	Non	Oui	Non	Non	Non
Notification	FAI	FAI	FAI	FAI	FAI	FAI
Site d'information en ligne	Oui	Oui	Oui	Oui	Non	Non
Ligne d'assistance téléphonique	Non	Non	Oui	Oui	Non	Non
Outil gratuit de désinfection	Non	Oui	Oui	Oui	Non	Non
Mise en quarantaine	Oui	Non	Oui (partiel)	Non	Oui	Oui (partiel)
Statistiques publiques	Oui (partiel)	Oui	Oui (partiel)	Oui (partiel)	Non	Non
Évaluation indépendante	Non	Non	Non	Non	Oui (partiel)	Non

Si des variations distinguent chacun des six programmes, ces derniers sont régis par des principes directeurs communs, dont la notion de partenariat constitue la clé de voûte : souvent mises sur pied par des organismes publics de régulation d'Internet dépendant des ministères de l'Économie et des Télécommunications plutôt que de la justice ou de la sécurité publique, ces initiatives fédèrent des acteurs privés habituellement en compétition pour des parts de marché. Nous avons déjà vu que les FAI jouent un rôle central, mais les entreprises qui commercialisent des logiciels antivirus apportent également une contribution importante à la détection et au nettoyage des ordinateurs infectés. Le mode de fonctionnement des programmes anti-botnets suit généralement le schéma suivant : les FAI et les divers organismes publics impliqués établissent un système d'agrégation des renseignements concernant les flux malveillants de données générés par les botnets[4], et se servent de leur poste privilégié d'observation de l'écosystème numérique pour dresser une liste régulièrement mise à jour des machines infectées. Cette liste sert à informer chacun des FAI participants des adresses IP (Internet Protocol, le mode d'identification unique des équipements informatiques raccordés à Internet) appartenant à ses clients dont l'activité parait suspecte. Les FAI informent à ce stade leurs usagers de l'infection probable de leur machine, par courriel, courrier postal ou encore au moyen d'un appel téléphonique. Les marges de profit dans ce secteur d'activité étant relativement faibles, ce travail d'alerte et de sensibilisation des usagers entraîne des coûts qui peuvent dissuader les FAI de se comporter de manière vertueuse. Afin de renforcer les incitatifs à s'impliquer dans de telles initiatives, les partenariats anti-botnets obtiennent fréquemment des subventions publiques permettant de concevoir des outils mutualisés d'information mis à la disposition des FAI et de leurs clients. Des sites Internet expliquant sans jargon technique ce qu'est un botnet et quelle est la procédure à suivre afin d'en débarrasser son ordinateur, ou encore des lignes d'assistance téléphonique accompagnant les usagers peu férus en informatique dans le processus de désinfection viennent ainsi alléger le travail des équipes de soutien technique des FAI – et par extension les coûts induits pour ces derniers. Les pays ayant intégré les entreprises d'antivirus à leur

4. Seuls deux pays (l'Allemagne et les É.-U.) ont délégué aux FAI la tâche de détecter les machines infectées, pour des raisons liées à la protection de la vie privée dans le premier cas et à l'absence d'une infrastructure administrative permanente dans le second.

partenariat mettent à la disposition des victimes des applications téléchargeables gratuitement afin de simplifier le processus de nettoyage et leur éviter ainsi de possibles fausses manœuvres.

La mise à jour régulière des listes de machines compromises permet également aux FAI d'identifier les usagers qui sont incapables, retardent ou refusent de corriger la situation. Au Japon, en 2010, 29 % des destinataires d'une notification d'infection ne prenaient ainsi aucune mesure palliative (Dupont, 2013b, p. 18). Des rappels sont alors envoyés, mais des mesures plus contraignantes peuvent également être envisagées. En Corée du Sud, en Hollande et aux États-Unis, les FAI confrontés à des usagers récalcitrants ont la possibilité de recourir à des mesures draconiennes en interrompant ou en restreignant l'accès de ces derniers à Internet jusqu'à ce que leurs machines soient débarrassées des applications malveillantes. La mise en quarantaine imposée aux machines infectées s'inspire ainsi directement des approches épidémiologiques, faisant des FAI les garants de la bonne « santé » de l'écosystème numérique. Ce recours à des moyens coercitifs soulève toutefois un certain nombre de problèmes éthiques et juridiques, particulièrement dans un contexte où l'accès à Internet tend à être considéré par certains comme une extension de droits fondamentaux tels que la liberté d'opinion et d'expression, et que la délégation du pouvoir de restreindre l'exercice de ces droits à des entités privées comme les FAI pourrait être vigoureusement contestée (La Rue, 2011, p. 12).

Bien que les données sur l'efficacité des initiatives anti-botnets restent fragmentaires et sujettes à interprétation, les résultats obtenus par la Corée du Sud, le Japon et l'Allemagne semblent indiquer une réduction significative de la proportion des ordinateurs compromis dans ces pays après l'implantation de ces partenariats. Le taux d'infection du parc informatique coréen est ainsi passé de 26 % à 0,5 % entre 2005 et 2011 (Asia Pacific Computer Emergency Response Team [APCERT], 2011 ; Korea Internet Security Agency [KISA], 2010), alors qu'au Japon, il a chuté de 2,5 % à 0,6 % durant la même période (Noritake, 2011). En Allemagne, où des outils de mesure différents sont utilisés, le volume de pourriels expédiés par des botnets a diminué de 75 % entre septembre 2010 et mai 2011 (Office fédéral pour la sécurité de l'information, 2011). En ce qui concerne les autres pays, l'absence d'évaluations est en partie attribuable à la nature volontaire des partenariats : dans la mesure où les FAI s'impliquent dans ces initiatives sans obligation légale, et où chaque participant conserve une large autonomie quant à

la démarche à suivre auprès de ses clients infectés, il peut s'avérer délicat de mesurer les résultats d'ensemble du dispositif sans distinguer la contribution respective de chaque partenaire, et de créer ainsi un palmarès des FAI les plus (ou moins) impliqués et efficaces dans la lutte contre les botnets. L'évaluation est ici perçue par les partenaires comme une interférence dans les modes de fonctionnement traditionnels du marché et risque de susciter plus de défections que d'adhésions au programme. Pourtant, sous certaines conditions, ces pratiques de divulgation publique (qui équivalent plus prosaïquement à nommer et dénoncer les acteurs inefficaces ou négligents) offrent de puissants leviers aux autorités régulatrices pour modifier le comportement et renforcer la conformité des acteurs placés sous leur contrôle. Elles sont fréquemment employées avec succès dans les secteurs de la santé, de l'éducation, de l'assurance ou de la protection de l'environnement (Pawson, 2002 ; Tietenberg, 1998).

Si la régulation des botnets par le biais de partenariats public-privé non contraignants semble produire des résultats plus significatifs et durables que l'arrestation épisodique de botmasters à la compétence variable, les promoteurs de cette approche vont rapidement se trouver confrontés à quatre défis de taille. Le premier est d'ordre technique : l'avènement de l'Internet des objets (IDO), c'est-à-dire de la mise en réseau d'une multitude d'équipements électroniques comme des téléphones intelligents, des tablettes informatiques, mais aussi des distributeurs automatiques de billets, des véhicules automobiles, des caméras de vidéosurveillance, des compteurs électriques intelligents ou des milliards de capteurs électroniques disséminés dans notre environnement ont rendu nécessaire le passage à un protocole de routage des flux de données capable d'accommoder des centaines de milliards d'adresses IP. Ce protocole, connu sous le nom d'IPv6, va complexifier le travail de surveillance et d'identification des machines compromises, dans la mesure où il sera beaucoup plus difficile d'établir avec certitude quelle est la personne ou l'organisation qui en est l'utilisatrice primaire, et de procéder à la désinfection de ces objets connectés, dont les interfaces sont d'une gestion beaucoup moins intuitive que celles des ordinateurs (Fenn & LeHong, 2011). Sur le plan social, les délinquants qui tirent profit des botnets sont également susceptibles d'exploiter les procédures de notification mises en œuvre par les programmes anti-botnets pour convaincre leurs victimes de télécharger des applications malveillantes. On observe déjà cette forme d'exploitation avec les fraudes aux faux

anti-virus, où la peur d'une infection inexistante permet aux délinquants d'obtenir de leurs victimes qu'elles s'acquittent de supposés frais de téléchargement pour un produit inutile et souvent nuisible au bon fonctionnement de la machine (Stone-Gross *et al*., 2013). Cette forme d'adaptation compétitive (Kenney, 2007) pose le problème de l'acquisition et de la rétention de la confiance des usagers, qui devront être en mesure de distinguer les notifications légitimes des tentatives frauduleuses. Le troisième obstacle est de nature juridique : dans le sillage des révélations concernant la surveillance généralisée dont font l'objet les internautes (le cas de la NSA n'étant que le révélateur médiatique d'une tendance mondiale – Deibert, 2013), convaincre ces derniers de l'innocuité, voire des bénéfices, d'un système reposant sur l'analyse systématique des flux de données numériques émanant de chaque utilisateur et le partage de cette information avec des agences gouvernementales relèvera de la gageure. L'Allemagne, qui a mis en place un rigoureux système de protection de la vie privée des propriétaires de machines infectées a fait le compromis d'une efficacité moindre afin de conserver la confiance des usagers et écarter ainsi tout soupçon d'espionnage (Organisation de coopération et de développement économiques [OCDE], 2011). Finalement, ces mécanismes de régulation restent pour le moment définis et mis en œuvre à l'échelle nationale, alors que le problème est fondamentalement transnational. Certains pays, comme le Japon, la Corée du Sud ou l'Allemagne, tentent de projeter leurs capacités de prévention dans les pays limitrophes, mais ces initiatives restent encore embryonnaires et aucune instance internationale n'y a encore porté attention, par contraste avec les modes de régulation transnationaux qui caractérisent le transport aérien, l'énergie nucléaire ou encore les activités bancaires (Braithwaite & Drahos, 2000).

Conclusion

Ce rapide panorama de six programmes de régulation des botnets axés sur la désinfection et le renforcement de la résilience des victimes plutôt que sur des stratégies juridiques de neutralisation des botmasters a montré que, relativement à l'émergence d'une délinquance numérique intrinsèquement transnationale, les interventions répressives classiques s'avèrent bien mal adaptées pour faire face à la prolifération d'incidents dont l'impact individuel est limité, voire négligeable, mais dont le préjudice global sur l'écosystème numérique demeure préoccupant. Bien

que les résultats d'évaluations démontrant la supériorité de la régulation sur la judiciarisation restent encore incomplets, et que des efforts additionnels doivent être consentis afin d'accumuler plus de données sur ce point, les éléments à notre disposition suggèrent néanmoins que l'approche de régulation pluraliste examinée ici pourrait être envisagée de manière plus systématique comme mécanisme de renforcement de la sécurité numérique. Le rôle que les institutions ou les réseaux de la police transnationale pourraient jouer dans cette nouvelle architecture décentralisée de la régulation du cybercrime reste cependant imprécis.

Des six programmes examinés, aucun n'associe (à notre connaissance) à ses activités des unités d'enquête ayant la capacité d'analyser les vastes quantités de données accumulées afin d'orienter les interventions policières. Si des collaborations associent ponctuellement services de police et entreprises (notamment le géant Microsoft, très actif dans la lutte contre les botnets – Krebs, 2012c), ces opérations conjointes se limitent en règle générale à une division du travail où l'enquête criminelle est menée en amont par le secteur privé, et où les policiers prennent le relais au moment de l'arrestation, du recueil de la preuve et du dépôt des accusations devant un tribunal. De tels procédés, qui confinent à une instrumentalisation des institutions policières par des intérêts privés, ont fréquemment été documentés dans d'autres contextes d'enquête où la police se trouve en déficit d'expertise (Dorn & Levi, 2007 ; Marx, 1987 ; Schneider, 2006). Néanmoins, ce modèle d'intervention reste fondamentalement répressif. Une autre approche, inspirée des théories sur la tierce police de Mazerolle et Ransley (2005), est toutefois envisageable. La notion de tierce police évoque la mobilisation par la police d'une variété de nœuds (ou d'acteurs) de régulation afin de résoudre des problèmes particuliers de délinquance. Ces partenariats reposent sur l'autorité légale dont dispose l'institution policière afin de persuader ou de contraindre des nœuds de régulation à une intervention dans certains contextes et selon certaines modalités afin de prévenir ou de réduire la criminalité visée (Mazerolle & Ransley, 2005, p. 2). L'objectif de la police n'est plus alors de procéder aux interventions requises sur une base monopolistique (du moins pas en premier recours), mais plutôt de mandater les organisations détenant les capacités idoines afin qu'elles s'insèrent dans un réseau coproducteur de sécurité coordonné par des structures étatiques. Dans cette configuration, les moyens limités de la police sont compensés par sa capacité à catalyser les activités de régulation de tierces parties dans l'intérêt

public. Une telle approche se prête particulièrement bien aux problèmes de cybersécurité, mais reste encore très marginale dans ce domaine (Wall, 2007).

Loin d'être accessoire, cette question sur le rôle de la police exprime un doute sur les capacités de l'institution, dans la conception actuelle qu'elle se fait d'elle-même et de son mandat, d'opérer la transition requise afin de s'adapter à la révolution numérique entreprise au début des années 1990. Émanations de la révolution industrielle du XIX^e^ siècle et du besoin de professionnaliser les fonctions locales de maintien de l'ordre urbain et social (Brodeur, 2010), les institutions policières semblent éprouver des difficultés à dépasser ce modèle fondateur et à envisager leur place dans un environnement polycentrique transnational où la sécurité est produite par des réseaux d'acteurs publics, privés et hybrides mobilisant une pluralité de ressources afin de garantir l'intégrité de flux dématérialisés. Ce désintérêt institutionnel est en grande partie entretenu par une réalité budgétaire qui fait des agences de renseignement et des forces armées, plutôt que de la police, les principales bénéficiaires des ressources publiques allouées aux politiques de cybersécurité (Deibert, 2013 ; Dupont, 2013c). On comprend bien à travers ce choix la dimension stratégique qu'ont acquise les infrastructures numériques dans nos sociétés contemporaines. Toutefois, il nous replonge dans un univers hobbesien où le botnet est le nouveau loup, et où les usagers se trouvent réduits pour leur protection à l'alternative suivante : faire confiance à des services de renseignement avides de données personnelles mais opaques et peu concernés par une cybercriminalité de basse intensité, ou se tourner vers des entreprises tout aussi impénétrables qui peuvent être tentées de voir dans les mesures volontaires de prévention des risques numériques un facteur d'érosion de leurs profits – les uns et les autres entretenant par ailleurs des relations symbiotiques. *A contrario*, les six initiatives présentées ici figurent parmi les rares exemples documentés d'une régulation pluraliste de la cybercriminalité. Cependant, force est de constater que l'imagination et la capacité d'innovation ayant rendu possible la révolution numérique restent encore bien insuffisantes pour provoquer une révolution régulatoire.

Références

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. (2006). A multifaceted approach to understanding the botnet phenomenon. *Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement, Rio de Janeiro*, 41-52.

Abu Rajab, M., Zarfoss, J., Monrose, F., & Terzis, A. (2007). My botnet is bigger than yours (maybe, better than yours) : why size estimates remain challenging". *Proceedings of the First Conference on First Workshop on Hot Topics in Understanding Botnets, New York*, 1-8.

Aebi, M., & Linde, A. (2010). Is there a crime drop in Western Europe ? *European Journal on Criminal Policy and Research, 16*(4), 251-277.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime : a workshop held in Berlin, June 25 and 26, 2012. Repéré sur Workshop on the Economics of Information Security (WEIS) : http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

APCERT. (2011). *APCERT annual report 2011.* Tokyo : Asia Pacific Emergency Response Team.

Ayres, I., & Braithwaite, J. (1992). *Responsive regulation*. New York, NY : Oxford University Press.

Baldwin, R., Cave, M., & Lodge, M. (2010). Introduction : Regulation–The field and developing agenda. Dans R. Baldwin, M. Cave & M. Lodge (Éds.), *The Oxford handbook of regulation* (pp. 3-16). Oxford : Oxford University Press.

Black, J. (2002). Critical reflections on regulation. *Australian Journal of Legal Philosophy, 27*, 1-35.

Braithwaite, J., & Drahos, P. (2000). *Global business regulation.* Cambridge : Cambridge University Press.

Brodeur, J.-P. (2010). *The policing web.* New York, NY : Oxford University Press.

Camus, A. (1942). *Le mythe de Sisyphe : Essai sur l'absurde.* Paris : Gallimard.

Choo, R. (2007). Zombies and botnets. *Trends & Issues in Criminal Justice*, 333. Canberra : Australian Institute of Criminology.

Cluley, G. (2012, 23 mai). Bredolab : Jail for man who masterminded botnet of 30 million computers [Web log post]. Repéré à http://nakedsecurity.sophos.com/2012/05/23/bredolab-jail-botnet/. Consulté le 30 septembre 2013.

Décary-Hétu, D., & Dupont, B. (2012). The social network of hackers. *Global Crime, 13*(3), 160-175.

Deibert, R. (2013). *Black code : Inside the battle for cyberspace.* Toronto : McClelland & Stewart.

De Graaf, D., Shosha, A., & Gladyshev, P. (2012, 25-26 octobre). BREDOLAB : Shopping in the cybercrime underworld. Lecture conducted from *4th International Conference on Digital Forensics & Cyber Crime*, Lafayette, LA.

Dorn, N., & Levi, M. (2007). European private security, corporate investigation and military services : collective security, market regulation and structuring the public sphere. *Policing and Society, 17*(3), 213-238.

Dupont, B. (2010). L'évolution du piratage informatique : De la curiosité technique au crime par sous-traitance ». Dans AAPI (Éd.), *Le respons@ble 2.0 : Acteur clé en AIPRP* (pp.63-81). Cowansville : Éditions Yvon Blais.

Dupont, B. (2013a). Skills and trust : a tour inside the hard drives of computer hackers. Dans C. Morselli (Éd.), *Crime and networks* (pp.195-217). New York, NY : Routledge.

Dupont, B. (2013b). *An international comparison of anti-botnet partnerships.* Ottawa : Sécurité Publique Canada.

Dupont, B. (2013c). The proliferation of cyber security strategies and their implications for privacy. Dans K. Benyekhlef & E. Mitjans (Éds.), *Circulation internationale de l'information et sécurité* (pp. 67-80). Montréal : Les Éditions Thémis.

Drahos, P., Shearing, C., & Burris, S. (2005). Nodal governance as an approach to regulation. *Australian Journal of Legal Philosophy, 30*, 30-58.

Eudes, Y., & Seelow, S. (2014, 25-26 mai). Vaste coup de filet contre les utilisateurs d'un logiciel grand public de piratage. *Le Monde*, p. 10.

Farrell, G., Tseloni, A., Mailley, J., & Tilley, N. (2011). The crime drop and the security hypothesis. *Journal of Research on Crime and Delinquency, 48*(2), 147-175.

FBI. (2012). *FBI, international law enforcement disrupt international cyber crime ring related to Butterfly botnet* (Communiqué de presse). Consulté le 30 septembre 2013. Repéré à http://www.fbi.gov/news/pressrel/press-releases/fbi-international-law-enforcement-disrupt-international-organized-cyber-crime-ring-related-to-butterfly-botnet.

Fenn, J., & LeHong, H. (2011). *Hype cycle for emerging technologies, 2011.* Stamford : Gartner.

GO-Gulf. (2012, 2 mai). *Global online advertising spending statistics.* Consulté le 11 septembre 2013. Repéré à www.go-gulf.com/blog/online-ad-spending/.

Goncharov, M. (2012). *Russian underground 101.* Cupertino : Trend Micro.

Grabosky, P. (2012). Beyond Responsive Regulation : The expanding role of non-state actors in the regulatory process. *Regulation & Governance, 7*(1), 114-123.

Homère. (1766). *Oeuvres d'Homère* (traduit par M. Dacier & A. Leide). Paris : Chez J. de Wetstein & Fils.

Kenney, M. (2007). *From Pablo to Osama : Trafficking and terrorist networks, government bureaucracies and competitive adaptation*. University Park, PA : The Pennsylvania State University Press.

KISA. (2010, 25-26 janvier). *Report on July DDoS attack in Korea and Korea's countermeasure.* Présenté lors de la conférence INCO-TRUST, Séoul.

Krebs, B. (2012a, 19 juillet). Top spam botnet, "Grum," unplugged" [Web log post]. Consulté le 30 septembre 2013. Repéré à https://krebsonsecurity.com/2012/07/top-spam-botnet-grum-unplugged/.

Krebs, B. (2012b, 1er février). Who's behind the world's largest spam botnet ? [Web log post]. Consulté le 30 septembre 2013. Repéré à http://krebsonsecurity.com/2012/02/whos-behind-the-worlds-largest-spam-botnet/.

Krebs, B. (2012c, 26 mars). Microsoft takes down dozens of Zeus, Spyeye botnets" [Web log post]. Consulté le 30 septembre 2013. Repéré à http://krebsonsecurity.com/2012/03/microsoft-takes-down-dozens-of-zeus-spyeye-botnets/.

La Rue, F. (2011). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression to the Sixty-sixth session of the General Assembly*. New York, NY : Organisation des Nations Unies.

Leman-Langlois, S. (2003). Rationalité pénale moderne et terrorisme : Peut-on contrôler le « méga-crime » à l'aide du système pénal ? Dans D. Casoni & L. Brunet (Éds.), *Comprendre l'acte terroriste* (pp.113-119). Montréal : Les Presses de l'Université du Québec.

Maass, P., & Rajagopalan, M. (2012, 1er août). Does cybercrime really cost $1 trillion ? [Web log post]. Consulté le 25 septembre 2013. Repéré à http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion.

Marx, G. T. (1987). The interweaving of public and private undercover work. Dans C. Shearing & P. Stenning (Éds.), *Private policing* (pp. 172-193). Thousand Oaks, CA : Sage Publications.

Maurushat, A. (2012). The role of internet service providers in combatting botnets : An examination of recent Australian initiatives and legislative reform. *Telecommunications Journal of Australia*, *62*(4), 61.1-61.18.

Mazerolle, L., & Ransley, J. (2005). *Third party policing*. Cambridge : Cambridge University Press.

McCoy, D., Pitsillidis, A., Jordan, G., Weaver, N., Kreibich, C., Krebs, B., Voelker, G., Savage, S., & Levchenko, K. (2012, 8-10 août). *PharmaLeaks : Understanding the business of online pharmaceutical affiliate programs*. Symposium conducted at the *21st USENIX Security Symposium*, USENIX, Bellevue, WA.

Namestnikov, Y. (2009). *The economics of botnets*. Moscou : Kaspersky Lab.

Noritake, S. (2011). Transition from the anti-botnet project to a new project : Prediction and quick response against cyber attacks through international collaboration : a workshop held in Rangoon, November, 29 to December, 1st. Consulté le 13 septembre 2013. Repéré à http://www.itu.int/ITU-D/asp/CMS/Events/2011/CIRTWkshp/S3_Satoshi_Noritake.pdf.

OCDE. (2011). *The role of internet intermediaries in advancing public policy objectives*. Paris : OCDE Éditions.

Office Fédéral pour la Sécurité de l'Information. (2011). *The IT security situation in Germany in 2011*. Bonn : BSI.

Ouimet, M. (2002). Explaining the American and Canadian crime "drop" in the 1990's". *Revue Canadienne de Criminologie et de Justice Pénale*, *44*(1), 33-50.

Pawson, R. (2002). Evidence and policy and naming and shaming. *Policy Studies*, *23*(3), 211-230.

Perreault, S. (2011). Les incidents autodéclarés de victimisation sur Internet au Canada, 2009. *Juristat*. Statistique Canada : Ottawa.

Perreault, S., & Brennan, S. (2010). La victimisation criminelle au Canada, 2009. *Juristat*, *30*(2). Ottawa : Statistique Canada.

Rowe, B., Wood, D., Reeves, D., & Braun, F. (2011). *The role of internet service providers in cyber security*. Durham, NC : Institute for Homeland Security Solutions.

Schneider, S. (2006). Privatizing economic crime enforcement : Exploring the role of private sector investigative agencies in combating money laundering. *Policing and Society*, *16*(3), 285-312.

Shearing, C., & Wood, J. (2003). Nodal governance, democracy and the 'new denizens. *Journal of Law and Society*, *30*(3), 400-419.

Smith, R., Grabosky, P., & Urbas, G. (2004). *Cyber criminals on trial*. Cambridge : Cambridge University Press.

Stevens, K., & Jackson, D. (2010). *ZeuS banking trojan report*. Atlanta : SecureWorks.

Stone-Gross, B., Abman, R., Kemmerer, R., Kruegel, C., Steigerwald, D., & Vigna, G. (2013). The underground economy of fake antivirus software. Dans B. Schneier (Éd.), *Economics of information security and privacy III* (pp. 55-78). New York, NY : Springer.

Symantec. (2009, 10 septembre). *Cyber crime has surpassed illegal drug trafficking as a criminal moneymaker : 1 in 5 will become a victim*. Communiqué de presse. Repéré à http://www.symantec.com/about/news/release/article.jsp?prid=20090910_01. Consulté le 25 septembre 2013.

Tietenberg, T. (1998). Disclosure strategies for pollution control. *Environmental and Resource Economics*, *11*(3-4), 587-602.

Trusteer. (2009), *Measuring the in-the-wild effectiveness of antivirus against ZeuS*. New York, NY : Trusteer.

Van eeten, M., Bauer, J., Asghari, H., Tabatabaie, S., & Rand, D. (2010). The role of internet service providers in botnet mitigation : An empirical analysis based on spam data : a workshop held in Cambridge, June, 7 and 8.

Van eeten, M., Asghari, H., Bauer, J., & Tabatabaie, S. (2011). *Internet service providers and botnet mitigation : A fact-finding study on the Dutch market*. Delft : Delft University of Technology.

Vicario, M. (2010, 27 octobre). Bredolab is still in the wild. Consulté le 12 septembre 2013. Repéré à http://www.symantec.com/connect/blogs/bredolab-still-wild.

Vratonjic, N., Manshaei, M., Raya, M., & Hubaux, J.-P. (2010). ISPs and ad networks against botnet ad fraud. Dans T. Alpcan, L. Buttyan & J. Baras (Éds.), *Decision and game theory for security* (pp.149-167). Berlin : Springer.

Wall, D. (2007). Policing cybercrimes : Situating the public police in networks of security within cyberspace. *Police Practice and Research*, *8*(2), 183-205.

Wyke, J. (2012). *The ZeroAccess botnet – Mining and fraud for massive financial gain*. Burlington, VT : Sophos Labs.

Zarfoss, J. (2007). *A scalable architecture for persistent botnet tracking, A thesis submitted in conformity with the requirements for the degree of Master of Science in Engineering*. Baltimore, MD : John Hopkins University.

ABSTRACT • *Botnets, which are computers controlled by malicious hackers, currently represent the most serious threat to the digital ecosystem, providing the infrastructure to commit bank fraud, distributed denial of service attacks (DDoS), or click fraud. During the past few years, two main approaches have been used to fight botnets : First, police organizations have arrested high profile hackers and dismantled their command and control systems. Second, some countries, more precisely Japan, South Korea, Australia, the Netherlands and Germany have encouraged public-private partnerships involving Internet service providers and anti-virus companies. Inspired by regulatory principles, these initiatives seek to identify infected computers, notify their owners and help them clean their machines. This article compares these two approaches (criminalization vs. regulation) by trying to establish their respective effectiveness with respect to securing the digital ecosystem.*

KEYWORDS • *Cybercrime, botnets, criminalization, regulation, prevention.*

RESUMEN • *Los botnets, o las redes informáticas comprometidas por los piratas informáticos, representan actualmente la amenaza criminal más grave, sirviendo de soporte al fraude bancario, a los ataques distribuidos a través de la denegación de servicio (DDoS), o también al fraude del clic. En el transcurso de los últimos años, dos enfoques distintos han sido privilegiados para combatir estos botnets : por un lado, los servicios policiales han procedido al arresto fuertemente mediatizado de algunos piratas informáticos de alto vuelo y al desmantelamiento de sus infraestructuras de comando y de control. Por otro lado, en algunos países, especialmente en Japón, en Corea del Sur, en Australia, pero también en Holanda o en Alemania, los gobiernos han favorecido la emergencia de asociaciones público-privadas implicando los proveedores de acceso y las empresas de seguridad informática. En una gestión reguladora, estas iniciativas apuntan a identificar las computadoras infectadas, a notificar a sus propietarios y a ayudar a éstos a limpiar su máquina. Este artículo tiene entonces como objetivo comparar los dos enfoques (judiciarización vs. regulación), intentando, especialmente, evaluar los efectos producidos por cada uno de ellos sobre el nivel de seguridad del ecosistema numérico.*

PALABRAS CLAVE • *Cibercrimen, botnets, judiciarizacion, regulación, prevención.*