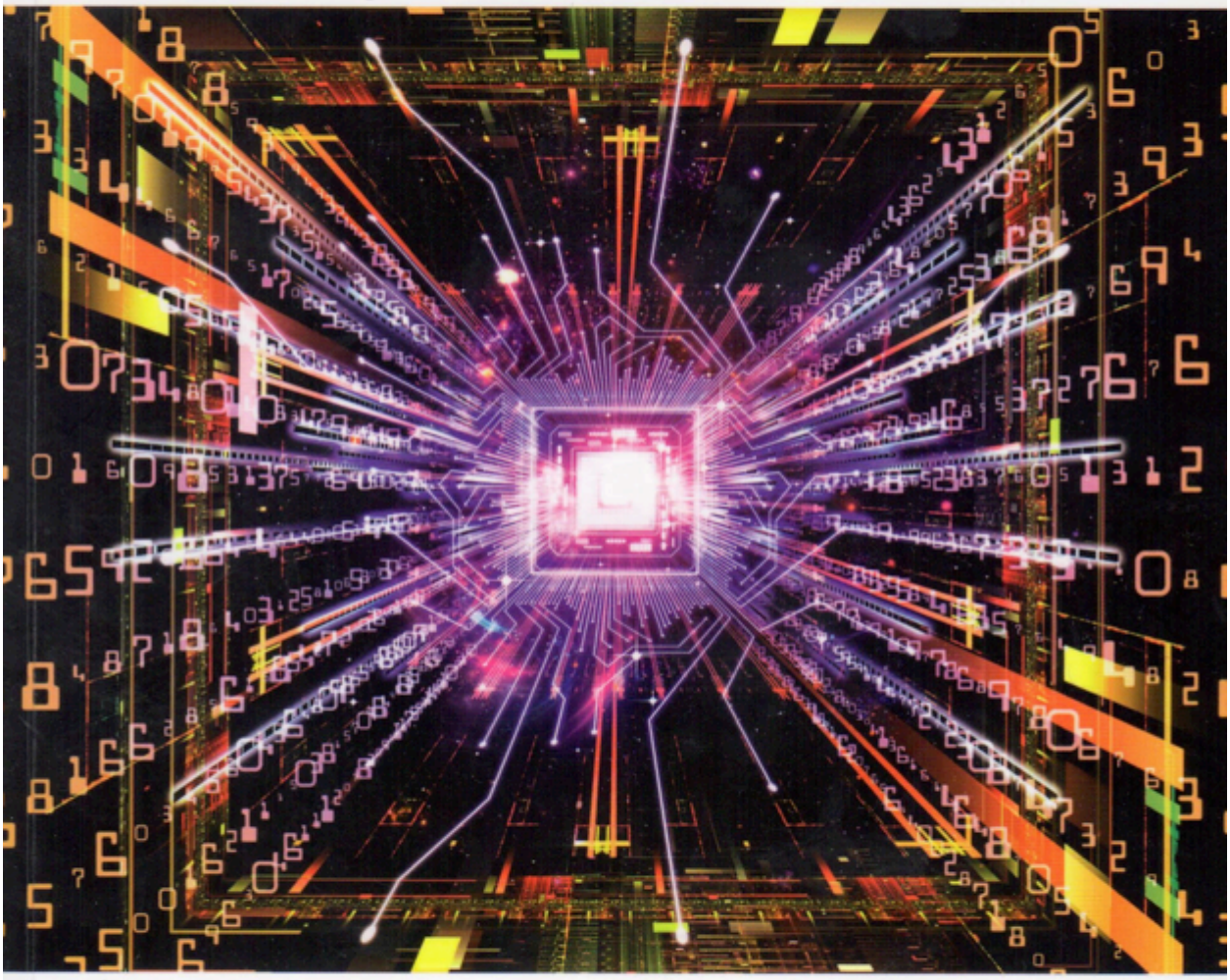
11
DÉCEMBRE 2012 /FÉVRIER 2013

Sécurité & Stratégie



LES CYBER-MENACES : MYTHE OU RÉALITÉ ?

- L'univers des hackers décrypté de l'intérieur
- La cyber-guerre : un fantasme qui fait vendre ?
- La cyber-résilience des entreprises mise à rude épreuve

Cybercriminalité et expertise : enjeux et défis

Franck Guarnieri & Eric Przyswa

Analyses et statistiques relatives à la cybercriminalité prolifèrent depuis quelques années. Pour autant, rares sont les études qui posent un regard critique sur ces « expertises ». Franck Guarnieri, directeur du Centre de recherche sur les Risques et les Crises de Mines ParisTech, et Eric Przyswa, chercheur dans ce même Centre, suggèrent de remédier à cet écueil en étudiant les différents biais créés par « l'expertise » en matière de cybercriminalité. Ils discutent la qualité des sources d'information privées ou publiques et le poids excessif du juridique dans les expertises. Les auteurs défendent l'idée que la cybercriminalité s'apparente davantage à une construction sociale complexe, permettant d'entretenir un climat de méfiance permanente, plutôt qu'à un phénomène clairement repéré et analysé. Ils en déduisent un certain nombre de pistes d'amélioration, plaidant notamment pour que des expertises multidisciplinaires se mettent en place avec de nouvelles approches en termes d'anticipation et de résilience.

La cybercriminalité a pris une part croissante dans le débat public et médiatique sous le double effet de l'accessibilité d'Internet offerte à de nouvelles populations et surtout de la globalisation des échanges. Le phénomène cybercriminel ne se résume donc plus à des actes isolés, anecdotiques ou spectaculaires, et la cybercriminalité est désormais souvent considérée comme un risque sécuritaire majeur par la plupart des experts. Pourtant, la question même de cette expertise est rarement posée et ce déficit de distance critique est pour le moins anachronique si l'on en juge par l'importance médiatique du phénomène. Cet article s'attachera donc à poser les enjeux liés à l'expertise dans le domaine de la cybercriminalité notamment en s'appuyant sur le cas de la contrefaçon de biens physiques qui permet d'étayer notre réflexion sur un territoire repéré. En effet, le discours sur la contrefaçon est plus ancien et éclaire la cybercriminalité de manière plus accessible[1]. La contrefaçon de supports physiques met enfin en relief les tensions existant entre les expertises du monde « *réel* » et du monde « *virtuel* ».

Dans une première partie nous apprécierons dans quelle mesure la plupart des expertises en cybercriminalité pose problème. Puis nous verrons comment ces expertises sont liées à un problème de cadrage du phénomène et à une construction sociale du risque. Nous proposerons enfin quelques pistes pour améliorer les expertises en question.

1 F. Guarnieri & E. Przyswa, « Cybercriminalité - contrefaçon : les interactions entre « réel et virtuel », Cahiers de la sécurité n° 15, 2011.

Etat des lieux de la pratique de l'expertise

Avant toute chose, il convient de préciser que la cybercriminalité est un concept récent et que les experts impliqués sur ce champ ont par conséquent une expérience forcément limitée. Pourtant, ces mêmes experts jouent un rôle majeur dans l'analyse de ce phénomène émergent en particulier car la cybercriminalité peut être assimilée au « *concept d'ennemi désétatisé et déterritorialisé* »[2], ce qui rend ces derniers ou les « *organes de perception* »[3] d'autant plus stratégiques dans le décryptage du phénomène.

Trois enjeux sont particulièrement stratégiques pour cerner cette problématique d'expertise : la question des sources des études, l'importance du juridique et la faible présence de recherche académique ou *think tanks* sur le sujet.

La plupart des études ou rapports sur le phénomène de lutte contre la cybercriminalité (en relation avec la contrefaçon) sont issus de deux sources principales, l'une émane du secteur privé, l'autre du secteur institutionnel. Au sein du secteur privé, on peut distinguer les études de sociétés directement impliquées dans la sécurité des systèmes d'information (les concepteurs de logiciels Symantec, McAfee, Kaspersky...) et celles issues des sociétés de veille sur Internet (MarkMonitor, OpSec Security...) plus orientées sur des aspects liés à la contrefaçon. Les études en question peuvent être conduites pour des missions *ad hoc* dans un cadre confidentiel ou bien dans un cadre public. Elles constituent alors une publicité ambiguë pour les entreprises qui les publient.

Si certaines études, en particulier issues de MarkMonitor[4], semblent présenter une crédibilité en termes d'analyse, il reste difficile de vérifier les sources de leurs investigations. Le cas des statistiques plus globales des concepteurs de logiciels posent davantage problème car elles se positionnent comme des analyses quasi officielles sur le phénomène cybercriminel et sont généralement reprises telles quelles par les médias[5]. Dans le secteur institutionnel, l'OCDE[6] et l'ENISA[7] publient ponctuellement des rapports sur le thème de la sécurité des systèmes d'information. Les études publiées, qui n'abordent pas le cas de la contrefaçon, restent soumises à un poids politique (ou bureaucratique) ne pouvant garantir la qualité académique escomptée pour de tels travaux.

Pour ce qui est de la prédominance du juridique, il ne s'agit pas ici de remettre en cause l'importance du droit, à la fois dans la définition de la cybercriminalité mais aussi comme outil d'aide à la répression, mais de constater que certains juristes se positionnent comme des experts en cybercriminalité *stricto sensu*. On peut sérieusement émettre l'hypothèse d'une captation du secteur juridique sur le marché de la cybercriminalité qui aurait pour effet d'engendrer une complexification grandissante du droit dans ce domaine. Cette captation s'opère moins dans le but de lancer une lutte efficace que de créer et pérenniser des situations de rente d'expertise juridique. La question peut se poser de savoir si les procès coûteux et à répétition entre LVMH et Google[8] n'auraient pas pu être évités sans le recours automatique et simplificateur au droit. Force est de constater que

2 *Expression d'U. Beck, Pouvoir et contre-pouvoir à l'heure de la mondialisation, Flammarion Champs Essais, 2009.*
3 *Ibidem.*
4 *MarkMonitor, Brandjacking Index, été 2009.*
5 *On peut penser aux informations régulièrement relayées par les médias accidentaux qui nous annoncent un Pearl Harbour électronique, avec un « bug géant » du réseau Internet, depuis une vingtaine d'années...*
6 *OCDE, OECD Conference on empowering e-consumers: strenghtening consumer protection in the Internet economy, Summary of key points and conclusions, 23 avril 2010.*
7 *ENISA, Annual Incident Reports 2011, octobre 2012.*
ENISA : The European Network and Information Security Agency est une agence européenne créée en 2004, basée en Crète, qui a pour objectif d'améliorer la cyber- sécurité au sein de l'Union européenne. Parmi les think tanks qui s'intéressent de près aux problématiques de cyber- sécurité on peut citer le RAND Corporation à Santa Monica en Californie et le Center for Strategic and International Studies (CSIS) de Washington D.C.
8 *En 2006 des marques sous l'impulsion de LVMH ont en effet commencé à lancer des procès à des sites d'envergure et plus généralement « de nombreuses actions ont été tentées contre les ventes frauduleuses réalisées grâce aux fournisseurs d'accès (...), notamment aux États-Unis, en France ou en Allemagne ». P. Collier, « Spécial Internet : Fin de l'immunité pour les opérateurs techniques ? », Contrefaçon Riposte, n° 18/19, oct. nov. 2006.*

les juges s'orientent par ailleurs de plus en plus vers des décisions à l'amiable entre les acteurs, une solution qui aurait pu être mise en place plus en amont. Sur un plan académique on peut relever la faiblesse des recherches à une échelle internationale : il n'existe pas à proprement parler de centre de recherche universitaire directement ou indirectement dédié aux enjeux de cybercriminalité selon une approche pluridisciplinaire en sciences humaines et sciences sociales. On peut d'ailleurs remarquer que les meilleures universités américaines orientent leurs recherches concernant Internet sur un axe en grande partie juridique. Les deux plus célèbres départements américains (le « *Center for Internet and Society* » de Stanford University et le « *Berkman Center* » de Harvard University) sont tous deux hébergés au sein de la faculté de droit. Dans le meilleur des cas, les centres de recherche universitaire ou encore les *think tanks* abordent Internet sur des problématiques liées aux libertés civiles.

Il n'existe pas à proprement parler de centre de recherche universitaire directement ou indirectement dédié aux enjeux de cybercriminalité.

Confronté à ce déficit analytique, un grand nombre de chercheurs vont jusqu'à considérer que la cybercriminalité a abouti à une forme d'impasse scientifique car la notion de cybercriminalité procèderait davantage « *d'impératifs commerciaux, de nécessités politiques et d'une panique morale nourrie par une mauvaise compréhension du fonctionnement et des possibilités de l'informatique réseautée, (plutôt) que d'une réflexion rationnelle* »[9]. Point de vue radical ? En tout état de cause, il y a manifestement un déficit en termes de controverse d'expertise même sur le plan technique.

De la difficulté de cerner les champs d'expertise

Les obstacles pour bien décrypter les enjeux en cours et une faible mobilisation d'expertises transversales rendent ces champs d'expertise difficiles à cerner. Face aux nombreuses incertitudes qui ne permettent pas de définir de manière standardisée et claire l'étendue du cyber-risque, celui-ci se situe en permanence entre « *fiction et réalité* ». Dans ce « *vertige de la réalité* » la frontière entre la fiction sur la cybercriminalité (ce qui pourrait se passer) et la réalité du phénomène (ce qui se passe) est brouillée[10]. Résultat : les nouvelles des médias sur chaque affaire de cybercriminalité favorisent par leur succession rapide des paniques morales déconnectées en grande partie de la réalité du phénomène[11]. Ces phénomènes médiatiques, relais privilégiés de certaines expertises, tendent à poser en permanence des problèmes de cadrage, d'autant qu'il y a dans de nombreux médias une forte tendance à utiliser une rhétorique dramatique et des signaux alarmistes sur ce thème. La focalisation médiatique sur la menace cybercriminelle chinoise et le déficit patent d'informations sur les cyber-attaques occidentales (en particulier américaines) est révélatrice de cette dramaturgie « *pré-orientée* ».
Il est également important de relever que cette captation du débat par certains experts (juri-

[9] S. Leman-Langlois, « Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial », Criminologie, vol. XXXIX, n° 1, printemps 2006.
[10] Sur le brouillage des frontières lire F. Guarnieri & E. Przyswa, « Cybercriminalité et contrefaçon : pour une nouvelle analyse des risques et des frontières », Murs et frontières, Hermès, n°63, 2012.
[11] D. Garland, « On the concept of moral panic », Crime, Media, Culture, vol. IV, n° 1, avril 2008.

diques, informatiques) est également facilitée par la faiblesse des compétences de la plupart des décideurs politiques sur le sujet des nouvelles technologies de l'information. Ce déficit d'intérêt pour le sujet laisse la possibilité à des groupes de pression de placer sur l'agenda des thèmes à leur avantage. Cette dérive est révélatrice des mutations du capitalisme contemporain où « l'*expertise peut désormais être considérée comme une ressource qui alimente un marché de travailleurs du savoir qualifiés, et non plus simplement une ressource contrôlée par une communauté professionnelle* »[12]. En d'autres termes, la cyber-sécurité offre donc toute une panoplie de menaces au service d'experts en tous genres, juristes mais aussi écrivains, journalistes, experts à la compétence technique limitée. Le sujet reste donc en grande partie « *dans le champ des professionnels de la gestion des inquiétudes* » qui émerge d'une « *déconstruction de la frontière* » entre « *le savoir sur l'interne et le savoir sur l'externe* » et d'une « *dé-différenciation des questions de sécurité intérieure et extérieure* ».[13] Les cyber-attaques d'avril 2007 en Estonie entrent dans cette catégorie car les enjeux de sécurité intérieure (blocage temporaire des systèmes d'information) ont aussi eu des impacts géopolitiques réels notamment avec une relative résurgence d'une rivalité Occident / Russie en arrière-plan de ces événements qui ont laissé libre cours à nombre de discours approximatifs autour du cyber-risque. Ces « expertises » en cyber-risque se caractérisent aussi par un brouillage des frontières car des experts en cybercriminalité peuvent s'improviser *de facto* compétents en cyber-terrorisme et cyber-guerre, concepts qui posent des enjeux et des problématiques pour le moins différents. Le cas américain est sans doute le plus extrême dans sa capacité à déplacer et à multiplier les discours sur la menace cybercriminelle notamment avec des axes sécuritaires ou géopolitiques. Cette tendance s'explique par le fait que des experts de la guerre froide (surtout issus du nucléaire et de la RAND Corporation[14]) ont dû se reconvertir avec la chute du mur de Berlin. À la suite de la publication d'un célèbre article d'Arquilla et Ronfeldt[15] sur la cyber-guerre, le thème du cyber-risque est alors devenu porteur sur le plan de l'expertise.

Plus généralement, on peut enfin s'étonner que des expertises véritablement transversales sur ces sujets ne se soient pas davantage mises en place. La complexité technique des défis peut être une explication mais on peut également poser l'hypothèse qu'une démarche véritablement transversale remettrait en cause la pérennité de certains réseaux d'expertises. Sur ce point, les approches en termes de champ d'expertise[16] peuvent se révéler stimulantes pour mieux comprendre les rapports de force en jeu : « *l'analyse en termes de champ a l'avantage de mettre l'accent sur les relations et en quelque sorte de déterminer les frontières significatives des réseaux. Elle permet d'éviter certaines formes d'illusions individualistes, et de réduire par exemple l'analyse des réseaux à l'analyse de multiples trajectoires individuelles, voire à la possession de carnets d'adresses (...). Ce qui importe dans la démarche, c'est de mettre l'accent sur les relations objectives aux autres positions, sur les "écarts" distinctifs entre ces positions et sur l'intérêt des agents à jouer le même jeu.* »[17]

Pourtant, même si le problème est mal cerné et mal cadré, il reste réel et sans doute croissant. Par conséquent, des initiatives en termes d'expertises s'imposent.

[12] *S. Brint, In an Age of Experts. The Changing Role of Professionals in Politics and Public Life, Princeton, Princeton University Press, 1994.*
[13] *Citations de D. Bigo, « La mondialisation de l'(in)sécurité ? Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d'(in)sécurisation », Cultures & Conflits, n° 58, été 2005.*
[14] *La RAND Corporation est un think tank américain de premier plan, réputé proche du lobby militaire et souvent en pointe dans ses réflexions sur les nouvelles technologies. www.rand.org*
[15] *J. Arquilla, & D. Ronfeldt, « Cyberwar is coming! », Comparative Strategy, vol. XII, n° 2, printemps 1993.*
[16] *D. Bigo, « La mondialisation de l'(in)sécurité ? Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d'(in)sécurisation », Cultures & Conflits, n° 58, été 2005.*
[17] *Ibidem.*

Quelques pistes pour améliorer l'expertise

Si l'on exclut les solutions pour le moins utopiques (une gouvernance mondiale d'Internet se coordonnant avec des problématiques industrielles) ou trop radicales (la fin de la « *neutralité* » d'Internet en vue de « *sécuriser* » les trafics mais à quel coût pour les libertés individuelles...), les expertises doivent alors se penser dans un environnement qui restera instable. Il faudra apprendre à penser et gérer des tensions entre un monde « *physique* » et un monde « *virtuel* » ainsi que de nouvelles relations avec les sociétés leaders d'Internet et les pays émergents, souvent à l'origine des produits contrefaits, pour s'orienter sur des solutions plus pragmatiques.

Une bonne approche doit avant tout éviter les remèdes trop simplistes déclinant une conception du monde « *physique* » sur le monde « *virtuel* ». Les deux environnements sont particulièrement liés et il importe d'avoir une vision holistique des défis qui intègrent le risque Internet avec d'autres types de flux, financiers ou logistiques, trop souvent absents des débats publics. Il convient donc pour les organisations victimes de cybercriminalité liée à des trafics illicites de faire preuve à la fois d'anticipation et d'adaptation face à ces nouveaux défis mais aussi de se préparer à des situations de crise. La mise en place de nouvelles formes de forums et d'expertises s'avère également nécessaire.

L'anticipation doit passer par un rapprochement entre acteurs industriels et issus d'Internet le plus en amont possible des risques émergents. En termes d'adaptation, ces entreprises ne doivent pas se réfugier de manière frontale et simplificatrice derrière des outils juridiques en particulier liés à la propriété intellectuelle et des outils de veille devraient notamment être développés lors du lancement de nouveaux produits.

Les meilleurs efforts d'anticipation et d'adaptation ne peuvent toutefois éviter des situations de crise en particulier sur un réseau aussi flexible qu'Internet. L'instabilité doit donc aussi être considérée comme un « *ordre normal* » même si les entreprises considèrent la situation comme « *non acceptable* ». Elles doivent aussi se projeter dans un temps long en « *acceptant la perspective de situations critiques durablement dégradées* »[18]. Dans un tel environnement d'instabilité il s'agit « *moins de faire face* » que d'être vigilant dans ces situations en se préparant avec une gestion régulière de la sécurité. Cette résilience, qui peut *a priori* avoir une efficacité certaine sur le réseau par définition résilient qu'est Internet, doit aussi se concevoir dans le réel car, comme nous l'avons vu, une approche holistique est essentielle à la fois pour ne pas « *s'épuiser* » à pourchasser chaque contrefacteur sur la toile mais aussi en impliquant toujours le « *monde physique* » dans les analyses.

Penser cette résilience est un vaste défi qui va au-delà des spécialistes de la cybercriminalité (ou de la contrefaçon) et implique aussi la mise en place de « *forums hybrides* »[19] qui visent à une co-production des connaissances en particulier entre scientifiques (ou ingénieurs) et acteurs politiques. Il est donc essentiel que ces forums trouvent des champs d'expression et que des informations crédibles même parcellaires puissent appuyer leur démarche car nous avons aussi pu constater dans quelle mesure des expertises peu fiables pouvaient potentiellement orienter le débat public de manière problématique. Dans le contexte d'un terrain instable, des experts illégitimes trouveront

[18] *C. Gilbert, Conférence Mines ParisTech : De la gestion des risques à l'organisation de la résilience. Implications d'un changement de perspectives, 7 juin 2011.*
[19] *Y. Barthe, M. Callon & P. Lascoumes, « Réponse à Franck Aggeri », Gérer et comprendre, n° 68, juin 2002.*
[20] *B. Dupont & V. Gautrais, « Crime 2.0. le web dans tous ses états », Nouvelle revue internationale de criminologie, Vol. VII, 2010.*

de nombreuses opportunités pour utiliser le débat public à leur seul avantage en employant la technique marketing du FUD[20] : *fear, uncertainty, doubt*. Il est peu probable que des experts légitimes puissent venir du champ criminologique classique car « *la criminologie qui semble idéalement positionnée pour déployer ses cadres théoriques et ses outils méthodologiques afin d'analyser la cybercriminalité a bien du mal à appréhender les déviances observées dans un univers numérique* »[21]. Quant aux chercheurs en informatique ils restreignent leur réflexion aux aspects techniques et négligent souvent les aspects sociaux. Enfin, l'expertise juridique gardera de sa pertinence si elle arrive à s'adapter à la flexibilité d'Internet. Des chercheurs en droit novateurs et capables d'une distance critique sur leur discipline devraient donc être davantage mobilisés. En résumé, un forum hybride devrait aider à faire émerger des spécialistes crédibles sur ces sujets encore émergents.

Mais la résilience des organisations, les forums hybrides ou encore de nouvelles expertises ne seront pas suffisants. Il importe aussi d'avoir des experts « *lanceurs d'alerte* » au sein du débat public car le discours actuel est pour le moins monolithique malgré une floraison de propos sur la cybercriminalité très rarement étayés par des éléments objectifs et rationnels. Au-delà d'un message alternatif plus proche des enjeux réels, il est également important d'adapter l'information sur les risques en fonction des publics (politiques, consommateurs, jeunes adeptes du numérique...). Il a en effet été démontré à quel point « *les modalités d'appréhension des dangers, comme leur hiérarchisation, diffèrent grandement selon la structure des groupes sociaux et les réseaux d'obligations particulières dans lesquels les individus sont insérés* »[22]. Ceci implique donc une information « experte » adaptée en fonction de certains groupes sociaux, ce qui n'est manifestement pas le cas aujourd'hui dans le cadre de notre problématique.

Conclusion

Pour la qualité du débat public et une meilleure transparence, il importe que des centres de recherche indépendants se positionnent sur des analyses liées aux technologies de l'information car il y a un réel déficit de recherche dans un cadre académique transversal pourtant incontournable[23]. Par ailleurs, les problèmes restent peu posés par des experts dans une perspective dynamique de réseaux transnationaux « *réel* » et « *virtuel* » qui devrait être la grille d'analyse centrale du binôme « *cybercriminalité - contrefaçon.* »[24] En ce qui concerne les entreprises, nous avons vu que d'une manière générale l'anticipation, un rapprochement entre acteurs industriels et acteurs issus de la société de l'information en amont des enjeux, ainsi que la mise en place d'une organisation résiliente seront les meilleures parades au risque cybercriminel à court et moyen termes. ■

Franck Guarnieri, directeur du Centre de Recherche sur les Risques et les Crises de Mines ParisTech
& Eric Przyswa, chercheur dans ce même Centre

Bibliographie

J. Arquilla, & D. Ronfeldt, « Cyberwar is coming! », Comparative Strategy, vol. XII, n° 2, printemps 1993.

[21] *Ibidem., « Lors de la dernière conférence annuelle de la Société américaine de criminologie (Saint-Louis 2008) qui constitue le plus important rassemblement mondial de chercheurs dans cette discipline et a réuni près de 2 000 participants, l'ensemble des communications portant sur les crimes technologiques, les crimes informatiques et les crimes reliés à Internet représentaient exactement 1% des contributions. »*

[22] *Y. Barthe & C. Lemieux, « Les risques collectifs sous le regard des sciences du politique. Nouveaux chantiers, vieilles questions », Politix, n° 44, 1998, p. 23.*

[23] *P. Sommer & I. Brown, « Reducing Systemic Cybersecurity Risk », Organisation for Economic Cooperation and Development. Working Paper n° IFP/WKP/FGS 3, 2011.*

[24] *E. Przyswa, Cybercriminalité-Contrefaçon, FYP, 2010.*

2• La cyber-guerre : un fantasme qui fait vendre ?

Y. Barthe & C. Lemieux, « Les risques collectifs sous le regard des sciences du politique. Nouveaux chantiers, vieilles questions », Politix, n° 44, 1998.

Y. Barthe, M. Callon & P. Lascoumes, « Réponse à Franck Aggeri », Gérer et comprendre, n° 68, juin 2002.

U. Beck, Pouvoir et contre-pouvoir à l'heure de la mondialisation, Flammarion Champs Essais, 2009.

D. Bigo, « La mondialisation de l'(in)sécurité ? Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d'(in)sécurisation », Cultures & Conflits, n° 58, été 2005.

S. Brint, In an Age of Experts. The Changing Role of Professionals in Politics and Public Life, Princeton, Princeton University Press, 1994.

P. Collier, « Spécial Internet : Fin de l'immunité pour les opérateurs techniques ? », Contrefaçon Riposte, n° 18/19, oct. nov. 2006.

B. Dupont & V. Gautrais, « Crime 2.0. le web dans tous ses états », Nouvelle revue internationale de criminologie, vol. VII, 2010.

ENISA, Annual Incident Reports 2011, octobre 2012.

D. Garland, « On the concept of moral panic », Crime, Media, Culture, vol. IV, n° 1, avril 2008.

C. Gilbert, Conférence Mines ParisTech : De la gestion des risques à l'organisation de la résilience. Implications d'un changement de perspectives, 7 juin 2011.

F. Guarnieri & E. Przyswa, « Cybercriminalité - contrefaçon : les interactions entre 'réel et virtuel' », Cahiers de la sécurité n° 15, 2011.

F. Guarnieri & E. Przyswa, « Cybercriminalité et contrefaçon : pour une nouvelle analyse des risques et des frontières », Murs et frontières, Hermès, n° 63, 2012.

S. Leman-Langlois, « Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberespace commercial », Criminologie, vol. XXXIX, n° 1, printemps 2006.

MarkMonitor, Brandjacking Index, été 2009.

OCDE, OECD Conference on empowering e-consumers: strenghtening consumer protection in the Internet economy, Summary of key points and conclusions, 23 avril 2010.

E. Przyswa, Cybercriminalité-Contrefaçon, FYP, 2010.

P. Sommer & I. Brown, « Reducing Systemic Cybersecurity Risk », Organisation for Economic Cooperation and Development. Working Paper n° IFP/WKP/FGS 3, 2011.