Les motivations des cybercriminels

par **Faten SKAF***

Résumé
Pour que le crime soit possible, divers facteurs doivent être présents, notamment le facteur motivationnel du cyberdélinquants. La motivation est l'élément principal à la base de ces occasions criminelles et est jugée comme étant un élément discriminatoire très utile pour comprendre la cybercriminalité. Effectivement, s'il n'y avait pas un mobile poussant un délinquant à agir, la criminalité n'existerait pas.
Tout comme la criminalité informatique, les motivations des cybercriminels sont multiformes. Le cybercriminel ne constitue pas une catégorie d'individus clairement définie et les motifs d'une attaque informatique sont aussi variés qu'il existe de types de cybercriminels. Les motivations qui poussent des individus à prendre illégalement le contrôle de systèmes informatiques appartenant à autrui sont diverses. Quelques uns sont motivés par le besoin de reconnaissance de soi et les autres sont motivés par la volonté d'accéder à une reconnaissance sociale. Mais, ces motivations des fraudeurs n'ont pu être suscitées qu'en raison de l'existence d'un environnement favorable à la délinquance informatique (1).

Mots-clés: pirate informatique, criminel informatique, mobile, motivation, cible, cybercriminel, cyberdélinquant, cybermenaces, attaques informatiques, cybercriminalité.

Summary
For the crime to be possible, various factors must be present, including the motivational factor of the cyber offender. Motivation is the main element underlying these criminal opportunities and is seen as a very useful discriminatory element in understanding cybercrime. Indeed, if there were no motive for an offender to act, there would be no crime.
Like computer crime, the motivations of cybercriminals are multifaceted. The cybercriminal is not a category of clearly defined individuals and the motives for a cyber attack are as different as there are types of cybercriminals. The motivations that lead people to illegally take control of computer systems owned by others are diverse. Some are motivated by the need for self-recognition and others are motivated by the desire to access social recognition. But these motivations of fraudsters could only be aroused because of the existence of an environment favorable to delinquency computer.

Keywords: hacker, computer criminal, mobile, motivation, target, cybercriminal, cyber offenders, cyber threats, computer attacks, cybercrime.

1. Les mobiles relatifs à une reconnaissance de soi

Il est toujours difficile de connaître les motivations d'un acte, même si ces dernières telles que le besoin de reconnaissance, l'admiration, la curiosité, le pouvoir, l'argent et la vengeance sont le plus souvent moteur dans des actes délictueux. Il est cependant utile de chercher à les comprendre pour mettre en place des stratégies et des tactiques de réponses adaptées (2).

*Docteur en droit privé et sciences criminelles, Université d'Aix-Marseille.

1.1 La motivation sociale

La motivation sociale trouve ses racines dans le besoin de reconnaissance de l'individu par ses pairs, lié généralement à une structure de bande. Emulation collective, psychologie d'appartenance, chacun veut prouver sa valeur au groupe en se référant aux critères culturels internes (3). Pour mettre en lien le mobile intérieur avec le mobile comportemental, ce qui est paradoxal est que le réseau développé par le cybercriminel au sein du cyberespace sera important alors que dans le monde réel il subit une exclusion sociale.

1.1.1. Les mobiles interpersonnels

Les mobiles interpersonnels démontrent la tendance vers laquelle le cybercriminel justifie son acte au travers du cyberespace. Les mobiles interpersonnels se diviseraient en mobile ludique, curiosité et vengeance expliquant le passage à l'acte:

Ludique

Les attaquants sont motivés par le goût du jeu, de l'aventure, le sentiment de puissance face à un instrument sophistiqué; ils cherchent à démontrer la fragilité d'un système et se recrutent parmi de jeunes informaticiens n'ayant pas conscience de commettre un acte répréhensible (4) et qui cherche sans cesse à étendre ses connaissances dans ce domaine (5).

La curiosité

La soif de la connaissance et le désir d'explorer de nouvelles compétences sont à l'origine de l'apparition du phénomène de hacking. L'intrusion sur les réseaux et le détournement des systèmes ne sont que l'incarnation de cette curiosité qui développe chez certain nombre d'acteurs de l'univers underground notamment les *white hat hackers*, cette capacité à résister à toute épreuve. Cette caractéristique les conduit à consacrer temps et effort à l'exploration des limites des systèmes ciblés. La curiosité justifie pour de nombreux acteurs de l'univers underground le passage à l'acte de déviance dans le cyberespace (6). Cette attitude renvoie souvent au célèbre pirate Kevin MITNICK qui a toujours affirmé que sa motivation principale était la curiosité (7).

Les vandales sont motivés par le plaisir de la destruction des systèmes informatiques ou des sites Internet dont le seul but est de causer un dommage. Il s'agit donc de la réaction d'une personne en réponse à une frustration quelconque et qui n'a d'autre but que de détruire tout ou partie d'un système informatique ou de données pour infliger un coup préjudiciable à l'adversaire (8). Les vengeurs sont le plus souvent des anciens employés en sécurité informatique ressentant le besoin de se venger en essayant de rationaliser leurs actes. Ils peuvent s'en prendre à une entreprise mais aussi à une personne en la harcelant ou la manipulant (9). Ces employés utiliseront leurs codes d'accès pour voler des informations importantes à leur ancienne entreprise, à titre d'exemple, un ancien employé d'une société de services de santé fut poursuivi pour avoir effacé une bonne partie des bases de données de son ancien

employeur. À l'aide d'une bombe logique, un logiciel malveillant configuré dans le but d'exploser en causant l'effacement des données systèmes, l'homme pu ainsi infliger de graves dommages à la base de données gérant les médications de patients (10).

1.1.2. Les mobiles de nature financière

L'appât du gain constitue la motivation la plus répandue chez les criminels informatiques (11). Les cas ne manquent pas, et sont généralement les plus médiatisés, que ce soit aux États-Unis ou en Europe. Le dénominateur commun à tous ces cas est généralement la découverte d'une faille dans un système informatique qui sera utilisée pour s'approprier un profil financier direct (par exemple dans le cas du détournement de fonds) ou indirect (par exemple dans le cas du détournement d'informations ou de l'espionnage économique). Le gain financier comme motivation du crime informatique (12) répond aux principes de la théorie économique: il s'agira, pour le pirate informatique, de maximiser ses gains et de minimiser ses contraintes et ses risques. Le recours à l'informatique est judicieux car il permet, avec un minimum d'investissement personnel et financier d'obtenir des gains très importants.

Les cyberescrocs motivés par l'appât du gain correspondent à une délinquance à grande échelle, très organisée mais aussi très imaginative:

D'une part, toute la masse des escroqueries qui prennent des formes de plus en plus diverses pour convaincre l'internaute de commettre l'erreur qui lui sera fatale (le hameçonnage, l'escroquerie aux emplois d'appoint (c'est le cas du créateur du virus KOURNIKOVA qui s'est vu proposer du travail quelques heures seulement après son arrestation), le blocage avec demande de rançon, l'amende fictive à payer, l'escroquerie à la réservation de la chambre d'hôtel, l'escroquerie à la Nigériane ou à la fausse loterie, l'escroquerie sentimentale, le chantage à la «web-cam» et la plus lucrative d'entre toutes qui fait actuellement des ravages dans les entreprises françaises: l'escroquerie par faux ordres de virement);

D'autre part, les fraudes par cartes bancaires avec l'interception des données sur Internet, le skimming qui s'attaque aux distributeurs automatiques de billets, ou encore le piratage des terminaux de paiement chez les commerçants; mais aussi, les fraudes téléphoniques par détournement des services surtaxés et enfin tous les types possibles de contrefaçons liés à l'extension du commerce en ligne (contrefaçon de marques, de logiciels, de produits relevant de la propriété intellectuelle, de médicaments); sans oublier les jeux illégaux (13).

Il faut toutefois prendre aussi en compte les nombreux trafics qui prospèrent sur Internet, tel le florissant marché des drogues de synthèse ou le blanchiment du produit du crime.

1.2. Les mobiles variables

Les mobiles variables sont primordiaux car il n'existe pas qu'un seul profil de cyber agent mais une multitude causée par des différences d'intelligences et d'environnements entre les cybercriminels. Ces variations permettront de comprendre la singularité de chaque cyber délinquant.

1.2.1. Le mobile de l'intelligence virtuelle

Le jeu intellectuel constitue la motivation la plus connue parce qu'il apparaît généralement dans les cas médiatisés de pénétration de système ou de piratage de logiciels (14). Bien souvent, la différence entre le jeu et la recherche de profil est difficile à établir, si bien qu'on considère que ces motivations sont toutes les deux présentes.

L'aspect jeu ou défi intellectuel est présent dans la majorité des crimes informatiques ce qui s'explique par plusieurs raisons:

Tout d'abord, le hacker va trouver dans le jeu la reconnaissance sociale qui caractérise les hackers les plus doués. En effet, le jeu a toujours été synonyme de valeur, de courage et de volonté d'être (15).

Ensuite, il faut une certaine dose d'incertitude «*le jeu ne divertit plus celui qui, trop entraîné ou trop habile, gagne sans effort et infailliblement (….). il faut un renouvellement constant et imprévisible de la situation (…). Le jeu consiste dans la nécessité de trouver, d'inventer immédiatement une réponse qui est libre dans les limites des règles. Cette latitude du joueur (….) explique en partie le plaisir qu'il suscite*» (16). La contrainte joue également un rôle paradoxal. Si elle est librement acceptée dans le cadre du jeu, ce n'est pas le cas dans celui du travail. Par exemple les hackers qui se trouvent en situation d'échecs scolaires, les contraintes éducatives leur étant insupportables, contrairement à celles liées au piratage. Il faut en effet se plier aux règles de pénétration d'un système informatique, à commencer par la contrainte de trouver un mot de passe valable. Et si ces contraintes sont acceptées c'est parce qu'elles font appel à l'imagination et aux facultés d'adaptation du pirate, lui permettant ainsi de prouver toute son ingéniosité.

Enfin, une série de caractéristiques propres au joueur sont transposables aux criminels informatiques. Le joueur, c'est «*avant tout le défi, la compétition où il peut révéler un gagneur. Les lents et les prudents l'impatientent. Il aime prendre des risques et pousser les autres au delà de leur. allure normale. Il réagit au travail et à la vie comme à un jeu. La lutte le galvanise (…). Son principal but (….) c'est d'être un gagnant, et à chaque fois qu'on parle de lui, on aboutit à une discussion sur sa tactique et sa stratégie dans les luttes de l'entreprise (…). Il aime prendre des risques calculés*» (17).

Il existe aujourd'hui une intelligence virtuelle qui est «*la capacité d'évoluer dans un monde parallèle qui exige quelques ressources similaires aux autres familles d'intelligences (……), elle est la capacité de structurer, comprendre, concevoir, animer et développer un univers informatique technique, ayant un langage et des codes dédiés et de les intégrer dans le monde réel afin de créer un monde parallèle qui aboutira à un environnement avatarisé. Le potentiel des personnes dotées d'une intelligence virtuelle permet d'accéder à des univers différents en créant leurs propres codes ou en décryptant ceux qui existent sans avoir à les étudier*» (18). Cette intelligence se développe avec une culture axée sur tout ce qui touche au cyberespace.

1.2.2. Le mobile environnemental
Le mobile environnemental permet de comprendre la personnalité du cybercriminel. Le cybercriminel est considéré comme quelqu'un de sombre, ne prenant pas soin de sa personne et antisocial, ayant des aptitudes sociales défaillantes ou provenant de familles dysfonctionnelles. Le foyer du cyber agent est Internet. Le mobile environnemental du cybercriminel permet d'amener une justification géographique du passage à l'acte. C'est peut-être un mobile plus objectif mais c'est le cybercriminel qui s'approprie l'environnement dans lequel il vit, dans lequel il développe ses méthodes criminelles, d'une certaine manière il subjectivise les moyens qui sont à sa portée, c'est pourquoi son environnement est fait aussi de sa pensée et de sa culture.

2. La volonté d'accéder à une reconnaissance sociale

La récupération idéologique et politique de conflits amène inévitablement des groupes d'internautes à agir dans le cyberespace pour défendre leurs causes, leurs valeurs, leurs idéologies. La formation de ces groupes et leur implication dans les conflits peut entraîner des complications lors de résolution de crises diplomatiques et de sécurité.

2.1 Les motifs d'ordre idéologique et stratégique
L'attaque motivée par l'idéologique
L'idéologie vise à défendre une conviction (par exemple politique ou religieuse) à travers des attaques dont le but est d'interrompre des services à diffuser des messages partisans ou à divulguer les données d'une entreprise pour nuire à son image (19). Les hacktivistes sont des hackers dont la motivation est idéologique.

La motivation stratégique
La stratégie vise des informations concernant les secrets de défense et la sûreté de l'État, le patrimoine national (scientifique, technique, industriel, économique ou diplomatique), mais aussi la déstabilisation des systèmes dont dépendent ces informations, en effet, un état, des groupes organisés ou des entreprises, peuvent utiliser avec efficacité les faiblesses éventuelles des systèmes d'information afin de prendre connaissance d'informations sensibles ou confidentielles, notamment en accédant frauduleusement à des banques de données. L'attaque massive de systèmes vitaux d'un pays ou d'une entreprise afin de les neutraliser ou de les paralyser constitue une autre hypothèse. La désinformation et la déstabilisation sont des moyens très puissants et faciles à mettre en œuvre avec un effet multiplicatif dû à la dépendance vis-à-vis de l'information (20).

2.2. La cible de menace politique
La motivation politique consiste à créer un événement propre à alerter les médias pour les focaliser sur un problème grave, en espérant provoquer une

prise de conscience collective qui amènera sa résolution. Il est à noter alors que la frontière avec le terrorisme peut être ténue au moins d'un point de vue conceptuel. Il doit également souligner que bon nombre de personnes dissimulent leur motivation sociale derrière un objectif politique (21). Les principales motivations d'ordre politique sont l'hacktivisme et le cyberterrorisme.

2.2.1. L'hacktivisme

L'hacktivisme poursuit principalement des objectifs politiques. Certains objectifs peuvent être de nature économique mais la finalité est toujours politique. Les objectifs des hacktivismes peuvent être variés comme la destruction de sites pédophiles ou l'altération de sites prônant le racisme ou d'une manière plus générale le respect de la liberté d'information. Les actions des hacktivismes sont toujours très bien coordonnées, pouvant parfois nécessiter la contribution de plusieurs milliers d'internautes. Pour illustrer ce propos, un exemple de défacement (22), en janvier 2009, des hackers pro-palestiniens ont procédé au défacement de la version anglaise du site du grand quotidien israélien «Ynetnews.com». Les hackers avaient remplacé la page d'accueil habituelle du site, par des photos de guerre assorties du message politique suivant «*la seule solution pour que les Palestiniens, les Juifs, les musulmans comme les chrétiens, vivent en paix, est la fin de sionisme* (….) (23).

Le principal problème avec l'hacktivisme outre les dégâts qu'il peut causer, vient du fait que les hackers sont les seuls à juger, selon leur vision du monde, qui mérite d'être puni. Aux détracteurs de ce type d'actions qui évoquent l'illégalité et le manque de légitimité, les hacktivistes répondent qu'il s'agit d'un moyen de communications ou encore que ce n'est pas du hacking, c'est de la communication (24). D'ailleurs, la plupart des hacktivistes ne se considèrent pas comme des criminels mais bien comme des Robins des bois du réseau, défendant les pauvres contre les puissants (25).

2.2.2. Les motifs d'ordre terroriste

Les organisations terroristes ont recours à l'informatique pour stocker et transmettre les données relatives à leurs actions, ainsi que pour assurer la propagande relative à la cause qu'ils défendent (26). De plus, l'Internet est devenu une sorte de grand marché du terrorisme, où il peut trouver des sites expliquant en détails comment concevoir des bombes avec des produits facilement disponibles dans le commerce, comment réaliser des armes pour tuer, et même les meilleurs moyens techniques et juridiques pour contrecarrer les actions des autorités (27).

Il apparaît clairement que les motivations des hackers sont la conjonction de plusieurs facteurs comme dans toute forme de criminalité mais certains de ceux-ci se verront modifiés par la nature informatique du crime. C'est le cas de la distance séparant victime et auteur ou encore de la facilité de perpétration et de préparation de l'acte. Quelques soient leurs motivations, les délinquants informatiques ont toujours la possibilité de passer à l'acte, l'informatique diminuant fortement les contraintes spatiales et logistiques qui pourraient les décourager.

Dès lors, la connaissance des motivations des hackers par les autorités policières peut être utile, elle ne semble pas pour autant déterminante. Elle pourra donner des indications sur la personnalité du hacker ou du moins sur son *modus operandi* mais par contre, elle ne permettra pas toujours de déterminer si l'infraction est le fruit d'une personne seule ou si elle a été commise en groupe. Il pense que l'établissement de la motivation de l'auteur de l'infraction sera un élément parmi d'autres permettant d'aboutir à son arrestation mais non déterminant à lui seul.

Conclusion

Toute infraction suppose que son auteur ait agi avec intelligence et volonté. Dans le cyberespace, l'infraction est rarement commise de manière impulsive, elle est généralement le fruit d'une période de réflexion, durant laquelle le cybercriminel met en balance les intérêts qu'il peut retirer de son infraction et les risques qu'elle représente. Les cybercriminels disposent désormais d'une panoplie étoffée de méthodes et de modes opératoires pour réaliser des actes cybercriminels. Il est donc très important de connaître la diversité des attaques et des attaquants, d'identifier là où se trouvent les principales failles de sécurité. Mais deux des contraintes rencontrées dans les enquêtes sont l'anonymisation et la porosité croissante des réseaux sociaux dont le détournement est devenu un cheval de Troie privilégié des cybercriminels.

Bibliographie

BELLEFIN (L.), «Cybercriminalité: comment agir dès aujourd'hui», *les Synthèses SOLUCOM* n° 47, 2013, p. 4.

CAILLOIS (R.), *Les jeux et les hommes*, Gallimard, 1967.

CHATELAIN (Y.) et ROCHE (L.), *Hackers! le 5e pouvoir*, Paris, 2000.

CHAWKI (M.), *Combattre la cybercriminalité*, édition de Saint Amans, 2008.

CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John W. Rollins and Clay Wilson, 2007.

DUPONT (B.), «L'évolution du piratage informatique: De la curiosité technique au crime par sous-traitance», *Chaire de recherche technique du Canada en sécurité, identité et technologie*, Université de Montréal, 2010, p. 3.

EASTTOM (Ch.), *Computer crime, investigation, and the law*, Cengage Learning, 2011.

EL-AZZOUZI (A.), *La cybercriminalité au Maroc*, livre en ligne, 2010.

SKOPIK (F.), *collaborative cyber threat intelligence: Detecting and responding to advanced cyber attacks at the National level*, CRC Press, 16 octobre 2017.

https://www.solucom.fr/wpcontent/uploads/2013/10/Synthese_cybercriminalit%C3%A9_solucom-web.pdf.

HUMBERT (J.-Ph.), *Les mondes de la cyberdélinquance et images sociales du pirate informatique*, thèse, Université de Paul Verlaine, 2007.

JORDAN (T.) and TAYLOR (P.), "Sociology of Hackers", *Sociological Review*, volume 46 number 4, 1998, p. 757-81.

LALAM (N.), *La délinquance électronique: problèmes politiques et sociaux*, Documentation française, n° 953, octobre 2008.

LASBORDES (P.), *La sécurité des systèmes d'information- Un enjeu majeur pour la France*, La Documentation française, collection des rapports officiels, 2005, en ligne: http://securiteetinformatique.loria.fr/data/26_novembre_doc_definitif.pdf.

LATRIVE (F.) et DUFRESNE (D.), *Pirates et flics du Net*, SEUIL, 2000.

LWOFF (A.), «Le jeu et l'idée dans la création scientifique», *Science et Avenir*, mai 1976, p. 506 à 510.

MACCOBY (M.), *Le joueur*, Paris, InterEditions, 1980.

MARTIN (D.) et MARTIN (F.-P.), *Cybercrime: menaces, vulnérabilités et ripostes*, Presses Universitaires de France, Collection criminalité internationale, 2001.

PAINTER (C.), «Combattre le cybercrime: défis et perspectives, nécessité d'une coopération internationale», *Cahier de la sécurité* n° 6, 2008, p. 101.

ROBERT (M.), *Rapport du Groupe de travail interministériel sur la lutte contre la cybercriminalité: protéger les internautes*, février 2014, disponible sur le site: http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf.

ROSÉ (Ph.) et LAMERE (J.-M.), *Menaces sur les autoroutes de l'information*, Harmattan, 1996.

SOLANGE (G.-H.), *La cybercriminalité: le visible et l'invisible*, éditions Presses polytechniques et universitaires romandes, collection Le Savoir Suisse, 2009.

TOUZEAU (N.), *Net-profiling analyse du comportement des cybercriminels*, édition FRENCH, 2015.

Union internationale des télécommunications (ITU), *Guide de la cybersécurité pour les pays en développement*, UIT, édition 2007, en ligne: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-f.pdf.

«Premier fait d'armes des hackers pro-palestiniens», http://observers.france24.com, 2 janvier 2009.

Notes

1 B. DUPONT, «L'évolution du piratage informatique: De la curiosité technique au crime par sous-traitance», *Chaire de recherche technique du Canada en sécurité, identité et technologie*, Université de Montréal, 2010, p. 3.

2 P. LASBORDES, *La sécurité des systèmes d'information- Un enjeu majeur pour la France*, La Documentation française, collection des rapports officiels, 2005, p. 20, en ligne: http://securiteetinformatique.loria.fr/data/26_novembre_doc_definitif.pdf.

3 S. GHERNAOUTI-HÉLIE, *La cybercriminalité: le visible et l'invisible*, éditions Presses polytechniques et universitaires romandes, collection Le Savoir Suisse, 2009, p. 44.

4 N. LALAM, *La délinquance électronique: problèmes politiques et sociaux*, Documentation française, n° 953, octobre 2008, p. 6.

5 M. CHAWKI, *Combattre la cybercriminalité*, édition de Saint Amans, 2008, p. 78.

6 A. EL AZZOUZI, *La cybercriminalité au Maroc*, livre en ligne, 2010, p. 91; F. SKOPIK, *collaborative cyber threat intelligence: Detecting and responding to advanced cyber attacks at the National level*, CRC Press, 16 octobre 2017.

7 T. Jordan and P. Taylor, "Sociology of Hackers", *Sociological Review*, volume 46 number 4, 1998, p. 757-81.

8 J.-Ph. HUMBERT, *Les mondes de la cyberdélinquance et images sociales du pirate informatique*, thèse, Université de Paul Verlaine, 2007, p. 93.

9 N. TOUZEAU, *Net-profiling: analyse comportementale des cybercriminels*, édition FRENCH, 2015.

10 C. PAINTER, «Combattre le cybercrime: défis et perspectives, nécessité d'une coopération internationale», *Cahier de la sécurité* n° 6, 2008, p. 101.

11 S. GHERNAOUTI-HÉLIE, *La cybercriminalité: le visible et l'invisible*, op.cit., p. 44.

12 Ch. EASTTOM, *Computer crime, investigation, and the law*, Cengage Learning, 2011, p. 411.

13 M. ROBERT, *Rapport du Groupe de travail interministériel sur la lutte contre la cybercriminalité: protéger les internautes*, février 2014, p. 29, disponible sur le site: http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf.

14 Ph. ROSÉ et J.-M. LAMERE, *Menaces sur les autoroutes de l'information*, Harmattan, 1996, p. 217.

15 A. LWOFF, «Le jeu et l'idée dans la création scientifique», *Science et Avenir*, mai 1976, p. 506 à 510.

16 R. CAILLOIS, *Les jeux et les hommes*, Gallimard, 1967, p. 38.

17 M. MACCOBY, *Le joueur*, Paris, InterEditions, 1980, p.19 à 20 et 59 à 67.

18 N. TOUZEAU, *Net-profiling analyse du comportement des cybercriminels*, édition FRENCH, 2015.

19 L. BELLEFIN, «Cybercriminalité: comment agir dès aujourd'hui», *les Synthèses SOLUCOM* n° 47, 2013, p. 4, en ligne: https://www.solucom.fr/wpcontent/uploads/2013/10/Synthese_cybercriminalit%C3%A9_solucom-web.pdf.

20 P. LASBORDES, *Sécurité des systèmes d'information: un enjeu majeur pour la France*, la documentation française, 2006, p. 29.

21 Union internationale des télécommunications (ITU), *Guide de la cybersécurité pour les pays en développement*, UIT, édition 2007, p.35, en ligne: http://www.itu.int/ITU-D/cyb/publications/2007/cgdc-2007-f.pdf.

22 Ce mouvement est né avec le groupe de hacker «Cult of the dead cow» en 1994.

23 «Premier fait d'armes des hackers pro-palestiniens», http://observers.france24.com, 2 janvier 2009.

24 F. LATRIVE, D. DUFRESNE, *Pirates et flics du Net*, SEUIL, 2000, p. 55.

25 Y. CHATELAIN et L. ROCHE, *Hackers! le 5e pouvoir*, Paris, 2000, p. 57.

26 CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John W. Rollins and Clay Wilson, 2007.

27 D. MARTIN, F.-P. MARTIN, *Cybercrime: menaces, vulnérabilités et ripostes*, Presses Universitaires de France, Collection criminalité internationale, 2001, p. 69.