Jeunesse et Cybercriminalité : une Étude de la Diffusion du Cybercrime

Résumé :
Un nombre croissant de chercheurs déclarent que l'Internet présente « une opportunité unique pour un comportement déviant » (Rogers et al., 2006). Certains chercheurs ont travaillé sur ce thème via l'étude de l'éthique online (Kallman et Grillo, 1996) ou des business du cyber-crime (Kanich et al., 2009 ; Kshetri, 2009), mais les facteurs qui conduisent les adolescents et jeunes adultes à adopter un comportement cybercriminel ont reçu moins d'attention. Nous pensons donc qu'il peut être pertinent d'étudier de plus près la diffusion des connaissances dans le domaine du piratage informatique ; notre étude cherche ainsi à explorer les facteurs qui favorisent le cyber-crime. Dans le cadre du modèle conceptuel de la diffusion de l'innovation de Greenhalgh et al. (2004), nous décrirons la diffusion de comportements cybercriminels à travers une revue de la littérature qualitative.
Mots Clefs :
Usages, Cyber-crime, Déviance, Diffusion, Innovation
Axe thématique :
Pratique numériques : Les modalités de l'usage des TIC

***

L'objet de notre projet de recherche était d'étudier les comportements déviants sur internet, et plus précisément de tenter d'identifier les 'facilitateurs' du cyber-crime ; comment expliquer la diffusion de ce comportement déviant parmi les adolescents et jeunes adultes ?
Nous avons mené une revue de la littérature descriptive, en prenant pour appui le cadre conceptuel de Greenhalgh et al. (2004) de la diffusion d'une innovation.

Contexte : hackers et cybercriminalité

Le mot « hacker » est généralement utilisé de nos jours par les médias pour décrire une personne qui pénètre par effraction dans un système informatique pour voler ou détruire des données (Sterling, 1993) ; la police décrit presque tout crime commis à travers, avec, par ou contre un ordinateur comme du piratage informatique. L'emploi du terme « hacker » a changé au fil du temps, passant d'une définition positive et méliorative (le programmeur informatique passionné et particulièrement brillant) à une définition négative et péjorative (le cybercriminel). La définition du terme « hacker » est encore une pierre d'achoppement, tout comme le concept de « cyber-crime ».
Il n'y a en effet toujours pas de définition précise du terme cyber-crime (Fafinski et al., 2010). D'un côté, le cyber-crime peut comprendre l'emploi d'ordinateurs pour faciliter des délits dits traditionnels ; de l'autre, le cyber-crime peut être un crime ayant recours à la technologie (Wall, 2007), ou un crime purement technologique comme une attaque par déni de service par exemple. De nombreux spécialistes du droit criminel se concentrent sur le cadre légal de la définition. Par exemple, Wall (2001) transpose des catégories dérivées du droit criminel en catégories équivalentes pour l'univers cyber. D'autres classent les délits comme étant « en relation avec des systèmes informatiques et leur contenu ou portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des données et des systèmes informatiques. » (Conseil de l'Europe, Convention sur la cybercriminalité, 2001).
La cybercriminalité est un terrain globalement peu étudié ; et s'il y a des recherches sur le business du cyber-crime (Kanich et al., 2009 ; Kshetri, 2009), il n'y a pas d'étude sur la diffusion de ce phénomène. Dans le cadre de notre projet, nous étudierons seulement les comportements déviants cybercriminels ayant un but lucratif. Nous ne traitons pas les cyber-crimes à but non lucratifs (par exemple, l'hacktivisme (activisme politique sur internet)) ou les activités déviantes ne relevant pas de la définition par le conseil de l'Europe du cybercrime (contenus pornographiques extrêmes, sites web incitant au suicide, etc).

Hypothèse

Nous partons de l'hypothèse que le cyber-crime est une innovation par rapport au crime traditionnel et qu'il est bien plus qu'une extension du crime traditionnel. Nous pensons donc qu'une revue de la littérature, analysée à travers un modèle de diffusion de l'innovation, pourrait éclairer les facteurs qui favorisent le cyber-crime parmi les adolescents et jeunes adultes.

Méthodologie

Nous avons utilisé le modèle conceptuel de diffusion de l'innovation de Greenhalgh et al. (2004). Les auteurs ont effectué une revue systématique de la littérature empirique et des théories liées à la diffusion de l'innovation ; ils ont étudié 6 000 articles, livres et abstracts et se sont concentrés sur 495 sources pour leur rapport final. Ils ont formulé un modèle conceptuel à partir de la synthèse des conclusions théoriques et empiriques ; ce modèle catégorise les facteurs nécessaires pour que l'innovation soit un succès.

Les facteurs clefs de succès indiqués par le modèle de Greenhalgh et al. sont les suivants :
a- L'innovation doit être compatible (en accord avec les valeurs et besoins perçus par l'utilisateur) et sans risque (aucune incertitude au sujet de son avenir).
b- L'innovation doit fournir un avantage relatif (elle doit être clairement mieux que le modèle précédent pour ce qui est de l'efficacité, du coût ou du retour sur investissement), doit résoudre les problèmes de l'utilisateur (améliorer sa performance) et doit être observable (bénéfices clairement visibles).
c- L'innovation doit être facile à utiliser et demander peu de connaissances.
d- L'innovation doit être adaptable (modifiable en fonction des besoins de l'utilisateur). De plus, l'innovation doit permettre l'expérimentation et avoir une communauté de soutien qui fournit des formations, un service d'assistance et un système de personnalisation.

Nous avons utilisé ce cadre conceptuel pour analyser la littérature disponible sur le cyber-crime et le piratage informatique. Nous avons mené une revue descriptive exhaustive de la littérature (King et He, 2005), synthétisé les recherches précédentes et analysé les résultats en lien avec notre hypothèse.
Le plus souvent, les revues de la littérature ciblent les revues de renom et les conférences ; cette approche est pertinente pour des sujets de recherche établis mais pas pour une revue de la littérature sur le cyber-crime puisqu'il s'agit d'un phénomène moderne qui ne justifie donc pas de se concentrer sur des sources limitées. Nous avons donc concentré nos recherches sur des bases de données en ligne, en ciblant Business Source Complete, Proquest, ScienceDirect, Scirus, Scopus et Web of Science. Nous avons mené une recherche par mots-clés en regardant les abstracts de tous les articles disponibles dans ces six bases de données. Nous avons effectué un premier tri des articles en parcourant les titres et les abstracts, en enlevant les doublons et les articles qui ne faisaient que mentionner le piratage informatique ou le cyber-crime sans se concentrer sur ces sujets. Après avoir passé les textes en revue, nous avons éliminé les articles sans rapport avec le sujet et classé les articles restants en fonction des facteurs clés de succès décrits par Greenhalgh et al.

Résultats

1 – De jeunes hackers (risque et observabilité)

Dans son approche économique du crime, G. Becker (1968) affirme que l'on décide de commettre un crime en effectuant une analyse coût-bénéfice. Selon cette perspective, on choisit une alternative illégale au lieu d'une alternative légale tout comme on fait un choix économique ou de consommation au sein du marché. La décision de commettre un crime implique des calculs fondés sur une estimation de la disponibilité, du risque, du coût et de la possibilité de réussite d'une opportunité. Des revenus peu élevés ou le manque d'opportunités d'obtention d'un revenu sont deux facteurs importants qui peuvent pousser au crime. Les adolescents ont moins de revenus, moins d'opportunités d'en avoir et peuvent facilement ne pas tenir compte du futur lorsqu'ils évaluent les coûts d'opportunité du crime (Becker, 1976).
De nombreux sondages ont été menés sur les adolescents et le piratage informatique (Panda Security, 2009 ; Trend Micro, 2009 ; Tufin Technologies, 2010). Bien qu'il faille nous méfier de la subjectivité de l'industrie de la sécurité, ces études arrivent presque toutes à la même conclusion : le piratage informatique occasionnel fait presque autant partie de la vie des adolescents que de télécharger de la musique sur un iPod. Plus de quatre adolescents sur dix ont piraté le profil d'une autre personne pour lire ses emails, ont regardé ses comptes bancaires ou se sont connectés au profil de réseau social d'une autre personne. La majorité des jeunes interrogés admettent pirater un compte pour faire une blague de potache ; mais un adolescent sur trois a avoué être tenté d'essayer le piratage informatique ou l'espionnage sur internet pour gagner de l'argent.

Ainsi, le piratage informatique semble sans risques (les adolescents ont tendance a accorder moins de valeur au futur) et ses bénéfices sont clairement visibles ; comment est-ce qu'un adolescent pourrait gagner £100 000 par an autrement ? (Blincoe, 2010). Les média promeuvent indirectement les revenus des hackers, et

même les études académiques en font une promotion indirecte en montrant que le spam est hautement rentable ou que des botmasters peuvent gagner environ 3,5 millions de dollars par an (Kanich & al., 2009).

2 – Des barrières à l'entrée réduite (compatibilité, expérimentation, formation, support et coût)

Tout d'abord, les jeunes considèrent le piratage informatique comme une activité facile d'accès puisque le piratage informatique est compatible avec leur mode de vie. Par cela, nous voulons dire que les ordinateurs font partie de la vie de chacun et que les natifs de l'ère numérique ('digital natives') sont nés avec internet et un clavier (Prensky, 2001). Ces natifs de l'ère numérique ne distinguent que très peu l'univers en ligne et l'univers hors-ligne, le virtuel et le réel (Palfrey & Gasser, 2008). Il est même possible qu'ils ne sachent pas que leur comportement déviant sur le web est illégal (Kallman & Grillo, 1996) ; par exemple rechercher et télécharger un film sur le web à partir d'un forum de hackers peut leur sembler comme une activité désinvolte et négligeable. Ainsi, Im et Van Epps montraient dès 1991 que les populations étudiantes avaient tendance à ne pas se rendre compte que d'utiliser des logiciels avec des licences hackées était du vol pur et simple.

Par ailleurs, le piratage informatique est moins complexe qu'il y a quelques années puisque les communautés de hackers ont largement diffusé leurs connaissances sur internet. Ainsi, le web a grandement réduit la difficulté pour devenir un cybercriminel. Maintenant, avec une simple recherche Google, on peut trouver beaucoup de documentation, de guides pratiques et de conseils afin de se lancer dans le business. Ainsi, les blogs et les communautés en ligne ont contribué à ce partage d'informations : les débutants peuvent bénéficier des connaissances et conseils de hackers plus expérimentés sur les forums de discussion (Imperva, 2011). Les adolescents peuvent adopter un comportement déviant par expérimentation : il est facile d'essayer un logiciel d'analyse de réseau sur un réseau privé et puis de l'essayer sur un réseau publique par curiosité. De nombreux outils de piratage informatique sont faciles d'utilisation ou intuitifs (sur le modèle du 'Crime as a Service' ou de 'toolkits' prêts à l'emploi).

Le dernier facteur qui contribue à diminuer les barrières est le fait que le piratage informatique est moins cher que jamais. Les prestataires d'infrastructure-as-a-service/ platform-as-a-service fournissent ainsi un serveur virtuel qui permet de créer, accéder à et configurer des serveurs et systèmes de stockages virtuels. Le Cloud Computing permet à un étudiant de ne payer que pour la capacité dont il a besoin et de rajouter de la capacité en ligne dès que cela devient nécessaire. En d'autres termes, un adolescent doué en informatique pourrait utiliser la puissance de calcul phénoménale d'une plateforme en Cloud pour craquer un mot de passe par brute-force pour seulement $0,28 centimes par minute. Le logiciel de brute-force permettra de générer des millions de mot de passe, de les crypter et voir s'ils autorisent l'accès au réseau. $1,68 suffit pour rentrer dans un réseau sans fil protégé (Roth, 2011). Puisque souvent chez les prestataires d'infrastructure-as-a-service, il n'y a pas de limites de bande passante ni de détection au niveau serveur concernant l'exécution d'actions malveillantes, un hacker amateur peut facilement effecteur une attaque par déni de service, envoyant un flot de paquets vers le réseau de la compagnie cible à faible coût et à grande échelle (en utilisant l'immense capacité du service).

Les adolescents d'aujourd'hui étant des natifs de l'ère numérique habitués à utiliser les ordinateurs et Internet, le cyber-crime est compatible avec leur environnement. Par ailleurs, de nos jours, le piratage informatique est devenu plus simple que jamais à travers la diffusion sur le web de boîtes à outils, de conseils et de soutien d'autres hackers. Grâce à la facilité d'accès du Cloud Computing, les tentatives de piratage informatique sont moins chères et demandent encore moins de connaissances qu'auparavant.

3 – De nombreux avantages par rapport au crime traditionnel (avantage relatif et performance)

« *such crimes are less likely to be caught and prosecuted […] only about 5% of cyber-criminals are caught*» (Kshetri, 2009). Le cyber-crime peut être un crime commis à grande échelle et rapporter beaucoup : même un taux de réponse extrêmement faible au spam reste hautement profitable pour le spammer (Kanich et al., 2009).

Par ailleurs, le coût psychologique du crime commis sur le web est bas pour deux raisons principales. Tout d'abord, les victimes du cyber-crime sont souvent difficiles à identifier (Phukan, 2002). Cela veut dire que lors de campagnes massives d'envoi d'emails frauduleux, les hackers envoient une quantité immense d'emails et ne voient pas leur victime (ils ne font qu'appuyer sur le bouton « envoi »). Ou, quand un hacker crée et distribue un malware sur le web pour voler des numéros de cartes de crédits, il attrape « quelqu'un » (une série de chiffres), mais ne voit jamais le visage de sa victime et n'interagit pas avec elle. Ce n'est pas la même difficulté que le braquage d'une banque (contact physique, visuel).

Ensuite, les hackers ne voient pas leur comportement comme étant malhonnête. Des recherches ont démontré que de nombreux étudiants ne considèrent pas le piratage de logiciels comme étant un comportement non éthique et criminel (Im et Van Epps, 1991; Reid et al., 1992). Au contraire, certains pensent que de tels comportements peuvent leur permettre de réussir dans la vie (Davis et Vitell, 1991).

***

Pour conclure, nous pourrions dire que le modèle conceptuel de Greenhalgh et al. permet de délivrer une explication satisfaisante à la diffusion de ce type de comportement déviant (cybercrime) parmi les adolescents et jeunes adultes. Cette première étude pourrait être vérifiée par des interviews avec de jeunes hackers. En termes de portée, notre revue de la littérature descriptive peut fournir un aperçu à des chercheurs et professionnels s'intéressant à la diffusion du cyber-crime, et contribue à une culture cumulative qui est pertinente étant donné le faible nombre d'article publiés sur la cybercriminalité.

Eléments bibliographiques

Becker, G. (1968). Crime and Punishment: An Economic Approach. The Journal of Political Economy 76: pp. 169–217.

Becker, G. (1976). The Economic Approach to Human Behavior. Chicago: University of Chicago Press.

Blincoe, R. (2010). High-living hacker swaps Porsche for porridge. The Register, Retrieved january 13, 2011, from http://www.theregister.co.uk/2010/06/18/hacker_jailed/

Council of Europe Convention on Cybercrime (2001). Treaties, Retrieved february 16, 2011, from http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm

Davis, D.L. & Vitell, S.J. (1991). The Ethical Problems, Conflicts and Beliefs of Small Business Information Personnel. The Journal of Computer Information Systems, 53-57.

Fafinski, S., Dutton, W. H. and Margetts, H. Z., (2010). Mapping and Measuring Cybercrime. OII Working Paper No. 18.

Greenhalgh, T., Robert, G., Macfarlane, F., Bate, P., & Kyriakidou, O. (2004). Diffusion of Innovations in Service Organizations: Systematic Review and Recommendations. Milbank Quarterly, 82(4), 581-629

Im, J.H., & van Epps, P.D. (1991). Software Piracy and Software Security in Business Schools: An Ethical Perspective. Data Base, 15-21.

Kallman, E.A. and J.P. Grillo (1996). Ethical Decision Making and Information Technology. 2e, New York: McGraw Hill.

Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G.,Paxson, V., and Savage, S. (2009).
Spamalytics: An Empirical Analysis of Spam Marketing Conversion. Communications of the ACM, Vol. 52, No. 9, pp. 99-107.

King, W.R., and He, J. 2005. "Understanding the Role and Methods of Meta-Analysis in IS Research," Communications of the Association for Information Systems (16), p 1.

Kshetri, N. (2009). Positive externality, increasing returns, and the rise in cybercrimes. Communications of the ACM, v.52 n.12, December.

McAfee, (2010). Threats Report: Third Quarter 2010. Retrieved january 13, 2011, from http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2010.pdf

Palfrey, J., Gasser, U., (2008). Born Digital: Understanding the First Generation of Digital Natives. Basic Books.

Panda Security, (2009). Studying or Hacking? Today's Adolescents Could be the Hackers of the Future. Retrieved january 06, 2011, from http://www.pitchengine.com/preview-release.php?id=11537.

Phukan, S. (2002). IT Ethics in the Internet Age: New Dimensions. Proc. Informing Science & IT Education Conf. (InSITE). Informing Science Inst., 2002

Prensky, M. (2001). On the Horizon. MCB University Press, Vol. 9 No. 5.

Reid, R.A., Thompson, J.K., & Logsdon, J.L. (1992). Knowledge and Attitudes of Management Students Toward Software Piracy. Journal of Computer Information Systems, 46-51.

Rogers, M., Smoak, N., & Liu, J. (2006). Self-reported deviant computer behavior. Deviant Behavior, 27(3), 245-268.

Roth, T., (2011). Breaking encryptions. Black hat conference 2011, Retrieved april 12, 2011, from https://media.blackhat.com/bh-dc-11/Roth/BlackHat_DC_2011_Roth_Breaking%20encryptions-Slides.pdf

Sterling, B. (1993). The Hacker crackdown: Law and disorder on the electronic frontier. USA: Mass Market Paperback.

Trend Micro (2009). Brits Breeding the Next-Generation of Computer Hackers. Retrieved january 06, 2011, from http://www.globalsecuritymag.com/Trend-Micro-Brits-Breeding-the,20090403,8329

Tufin Technologies, (2010). Survey of hacking habits in New York. Retrieved january 06, 2011, from http://www.tufin.com/news_events_press_releases.php?index=2010-04-14

Wall, D. (2001). Cybercrimes and the internet. In D. Wall (ed.) Crime and the internet. London: Routledge.

Wall, D.S. (2007). Cybercrime: The Transformation of Technology in the Networked Age. Cambridge: Polity Press.