Revue d'Economie Théorique et Appliquée
Volume 2 – Numéro 2 – Déc. 2012 pp 155-176

Relecture de la rationalité du cybercriminel : quelques éléments d'analyse théorique[†]

Alastaire Sèna ALINSATO

Centre de Formation et de Recherche en Développement (CEFRED) – Université d'Abomey-Calavi.
Email : alastaires@yahoo.fr

Résumé : La présente étude propose une relecture du choix rationnel du criminel pour faire face à la cybercriminalité. L'étude montre, en analysant le marché de la cybercriminalité, l'inadéquation des mesures dissuasives conventionnelles reposant essentiellement sur trois caractéristiques à savoir la sévérité, la certitude et la célérité, dans la lutte contre la cybercriminalité. L'étude propose un model de lutte contre la cybercriminalité dans lequel le risque pour le cybercriminel lié à son activité, dépend de l'effort qu'il doit fournir ; cet effort dépend à son tour du niveau de protection des ordinateurs. L'étude montre que dans un tel système, la combinaison optimale des mesures de dissuasion-répression dépend du niveau d'élasticité de l'offre et de la demande des opportunités de cybercriminalité.

***Mots clés** : Cybercriminalité – choix rationnel – élasticité*
***Classification JEL** : D11 – D21 – D61*

Reviewing the rationality of cybercriminal: some theoretical analysis

Abstract: The study revisits the rational choice of the cybercriminal to fight cybercrime. Analyzing the cybercrime market, the study shows, the inadequacy of the conventional deterrence based on three main characteristics namely severity, certainty and promptness in the fight against cybercrime. The study proposes a model to control for cybercrime activities in which the risk for cybercriminal linked to his activity depends on the effort he must provide and this effort in turn depends on the level of computers protection. The study shows that in such a system, the optimum combination of deterrence and repression depends on the elasticity of supply and demand of cybercrime opportunities.

***Keywords** : Cybercrime – rational choice – elasticity*
***JEL Classification** : D11 – D21 – D61*

1. Introduction

Les préoccupations liées à la sécurité des ordinateurs et de l'information échangée via Internet ont reçu une attention soutenue ces dernières années au point où la cyber-sécurité est devenu une priorité pour plusieurs gouvernements, entreprises et organisations. Dans le cyberespace, tout le monde peut communiquer avec n'importe qui, n'importe quand et de n'importe où. Les utilisateurs (ménages, entreprises, organismes gouvernementaux, …) y côtoient virtuellement des acteurs malveillants de toute sorte. Internet est dès lors devenu un espace où le risque informatique d'origine criminelle est structurel, omniprésent et permanent.

Partout dans le monde et plus précisément en Afrique où la vitesse d'adoption des techniques de l'information et de la communication est la plus élevée sur la dernière décennie (CNUCED, 2008), l'économie numérique, bien que source incontestable de croissance économique et de création d'emploi, est de plus en plus mise à mal par la poussée exponentielle des actes de cybercriminalité. La cybercriminalité a fait perdre à l'Afrique 198,3 milliards de dollars en 2007 contre 20,5 milliards de dollars en 2003 ; soit une hausse de 90% en quatre ans[1]. Dans son classement des pays en termes d'origine des actes de cybercriminalité, le rapport du IC3, 2010[2] classe le Nigéria troisième juste après les Etats-Unis et la Grande Bretagne. Dans les dix premiers pays sur le plan mondial, on compte trois de l'Afrique Subsaharienne ; outre le Nigéria, le Ghana et l'Afrique du Sud viennent respectivement en 6ème et 7ème position. Les coûts associés à la cybercriminalité pour les victimes deviennent de plus en plus importants. Pour les pays qui sont dotés d'institutions de veille, de sécurité et de justice avec des compétences plus ou moins adaptées, résoudre un problème de cybercriminalité entraine un coût moyen de 334 US$ et 28 jours de formalités et d'investigation Norton (2010). Ces coûts monétaires et d'opportunité sont susceptibles d'être plus importants en Afrique subsaharienne où les institutions de sécurité et de justice sont très approximatives.

Le monde en général et l'Afrique en particulier est donc ainsi hautement concernée par la cybercriminalité et les coûts pour les victimes deviennent de plus en plus importants. Les théories traditionnelles de lutte contre le crime depuis le papier séminal de Becker (1968) mettent l'accent sur les mesures de dissuasion. Inspiré des théories de choix rationnel, Becker (1968) montre qu'en faisant une analyse coût-bénéfice avant de commettre un crime ou un délit, le criminel passera à l'acte seulement lorsque les bénéfices tirés du crime sont supérieurs aux coûts encourus. Ainsi, on peut réduire le nombre de crimes et délits en augmentant le coût de tels actes : d'où les mesures de dissuasion. Ces mesures consistent essentiellement à la sévérité de la peine (emprisonnement ou amende), à la certitude qu'un tel acte sera

[1] http://www.mediaf.org/fr/themes/fiche.php?itm=3300&md=&thm=5 dernière consultation 23/08/2011.
[2] Internet Crime Complaint Center du FBI.

en effet puni c'est-à-dire une forte probabilité d'être arrêté et condamné. Dans la pratique, ceci réfère à l'efficacité de la police, des officiers de justice et de la possibilité d'appliquer la loi si elle existe. Si pour les crimes traditionnels, les mesures de dissuasions ont démontré des effets plutôt optimistes sur la lutte contre la criminalité, il n'en va pas de même en ce qui concerne la cybercriminalité. La dissuasion n'est effective que si elle est crédible, autrement dit si elle englobe trois caractéristiques à savoir : la célérité, la certitude et la sévérité (Lavoie, 2008). En réduisant l'importance des frontières érigées par le temps et l'espace, la cybercriminalité réduit de façon drastique la portée des mesures dissuasives traditionnelles. Son mode d'action impersonnel et anonyme rend la probabilité de détection, d'arrestation et de condamnation du cybercriminel pratiquement nulle. Ce constat consacre la non pertinence des méthodes de dissuasion traditionnelle. Ainsi dans la logique du choix rationnel reposant sur une analyse coût-bénéfice, où les coûts sont déterminés par les mesures dissuasives traditionnelles, la cybercriminalité ne connaitra que l'expansion et un développement vertigineux.

Il apparait donc nécessaire sur la base du développement précédent, de relire la rationalité du cybercriminel à partir d'autres éléments de coût nouveaux afin de définir des mesures dissuasives susceptibles d'aider à contenir la cybercriminalité. La présente étude s'articule en trois sections. Dans une première section elle présente les acteurs du marché de la cybercriminalité et leurs caractéristiques. Dans une deuxième section elle fait un survol de la littérature sur les comportements de choix rationnel du cybercriminel. Enfin dans une dernière section, le papier dérive un modèle théorique de dissuasion vs répression de la cybercriminalité, où, les mesures dissuasives sont plus adaptées à la nature de l'objet et/ ou de l'instrument de ce crime (ordinateur). L'étude finie par des recommandations de politique.

2. Le marché de la cybercriminalité

Le marché de la cybercriminalité est considéré comme un marché de type Walrasien dans lequel le comportement agrégé des offreurs et des demandeurs est coordonné de manière à ce qu'un prix d'équilibre soit réalisé (Ehrlich, 1996). Selon Becker (1968) le marché du crime est composé des criminels et des garants de la loi ; l'interaction entre ces deux agents détermine l'équilibre sur le marché. Il est cependant important de faire observer comme Ehrlich (1996) que des acteurs autres que les seuls criminels et garants de la loi interviennent sur ce marché ; il s'agit par exemple des receleurs d'objet volé et des victimes.

Nous décrivons donc le marché de la cybercriminalité en présentant trois acteurs principaux que sont les cybercriminels, les victimes et les garants de la loi.

2.1. Les cybercriminels

La cybercriminalité est une notion large qui regroupe « toutes les infractions pénales susceptibles de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau. Przyswa (2010) propose un bon exposé sur les différentes formes de cybercriminalité. Elle a été utilisée pour décrire un large éventail d'infractions, y compris les infractions contre les données et les systèmes informatiques (piratage), la falsification des données informatiques, la fraude informatique, l'escroquerie ; la diffusion de matériel pornographique mettant en scène des enfants, les infractions des droits d'auteur (telles que la diffusion des contenus piratés).

Ainsi définie, la cybercriminalité diffère de la plupart des crimes conventionnels sur au moins quatre points. Il est plus ou moins facile d'apprendre à commettre un cybercrime, sa commission nécessite très peu de ressources comparativement aux dommages qu'elle peut entrainer, elle peut être commise dans une juridiction sans que l'auteur ne soit physiquement présent dans cette juridiction et à les actes de cybercriminalité ne sont pas clairement illégaux. Ainsi, le profil des cybercriminels est significativement différent de celui des criminels conventionnel. L'inexistence de base de données et de structure de lutte contre la cybercriminalité renforce davantage la difficulté dans la caractérisation des cybercriminels. Les quelques tentatives de caractérisation des cybercriminels identifiées dans la littérature reste sommaire pour les raisons évoquées plus hauts (Kshetri, 2010 ; Sutherland, 2008 ; Aggarwal, 2009 ; Giannangeli, 2008 ; Jen et al., 2006).

Les quelques statistiques existants sur les cybercriminels révèle qu'il s'agit d'une population complexe et hétérogène. L'hétérogénéité dans la composition des cybercriminels s'explique par le fait que c'est un groupe composé autant d'amateurs avec des qualités de programmation très faibles mais qui, pour perpétrer leurs attaques utilisent des programmes ou logiciels préconçus par des criminels professionnels aguerris avec les technologies de pointe. Cette difficulté de caractérisation vient aussi de la nature de son outil d'action : l'ordinateur. Iteanu (2004) défini la cybercriminalité comme toute action illégale dans laquelle un ordinateur est l'instrument ou l'objet du délit. Dans cette logique, tout utilisateur d'ordinateur ou tout internaute est un cybercriminel potentiel.

Cependant, des profiles de cybercriminel sont déclinés dans la littérature ; elle retient en général que les cybercriminels sont pour la plupart jeunes. Giannangeli (2008) montre qu'en Russie la plupart des cybercriminel (*hackers*) sont jeunes, bien éduqués et sont des indépendants ; les mêmes caractéristiques s'observent aussi auprès des cybercriminels de la Taiwan (Jen et al. 2006)[3]. Cette présence

[3] Le Rapport 2010 de Norton sur la cybercriminalité montre qu'elle est à 90% le résultat de la cybercriminalité organisée ; ceci nuance un peu les résultats sur le statut d'indépendant des

forte de jeunes diplômés porte à croire que l'activité de cybercriminalité est liée au manque d'opportunité économique pour la jeunesse. Dans un contexte de fort taux de scolarisation et d'expansion des formations dans le domaine des technologies de l'information et de la communication (TIC), l'activité de cybercriminalité risque de connaitre un essor si l'industrie des TIC n'arrive pas à occuper tous les diplômés. Les études montrent que les diplômés les plus tentés par des activités de cybercriminalité sont les diplômés des écoles de Technologie de l'Information (McAfee, 2006). Sullivan (2007) montre que les activités de cybercriminalité tendent davantage à prendre naissance dans les pays qui portent un accent particulier sur les mathématiques, la physique, les sciences informatiques mais qui ne rémunèrent pas suffisamment les emplois légaux dans le domaine des TIC.

Autrement dit, on peut s'attendre à voir comme cybercriminel des individus diplômés sortis des écoles de technologie qui jugent très faible le revenu qu'ils pourront tirer d'activités légales. Leur qualification dans le domaine des TIC les prédispose donc à l'activité de cybercriminalité mais les rend dans le même temps difficilement appréhendable par la police. Selon, Bell (2002), la mafia russe a développé au cours de ces dernières années une expertise dans la cybercriminalité et cette expertise est aux mains d'anciens agents du KGB. La relative facilité dans l'acquisition de la compétence en cybercriminalité (apprentissage sur le tas) laisse une porte ouverte de transmission du savoir des personnes qualifiées vers les individus moins qualifiés de manière à ce qu'à terme les cybercriminels travaillent en groupe et rendent ainsi plus faible la probabilité d'être attrapé.

S'il y a une évidente difficulté à profiler le cybercriminel, il existe cependant un consensus sur la nature du cybercriminel : c'est un individu très accroché à l'ordinateur avec le risque d'en être finalement dépendant. Des auteurs ont tenté d'établir une relation entre l'addiction à l'ordinateur et la cybercriminalité (Nykodym et al., 2005). L'addiction à l'ordinateur est définie entre autres par l'abus de l'ordinateur c'est-à-dire le fait de passer un temps exagérément long devant l'ordinateur que l'on peut exprimer en terme médicale par une utilisation pathologiquement obsessive de l'ordinateur. Les individus sous addiction ignoraient certainement l'existence d'opportunités aussi importantes sur Internet ; mais le fait d'y passer beaucoup de temps, pourrait les mettre en contact avec les multiples opportunités de cybercriminalité. Les adolescents connaissant des coûts d'opportunité bas sont susceptibles d'être plus victimes à cette forme d'addiction. Ceci peut constituer aussi une explication à la forte présence des jeunes et adolescents dans l'univers de la cybercriminalité.

Un autre consensus sur le cybercriminel porte sur les techniques généralement utilisées par les cybercriminels pour opérer. Il s'agit globalement de la technique

---

cybercriminel ; à moins que ces statistiques confirment le caractère complexe de cette forme de criminalité et sa rapide mutation.

de la manipulation que Dawkins (1982) analyse par le phénomène du syndrome de l'ennemi rare *(the rare enemy syndrome*). L'idée du syndrome de l'ennemi rare est que le type de manipulation de l'ennemi est si rare que l'évolution technologique n'a pas encore connue de progrès à même de rendre disponible à la victime un anti poison efficace. Les techniques de cybercriminalité prennent appui sur un processus similaire. Les rapports disponibles sur la cybercriminalité venant aussi bien des logiciels anti virus que des agences de lutte contre la cybercriminalité indiquent que les pirates sur Internet exploitent nos vulnérabilités psychologiques les plus profondes dans leurs dernières techniques de *scam* par *e-mail*. Les cybercriminels utilisent des méthodes toujours plus ingénieuses, par exemple en usurpant l´identité de personnes de confiance, en engageant un dialogue amical et en exploitant des émotions comme la peur, l´insécurité ou la cupidité.

Les cybercriminels associent de plus en plus un code furtif avec des tactiques psychologiques, pour manipuler leurs victimes et les persuader d´ouvrir les pièces jointes (en usurpant par exemple l´identité d´un ami ou d´un organisme de confiance comme une société de cartes de crédit), de cliquer sur un lien ou d´entrer des informations confidentielles, ce qui leur permettront de piller les informations personnelles et les comptes bancaires en ligne. En général, le cybercriminel utilise des techniques pour vaincre notre scepticisme au point où les victimes ne sont pas uniquement les utilisateurs inexpérimentés de l'Internet. Le rapport McAfee Mind Games (2006) révèle que les cybercriminels passent beaucoup de temps à étudier les cordes sensibles des victimes potentielles et des sujets « chauds » auxquels leurs victimes sont sensibles. Ainsi, l'utilisateur sensible aux séminaires et conférences internationales sera appâtés par des sujets de cette nature, alors qu'un collectionneur sera appâté par des œuvres d'art et ainsi de suite. De plus en plus les cybercriminels vont au-delà de la manipulation psychologique à travers Internet et vont directement appeler leurs potentielles victimes sur leur téléphone portable afin de recueillir des informations personnelles sur elles.

2.2. Les victimes de la cybercriminalité

Les victimes de la cybercriminalité représentent l'ensemble de ceux qui à un moment donné se sont senti victime de cybercrime. Tout comme les cybercriminels, très peu d'information sont disponibles sur les victimes de la cybercriminalité. Les victimes de cybercriminalité n'ont pas de profile identique ; elles comportent autant les individus Internet expérimentés que les individus non expérimentés ; on y retrouve toute sorte d'agent économique (ménages, entreprises, gouvernements) : tout ceux qui pour des besoins donnés ont recours à Internet ou à l'ordinateur sont de potentiels victimes.

Pour diverses raisons, les victimes de la cybercriminalité ne dénoncent pas les délits dont ils ont fait l'objet. *Selon Computer Crime Research* le nombre de plainte au niveau international déposé en 2009 ne représente que 20% de l'ensemble des

actes de cybercriminalité. Les raisons du refus de dénonciation varient selon le type de victime. En ce qui concerne les individus ou ménages deux principales raisons justifient leur silence face aux attaques de cybercriminalité. Premièrement, ils se sentent souvent embarrassés car s'attribuant la culpabilité de leur victimisation (Norton, 2010 ; Salu, 2004). Cette catégorie de victimes pensent pour la plupart du temps qu'ils sont les premiers à être blâmer ; ensuite, il y a les victimes qui n'ont aucune confiance à la justice quant à sa capacité à poursuivre les cybercriminels ; ce sentiment nait lorsqu'il n'existe pas de structures compétentes qui enregistrent les plaintes et engagent les poursuites ou lorsque les victimes jugent la compétence des autorités limitées face à un problème globale. Ceci s'explique par le caractère purement anonyme du crime car il est pratiquement impossible d'indiquer un suspect. S'agissant des entreprises ou unités de production de biens et services, la réticence à porter plainte s'explique par la peur de perdre la confiance des clients, de perdre sa réputation et sa crédibilité ou de donner un mauvais signal sur le marché boursier (Kshetri, 2010). Les structures financières et les banques sont les plus concernées par ce type de comportement. Une troisième série d'explication du silence qui affecte tous les types de victime est liée à leur ignorance des mécanismes de cybercriminalité et à l'absence de preuve de crime (Regan, 2006 ; Wall, 1998 ; Richtel, 1999).

Dans un cas comme dans l'autre le refus de dénonciation renforce davantage les cybercriminels car ne se sentant pas traqués ou poursuivi ; c'est ce que Kshetri (2010) appelle le cercle vicieux de la cybercriminalité. L'absence de traque renforce le sentiment de succès et la confiance du cybercriminel et le conforte dans sa stratégie d'opération. L'absence de dénonciation affaibli en retour les agences de sécurité et les institutions judiciaires car sans plainte il leur sera difficile d'appliquer la loi, de se rendre compte des limites de la loi existante et d'enrichir leur expérience face à ce crime nouveau. Les dénonciations sont d'autant nécessaires en ce sens qu'elles rendront possible l'estimation des coûts ou pertes à l'échelle de la population dus à la cybercriminalité et faciliter la mise en œuvre de politique dans une optique d'analyse coût-bénéfice. Compte tenu du rôle primordial que jouent les victimes de cyber-attaque dans le processus de contrôle de la cybercriminalité, il devient important de leur assurer un niveau minimum d'éducation dans la détection des cybercrime.

2.3. Les structures de veille et de surveillance

A la suite de la libéralisation du secteur des télécommunications au début des années 1990 en Afrique subsaharienne, les pays africains sont encore en 2011 au balbutiement en ce qui concerne les structures de régulation. Le rôle de ces institutions de régulation consiste essentiellement d'une part à prévenir les abus de position dominante et l'émergence d'une concurrence effective ou potentielle et, d'autre part à assurer la mise en œuvre du service universel. Ainsi, le rôle de veille et de cyber sécurité est laissé aux structures traditionnelles de sécurité telles que la

gendarmerie et la police. Ces dernières ont montré leur incapacité à lutter contre ce crime d'un genre nouveau. La police est généralement établie sur une juridiction bien délimitée et se voit donc considérablement limitée dans la lutte contre un crime globale aux moyens impersonnels. Les variables de dissuasion du crime traditionnel telles que la probabilité d'arrestation et l'importance de la peine sont pratiquement inefficaces dans la lutte contre la cybercriminalité. Mieux elles deviennent des variables de répression car n'intervenant plus pour empêcher le crime, tant la cybercriminalité est impersonnelle et globale ce qui annule presque la probabilité d'être arrêtée toute chose aggravée avec les moyens inappropriés dont disposent la police. La mesures classiques de dissuasion (nombre de policier, peine, probabilité d'être arrêté et d'être condamné, etc.) deviennent des mesures de répression car mises en œuvre seulement lorsque le cybercriminel est arrêté.

Des auteurs ont montré que l'incapacité de la police et de la gendarmerie à lutter efficacement contre la cybercriminalité réside aussi bien dans leur manque de compétence en matière d'appropriation des technologies de l'information et de la communication, de la lourdeur administrative qui les caractérisent que du caractère global de la cybercriminalité (Larsen et Lomi, 2002 ; Brenner 2004 ; Jones 2007 ; Wall, 2007). Outre ses éléments de faiblesse qui caractérisent les structures traditionnelles de lutte contre le crime, l'on peut noter dans la plupart des pays de l'Afrique subsaharienne, l'absence de textes de lois sur la protection des données (numériques) à caractère personnel, le e-commerce et la protection des mineurs sur Internet. La combinaison de l'ensemble de ces facteurs détruit la confiance que pourrait avoir les victimes en ces structures. L'incrédulité des victimes dans les capacités des structures traditionnelles à lutter contre la cybercriminalité renforce le sentiment d'impuissance des victimes et les amènent à juger d'inutiles les dépôts de plainte : tout ceci contribue au cercle vicieux de la cybercriminalité. L'absence de plainte qui est la conséquence de la perception que les victimes ont des structures traditionnelles de lutte contre le crime ne permet pas à celles ci de mettre à jour leur compétence et technique d'intervention ce qui constitue une protection de l'activité de cybercriminalité.

De plus en plus des unités spécialisées sont créées afin de rendre plus efficace la lutte anti cybercriminalité. Parmi ces unités, les plus connues se retrouvent dans les pays développés ; il s'agit du FBI cyber division (*Internet Crime Complaint Center*) aux Etats-Unis, du *Metropolitan Police Computer Crime Unit* au Royaume Unie, *des Computer Emergency Response Team* de la France, des Pays-Bas. La principale difficulté de ces centres est leur incapacité à retenir les détectives les plus talentueux (Blitstein, 2007) et l'absence de coopération internationale entre agences (Joshi, 2009). Cette absence de coopération s'explique par le degré d'hétérogénéité très élevé entre les lois anti cybercriminalité. Il faut cependant noter que des efforts se font dans ce sens à travers L'Union International des Télécommunication qui a crée en 2009 le Centre IMPACT (*International Multilateral Partenership Against Cyber Threats*) qui s'inscrit dans une logique de

coopération internationale contre la cybercriminalité ; l'on note aussi la Convention contre la cybercriminalité signé par quarante six pays (IUT, 2009) et diverses initiatives régionales.

En Afrique comme dans beaucoup de pays dans le monde, l'on est encore au mieux des cas au début de la création des *Computer Emergency Response Team* qui restent encore majoritairement des centres de veille et de surveillance s'investissant dans la sensibilisation des utilisateurs du service Internet et des intentions de coopération régionales contre la cybercriminalité[4]. Face à l'appel urgent des centres de recherches et des structures de lutte contre le crime au renforcement du cadre légal et de la mise à disposition de moyen pour une lutte efficace contre la cybercriminalité, on est en droit de penser que faire uniquement de la sensibilisation à l'intention des utilisateurs de Internet est une manière d'avouer ses limites et faiblesses.

3. Comportement économique du cybercriminel : survol de la littérature

Dans cette section, il est présenté et discuté le cadre traditionnel d'analyse théorique de la cybercriminalité.

3.1. Cadre d'analyse théorique de la cybercriminalité

Le cadre d'analyse économique du crime est basé sur l'hypothèse que les délinquants en moyenne, répondent aux incitations: le crime est considéré comme un choix social, en dépit du comportement non éthique, et immoral, ou même déviants de certains de ses auteurs. Sous cette hypothèse, Becker (1968) modélise le choix du criminel comme fonction des gains liés à la criminalité, la probabilité d'être arrêté et de la sévérité ou type de la condamnation. Son objectif est de minimiser la perte nette sociale associée au crime (crime génère une déséconomie externe parce que les coûts sur les victimes et le système de justice pénale dépasse tout bénéfice réalisé par les auteurs). Il montre que pour maximiser le revenu social global, les sanctions optimales contre les criminels devraient prendre la forme d'amendes. Il soutient que les amendes en termes de dissuasion contre le crime sont meilleures que l'emprisonnement (l'emprisonnement est plus coûteux à l'Etat).

Ainsi, depuis le papier séminal de Becker (1968), sur le crime, l'analyse économique du comportement du criminel (quelque soit le type de crime) se fait sur l'hypothèse que celui-ci est un agent économique rationnel qui maxime son profit autrement dit, le criminel est un individu qui prend sa décision dans le sous ensemble de choix qui correspond à des bénéfices supérieurs aux coûts encourus du

[4] The first West Africa Cybercrime Summit 2010. Conférence Régionale africaine sur la Cybersécurité (www.afcybersec.org).

fait de l'acte criminel. Le cybercriminel s'inspire aussi de ce type de comportement : un cybercrime est commis lorsque les bénéfices que tire le cybercriminel de cette attaque sont supérieurs aux coûts qu'il supporte.

L'augmentation des activités de cybercriminalité répond économiquement donc à la conjugaison de deux facteurs : la sensibilité de l'individu aux incitations monétaire et psychologique. Ces incitations à la cybercriminalité sont liées au fait que les gains potentiels liés à la cybercriminalité sont en nettes augmentation en lien avec la croissance des utilisateurs de Internet et des coûts très faibles liés à l'appréhension et à la condamnation des cybercriminels comparativement aux crimes traditionnels. Le rapport 2006 de Mcafee offre une illustration de ces incitations en comparant deux criminels, un conventionnel (passeur d'héroïne) et un cybercriminel ; il montre que le criminel conventionnel prend comme sentence au mieux des cas une prison à vie au pire une peine de mort alors que le cybercriminel prend quatre années de prison. Messmer (2009) rapporte le fait que pour réduire la probabilité d'être arrêté, le cybercriminel renonce à attaquer les individus se trouvant dans son propre pays. Les cybercriminels sont d'autant plus difficile à détecter et à poursuivre du fait de la mondialisation de la cybercriminalité et des problèmes juridictionnels qu'elle entraine. La cybercriminalité est donc plus rentable et moins risquée que les crimes traditionnels.

3.2. Analyse des incitations à la cybercriminalité

Une manière simple de conceptualiser cette analyse coût- bénéfice du cybercriminel en s'inspirant du cadre de Becker (1968) peut prendre la forme qui suit[5] :

$$M_b + P_b > O_{cp} + O_{cm} P_a P_c \quad (1)$$

Où le membre de gauche représente les bénéfices tirés de l'attaque cybercriminel et le membre de droite les coûts de l'attaque au le cybercriminel. M_b représente le bénéfice monétaire associé au crime, P_b le bénéfice psychique associé au crime, O_{cp} représente le coût psychique associé à l'acte criminel, O_{cm} le coût d'opportunité monétaire associé à la condamnation, P_a la probabilité d'être arrêtée et P_c la probabilité d'être condamné.

De façon volontaire nous choisissons de nous intéresser presque exclusivement au coût qu'implique la cyber attaque au cybercriminel (au membre de droite de l'équation (1)). Ceci est une manière de comprendre la formation de ces coûts et par conséquent l'expansion de la cybercriminalité. De (1), l'on peut tenter des

[5] Cette présentation est inspirée de Kshetri (2010)

explications additionnelles à la faiblesse du coût pour le cybercriminel lié à la cybercriminalité à partir de O_{cm} représentant le coût d'opportunité lié au fait d'être arrêté et condamné. O_{cm} n'est en fait que les gains perdus du fait du séjour en prison qui prive le cybercriminel de travailler légalement. Le coût d'opportunité ainsi considéré peut jouer un rôle ambigu. Un individu rationnel tourné vers le futur peut décider supporter ce coût d'opportunité lorsque les gains actualisés liés à la cybercriminalité sont largement supérieur aux coûts d'opportunité. Cette incitation peut naitre lorsque l'industrie des techniques de l'information et de la communication ne propose pas un salaire conséquent aux diplômés sortis des écoles de technologie de l'information. Un autre élément qui fait jouer un rôle ambigu à ce coût d'opportunité est lié à la relative facilité de transmission des techniques de cybercriminalité. Il a été documenté dans la littérature le risque de renforcement des capacités des cybercriminels dans les prisons (Poulsen, 2009). Au fur et à mesure qu'un cybercriminel est mis en prison, il y a de forte chance qu'il voit ses capacités de criminel renforcées et consolidées avec la rencontre d'autres cybercriminels. Un comportement identique est aussi observé dans les milieux terroristes. Le coût d'opportunité lié au séjour en prison dépend donc positivement de la sensibilité du cybercriminel à la perte de sa liberté de libre circulation et négativement de sa sensibilité aux opportunités de renforcement de capacité qu'il pourra rencontrer sur place. La seule alternative crédible de sanction qui reste consiste à la pénalité monétaire où le cybercriminel est astreint à rembourser les dommages causés par son acte. Ce type de sanction si elle prospère dans le cas des crimes traditionnels peut souffrir d'application dans le cas de la cybercriminalité à cause de la mondialisation de celle-ci, de la forte hétérogénéité des lois anti crimes et du retard qu'accusent certains pays dans la mise à jour des lois anti cybercriminalité (Kshetri, 2010).

Le coût psychologique du crime réfère à l'énergie mentale et psychologique nécessaire pour commettre un cybercrime. Il est lié au remord ou au sentiment de culpabilité, à la peur d'être arrêté ou d'être condamné. Le coût psychologique est donc lié à la prise de conscience du cybercriminel d'avoir commis un acte immorale, non éthique. Selon Kshetri (2009), la plupart du temps, les cybercriminels ignorent leur victime (ne l'on jamais rencontré). Cette absence de contact physique renforce le sentiment de non culpabilité des cybercriminel ; les criminels conventionnels ou traditionnels sont plus susceptibles de voir leur victime et de constater les conséquences négatives de leurs actes. Le coût psychologique lié à la cybercriminalité est pratiquement nul. D'un autre point de vue, en considérant la cybercriminalité comme une conséquence de l'addiction à l'ordinateur, les individus pensent que l'Internet permet de fuir la vie réel et leur permet d'être invisible derrière une barrière d'anonymat (Nykodym, et al., 2005). Ce sentiment donne à l'individu sous addiction un faux sentiment de sécurité, car estimant qu'il n'existe aucune règle donc aucun risque de sanction sur Internet. Ce sentiment amène le cybercriminel à ne sentir aucun remord du fait de ses crimes et

donc à ne supporter aucun coût psychologique lié à son acte. Un autre facteur qui pourrait déterminer le coût psychologique est l'état des valeurs morales (Kshetri, 2010). Si les perceptions éthiques et morales régressent, les comportements à priori non éthiques et blâmables deviendront de plus en plus des comportements admis et acceptés. Dans un cas comme dans l'autre, les coûts psychologiques liés à la cybercriminalité sont très bas ou presque nuls.

Si dans les modèles inspirés *stricto sensus* de Becker (1968) (comme l'équation 1), très peu d'importance est accordée à la prévention, les extensions du modèle intègrent les aspects protections technologiques (protection privée) dans une démarche de dissuasion. Il est espéré que pour réduire la cybercriminalité, il faut augmenter l'effort lié à l'acte criminel en renforçant la protection des ordinateurs et de l'Internet. Shavell (1991) s'interroge quant à lui sur l'effectivité des protections privées à diminuer le niveau des crimes ; il pense plutôt qu'elles reportent les crimes sur les individus les moins protégés. Brenner (2004) propose pour contourner cette difficulté de l'hétérogénéité dans les niveaux de protection d'utiliser un model de distribution de la sécurité qui exige des utilisateurs d'ordinateur ou des opérateurs du service Internet de disposer d'un niveau de sécurité adéquat pour leurs ordinateurs au risque de faire l'objet de poursuite criminel. Si l'on peut admettre qu'une telle réglementation a des chances de donner les incitations nécessaires pour renforcer les protections privées, il reste que ceci peut décourager les décisions de porter plainte une fois que l'on est victime. Une fois encore l'on rentre dans le cercle vicieux de la cybercriminalité.

De plus en plus, les aspects protections technologiques de l'utilisateur final sont évoqués sans que cela ne soit la conséquence d'un modèle économique. Depuis les travaux de Becker (1968), les modèles économiques du crime sont essentiellement des modèles de sanction et égalise le prix au risque. Sur la base d'un tel modèle il est par exemple difficile d'inférer la taille de protection technologique optimale et par conséquence d'évaluer la part des lois répressives dans la lutte contre la cybercriminalité. Lutte contre la cybercriminalité : vers une reconsidération des mesures de dissuasions.

Dans cette sous section il est discuté dans une première partie des limites des mesures traditionnelles de lutte contre le crime pour faire face à la cybercriminalité et dans une deuxième partie le papier dérive un modèle théorique de crime avec prise en compte de l'effort.

3.3. Cybercriminalité et dépassement des mesures traditionnelles de lutte contre le crime

Dans les modèles traditionnels de répression de la criminalité, les changements dans la punition ont été le principal moyen par lesquels les politiques publiques peuvent influencer le risque lié à l'activité criminelle. Mais comme nous l'avons

dit plus haut la punition n'a d'effet dissuasif que lorsqu'elle est entretenue par un mécanisme crédible. La crédibilité de la dissuasion repose sur trois principes : célérité, certitude, sévérité (Lavoie, 2008). Mais le choix rationnel du cybercriminel suppose qu'il décide de prendre le risque de violer la loi seulement après avoir évalué le risque d'appréhension, la gravité de la peine prévue, le gain tiré de la criminalité et l'imminence du besoin du gain criminel (Siegel, 1992). Un élément important de ce raisonnement est le risque lié à l'appréhension donc la probabilité d'être arrêté. Le criminel en décidant donc de commettre un crime réfléchi plus sur les voies et moyens pour ne pas se faire prendre que sur les sanctions car l'arrestation précède la condamnation (Lebranchu et Hazan, 2007[6]). Ainsi considéré, l'élément déterminant dans le choix rationnel du criminel est la probabilité d'être arrêtée laquelle probabilité est fortement liée aux mesures dissuasives telles que l'efficacité de la police. Or la cybercriminalité en relocalisant la criminalité à un niveau international, fait que la police en tant que force locale bureaucratiquement organisée est souvent confrontée à des problèmes de juridiction. Le risque d'être arrêté devient donc pratiquement nul. Afin de conforter davantage cette probabilité nulle d'être détectée, le cybercriminel, exception faite des cas de cyber harcèlement, choisi de s'attaquer à des victimes qui sont loin de son lieu de localisation (Messmer, 2009). Les mesures dissuasives traditionnelles ne sont donc plus dans le cas de la cybercriminalité des mesures de dissuasion générale mais réfèrent plus à des mesures de répression en ce sens qu'elles ne deviennent effectives qu'une fois mise en œuvre. Cette forme de répression peut avoir un effet de dissuasion spécifique en ce sens qu'une fois exercée, elle pourrait contribuer à décourager la récidive. Mais à ce niveau il est important de faire remarquer que la facilité relative de transmission des connaissances de cybercriminalité peut faire de la prison une école de la récidive.

Une autre modification apportée par la cybercriminalité à l'analyse traditionnelle repose sur le principe de sévérité des sanctions. Des travaux et enquêtes reportent le fait que même arrêtés, les cybercriminels ne sont généralement pas condamnés avec des peines sévères en comparaison avec les crimes traditionnels (Kshetri, 2010 ; Mcafee, 2006). Cette faiblesse des sanctions tient soit à l'inexistence de la loi ou au manque de compétence de la juridiction ou à l'incompétence des officiers de justice (procureurs, juges) dans la manipulation des outils informatiques ce qui rend parfois très complexe et difficile les procédures et la compréhension par eux des arnaques. Le rapport Mcafee (2006) montre que toute chose égal par ailleurs, un passeur d'héroïne est condamné à la prison à vie alors qu'un hacker est condamné à quatre ans de prison. Gabrys (2002) montre que si un cybercriminel est arrêté, la probabilité qu'il soit condamné est de 1 sur 22 000. Cette faiblesse de la

[6] Tribune publiée dans les pages Rebonds de Libération**,** par Marylise Lebranchu, députée du Finistère, ancienne ministre de la Justice, et Adeline Hazan, députée européenne, le 18 juillet 2007. http://reformer.fr/

sanction contribue à réduire les risques liés à la cybercriminalité pour le cybercriminel.

Il devient important de revoir la notion du risque dans l'analyse et l'élargir à l'effort et au temps nécessaire au cybercriminel pour commettre sa forfaiture. Augmenter l'effort et le temps, permettra de combler le déficit de célérité et de certitude lié aux mesures dissuasives traditionnelles. Il convient d'insérer de façon explicite dans l'analyse la protection des ordinateurs qui a pour objectif de renforcer davantage leur sécurité et par conséquent d'augmenter l'effort et le temps nécessaire pour commettre le cybercrime.

3.4. Modèle dissuasion vs répression avec prise en compte de l'effort

Dans la microéconomie classique, l'on utilise comme indicateur de bien être la variation du surplus du consommateur et du producteur. Mais conformément à Van Dijk (1992), qui utilise une terminologie adaptée au crime, nous parlerons de surplus de la victime et de surplus du criminel en lieu et place de surplus du producteur et surplus du consommateur respectivement. Une manière de voir ceci est de considérer la victime comme un producteur involontaire des opportunités de cybercriminalité et le cybercriminel comme un consommateur qui produit une demande d'opportunité de cybercriminalité. Il considère par conséquent les victimes comme des producteurs et les cybercriminels comme des consommateurs. Notre analyse emprunte beaucoup à ce cadre.

Le surplus de la victime correspond au surplus réalisé par les individus qui offre des opportunités de cybercriminalité à un niveau de risque inférieur au niveau d'équilibre de l'économie. Parmi ces individus figurent des individus qui offrent des opportunités de cybercriminalité à un niveau de risque zéro. Autrement dit le surplus de la victime correspond au surplus réalisé par les individus qui réalise un niveau de protection de leur ordinateur en dessous du niveau d'équilibre requis pour commettre la cybercriminalité dans l'économie. Il s'agit des individus ayant un niveau d'anti virus, de pare feu, d'anti spam, d'anti *malware* très faible ou d'individu n'ayant même pas installé de logiciel anti virus. C'est certainement pour réduire au minimum le nombre de ces individus et donc réduire le surplus de la victime que Brenner (2004) propose un model de distribution de la sécurité qui exige des utilisateurs d'ordinateur ou des opérateurs du service Internet de disposer d'un niveau de sécurité adéquat pour leurs ordinateurs au risque de faire l'objet de poursuite criminel. Le surplus de la victime est donc mauvais pour la société.

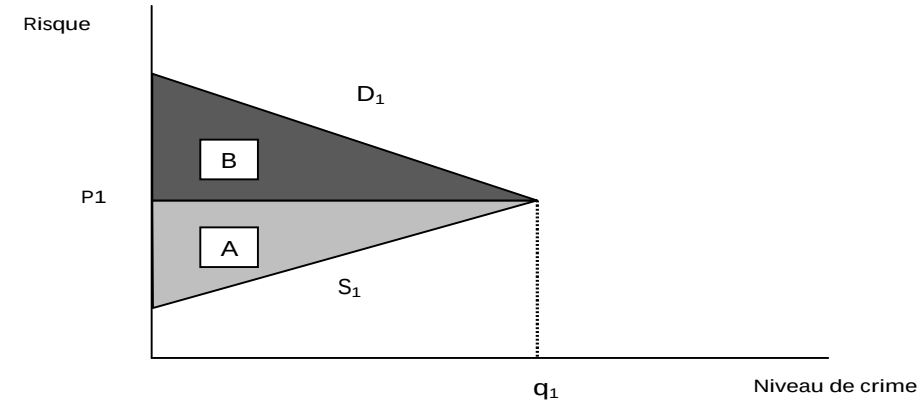
Le surplus du cybercriminel correspond au surplus dont il bénéficie parce que le niveau de risque d'équilibre associé au cybercrime sur le marché de la cybercriminalité est plus faible que le niveau de risque qu'il est disposé à prendre pour commettre une attaque cybercriminel. Le surplus du cybercriminel augmente avec la baisse du niveau de risque d'équilibre requis pour commettre un crime.

C'est donc mauvais pour la société. Sur le marché du cybercrime, la société gagne à la fois de la baisse du surplus de la victime que du surplus du cybercriminel. Il s'agit maintenant d'apprécier dans quelle mesure la loi (répression) et la protection (dissuasion) produise un bénéfice social net.

La figure (1a) présente les différents surplus de la victime et du cybercriminel. Avec S_1 la courbe d'offre involontaire d'opportunité de cybercriminalité de la victime et D_1 la courbe de demande d'opportunité de cybercriminalité. Sur la figure (1a), l'équilibre du marché de la cybercriminalité est caractérisé par un niveau de risque (p_1) et une quantité de cybercrime (q_1). Le surplus de la victime est représenté par l'aire du triangle *A* et le surplus du cybercriminel est représenté par l'aire du triangle *B*. Supposons ensuite que des mesures dissuasives sont prises pour lutter contre la cybercriminalité il s'agit entre autre de mesures de protection des ordinateurs telles que les anti virus, les anti spams, les pare feu, …ces différentes mesures de protection sont discutées dans la littérature dans les différents rapports des logiciels anti virus (Norton Symantec, McAfee, etc.). Lorsque ces mesures sont prises par l'ensemble des utilisateurs d'ordinateur, le niveau de risque pris par le cybercriminel pour commettre son forfait s'accroit. Sur la figure (1b) ceci est caractérisé par un déplacement de la courbe d'offre (S_1) vers la gauche et par une augmentation du risque qui passe de p_1 à p_2, ce qui se traduit par une diminution de la quantité de cybercrime commis dans l'économie.

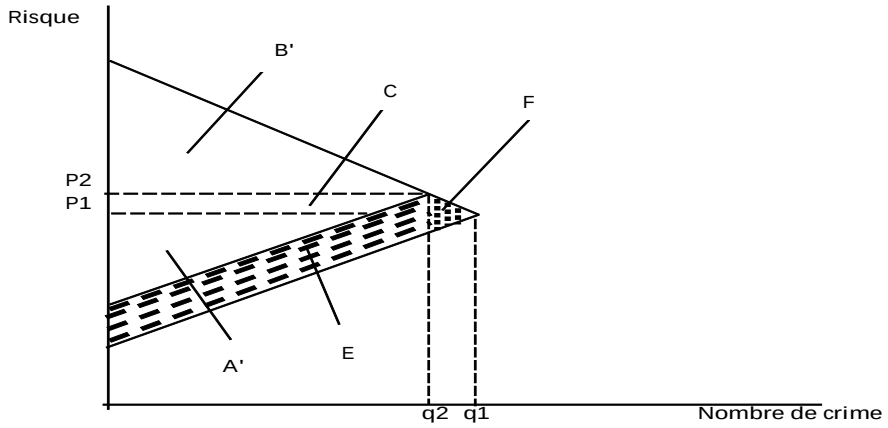
La prise de mesures préventives (de protection) a contribué sans doute à réduire le niveau de cybercriminalité dans l'économie. Les victimes ont perdu une partie de leur surplus (surface hachurée E) ; ceci correspond à un gain social. Cette perte de surplus constitue un gain pour les victimes ; dans le même temps, les cybercriminels ont enregistré une perte équivalente à l'aire C. L'aire C représente un transfert et ne correspond donc pas à une augmentation de bien être de la société. L'aire du triangle F (en pointillé) correspond à une perte des cybercriminels et représente à la fois une augmentation du bénéfice social. Les pertes de surplus E et F correspondent à un bénéfice social ; les mesures préventives permettent en conséquence de réduire la cybercriminalité et d'augmenter le bien être social. Mais dans la mesure où l'augmentation de la protection donc de la dissuasion est liée à la disponibilité de la technologie, on peut inférer que seule la dissuasion ne peut permettre d'éliminer la cybercriminalité car les surplus du consommateur (cybercriminel) et du producteur (victime) ne sont pas nuls. Théoriquement dans notre modèle dissuasion-répression, la réduction des surfaces (A et B) qui deviennent respectivement A' et B' dépendent donc de l'efficacité des mesures de répression donc des sanctions : nous rejoignons ici le cas étudié par Becker (1968).

Figure 1a – Equilibre du marché de cybercriminalité



Source : Auteur

Figure 1b – Equilibre après dissuasion



Source : Auteur

Il apparait donc claire que lutter contre la cybercriminalité revient à opérer une juste combinaison de dissuasion et de répression. Il s'agit maintenant de déterminer les niveaux de répression ou de dissuasion selon les niveaux d'élasticité des courbes de demande et d'offre d'opportunité de cybercriminalité. Il s'agit de faire de la statique comparative sur chaque cas et de mesurer l'efficacité relative de chaque mesure (répression et dissuasion). Nous étudierons alors respectivement quatre cas : (i) offre et demande fortement élastique, (ii) offre élastique et demande

inélastique, (iii) offre inélastique et demande élastique, (iv) offre et demande inélastique.

En microéconomie, l'élasticité de la demande se définie comme la capacité de la demande à augmenter ou à décroître en volume par rapport à la variation des prix. Notre définition de l'élasticité de la demande des opportunités de cybercriminalité est identique. Elle décrit la capacité des cybercriminels à augmenter ou à diminuer leurs activités au fur et à mesure que varient les risques (l'effort ou la protection) liés à l'activité cybercriminel. Ainsi la demande sera qualifiée d'inélastique quand une augmentation des risques n'entraine pas une diminution de la demande d'opportunité de cybercriminalité. Ceci peut s'expliquer par des cybercriminels technologiquement très actifs, qui trouvent le moyen de mettre à jour leur connaissance ; ainsi au fur et à mesure qu'est développé une nouvelle technologie de protection, les cybercriminels s'approprient la technologie et trouve un moyen pour la contourner. Par contre la demande d'opportunité de cybercriminalité est élastique lorsque l'augmentation de l'effort (des protections) nécessaire pour entreprendre une activité cybercriminel réduit sa demande. Ceci peut s'expliquer par un dépassement technologique des cybercriminels : les cybercriminels n'arrivant plus à contourner les systèmes de protection. Ceci n'est effectif que lorsque l'industrie des TIC arrive à retenir ses employés ou lorsqu'elle arrive à absorber tous les ‘‘diplômés TIC’’ produits.

L'offre des opportunités de cybercriminalité est dite élastique lorsqu'elle se réduit au fur et à mesure que les risques (l'effort ou la protection) liés à l'activité augmentent. Ceci s'explique par la prise de mesures de protection de plus en plus efficaces par les victimes à mesure que les activités de cybercriminalité augmentent. La notion d'élasticité de l'offre peut aussi être comprise ici comme une éviction des utilisateurs d'ordinateur qui n'ont pas les moyens de s'offrir une meilleure protection, ces utilisateurs décident, volontairement ou par contrainte, de ne pas utiliser d'ordinateur tant qu'ils n'ont pas la possibilité de le protéger de façon adéquate ; ce qui diminue les opportunités de cybercriminalité par une réduction des victimes potentielles (utilisateurs). Par contre, l'offre est dite inélastique lorsque l'augmentation des risques (effort ou protection) ne réduit pas les opportunités de cybercriminalité. On peut penser que les utilisateurs d'ordinateurs n'ont pas un accès financier et géographique aux meilleures technologies de protection des ordinateurs, de manière à ce que malgré l'augmentation du risque l'offre ne diminue pas.

Des figures (2a) (2b), (2c) et (2d) on observe d'importantes diminutions du surplus de la victime et du cybercriminel dans le cas où l'offre et la demande sont toutes élastiques (Fig 2b), et dans le cas où offre est inélastique et demande élastique (Fig 2c). La diminution la plus importante s'observe lorsque l'offre et la demande sont toutes élastiques. Ces résultats indiquent que les niveaux de dissuasion et de répression doivent alors varier selon les caractéristiques de la demande et de l'offre

afin de garantir l'efficacité des politiques publiques. Dans un système (dissuasion, répression), pour une meilleure efficacité des mesures anti cybercriminalité, il faut dans les cas correspondants respectivement à une offre et une demande élastique et une offre inélastique associée à une demande élastique, un niveau de dissuasion (protection) plus élevé qu'un niveau de répression. Autrement dit, les politiques de dissuasion ont une plus grande efficacité dans ces cas.

Figure 2 – Statique comparative sur un marché de cybercriminalité

Figure 2a

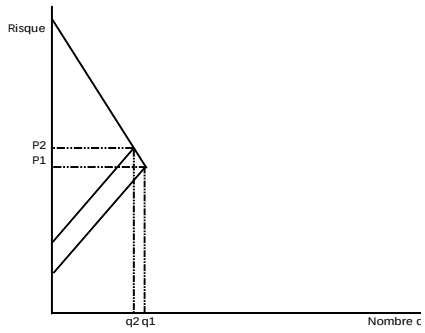


Figure 2b

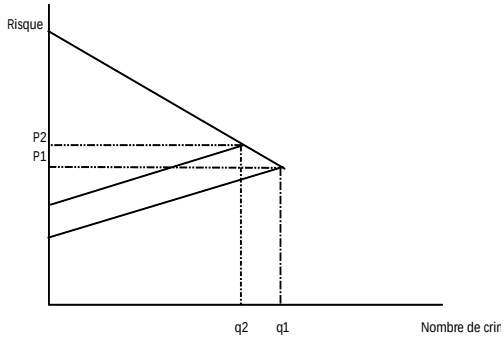


Figure 2c

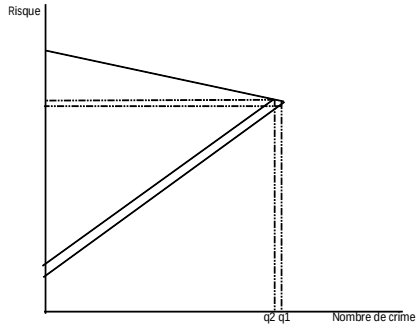
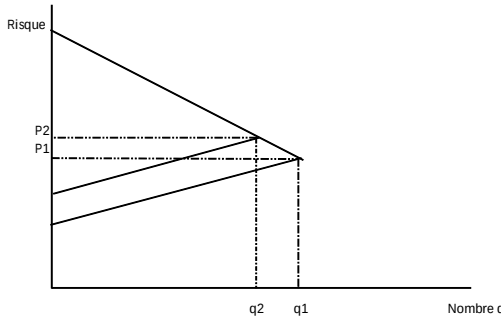


Figure 2d



Source : Auteur

4. Conclusion

La présente étude s'intéresse à la cybercriminalité d'un point de vue théorique en mettant l'accent sur la rationalité des cybercriminels c'est-à-dire les motivations et mécanismes qui les poussent à agir. Ainsi, l'étude caractérise le marché de la cybercriminalité en présentant et en définissant le rôle de chacun des acteurs de ce marché. Il ressort de cette présentation que la cybercriminalité est un crime de genre nouveau différent des crimes conventionnels et traditionnels qui sont plus ou moins localisés et pour lesquels les agences de sécurité et de régulation sont

équipées. L'étude révèle que compte tenue de sa nature les mesures de lutte traditionnelle contre le crime sont inefficace avec la cybercriminalité ; la plupart de ces mesures dissuasives avec les crimes traditionnelles deviennent des mesures répressives dans le cas de la cybercriminalité. Ainsi les peines, amendes qui sont tributaires de l'arrestation des criminels tombent pratiquement en désuétude dans le cas de la cybercriminalité. Dans cette logique le comportement rationnel du cybercriminel, qui fait de lui un agent économique rationnel évaluant les bénéfices et les coûts liés à son activité, permet de comprendre l'expansion de la cybercriminalité car les coûts qui y sont liés sont pratiquement nuls. La prise en compte de l'effort nécessaire pour accomplir une cybercriminalité et donc de la protection de l'ordinateur montre qu'il existe une possibilité pour lutter efficacement contre la cybercriminalité. L'étude en développant un modèle de dissuasion-répression montre que la combinaison de mesures dissuasives et de mesures répressives dépend des caractéristiques des fonctions d'offre et de demande d'opportunité de cybercriminalité.

En conséquence, pour venir à bout de la cybercriminalité, il faut opérer une combinaison de la dissuasion et de la répression selon les niveaux d'élasticité de la demande et de l'offre des opportunités de cybercriminalité. A ce niveau, deux recommandations principales émergent : Il est intéressant de recommander la prise de mesures de protection des ordinateurs par les utilisateurs ; la solution de distribution de la sécurité de Brenner (2004) devient efficace (cas correspondant à la Fig 2b) ensuite, une bonne politique de formation des diplômés en TIC qui réduit la massification doit être mise en œuvre de manière à ce que l'industrie des TIC absorbe l'ensemble des diplômés ; un système de rémunération qui réduit le turnover et la sortie des cadres TIC du marché formels d'emploi doit aussi être mise en œuvre (cas correspondant à la Fig 2c).

Dans les deux autres cas (Fig 2a et 2d), les politiques publiques de lutte contre la cybercriminalité doivent accorder une plus grande importance aux mesures de répression ; ces mesures de répression dépendent dans ce cas de la nature des peines et amendes appliquées aux cybercriminels arrêtés et condamnés.

Références bibliographiques

Aggarwal, V. (2009), Lead: Cyber crime's rampant, Express Computer, 03 August 2009. http://www.expresscomputeronline.com/20090803/market01.shtml. Dernière consultation 19 août 2011.

Bachmann, M. (2010), «The Risk Propensity and Rationality of Computer Hackers», *International Journal of Cyber Criminology* 4(1-2), 643-656.

Becker, G. (1968), « Crime and Punishment: An economic approach », *Journal of Political Economy* 76(2), 169-217

Bell, R.E. (2002), « The prosecution of computer crime », *Journal of Financial Crime*, 9(4), 308-325.

Blitstein, R. (2007), Cybercops: US targets terrorists as online thieves run amok. *San Jose Mercury News*, 14 november.

Brenner, S. W. (2004), « Toward a criminal law for cyberspace: A new model of law enforcement? », *30 Rutgers Computer and Technology Law Journal* 30, 1-9.

Cardenas, A. A., Radosavac, S., Grossklags, J., Chuang, J., Hoofnagle, C. (2009), An Economic Map of Cybercrime. Working Paper, http://chess.eecs.berkeley.edu/pubs/772/cardenas_2009.pdf .

Dawkins, R. (1982), The extended phenotype. Oxford University Press.

Ehrlich, I. (1996), « Crime, punishment and the market for offenses », *Journal of Economic Perspectives*, 10(1), 43-67.

Gabrys, E. (2002). The international dimensions of cyber-crime, Part 1. *Information Systems Security*, 11(4), 21–32.

Ghernaouti-Hélie, S. (2010), Comment lutter contre la cybercriminalité ? www.itu.int/cybersecurity/Articles/Ghernaouti_PLS391.pdf. Dernière consultation le 25/08/2011.

Giannangeli, M. (2008), Are we ready for Russian Mafia's crime revolution? Sunday Express, Scottish Edition, 3.

Internet Crime Complaint Center (2008), Internet Crime Report, 2007. http://www.ic3.gov/media/annualreport/2007_ic3report.pdf. Dernière consultation 10 juillet 2011.

Internet Crime Complaint Center (2010), Internet Crime Report, 2009. http://www.ic3.gov/media/annualreport/2009_ic3report.pdf. Dernière consultation 23 août 2011.

Iteanu (2004) *Tous cybercriminels*, éd. Jacques-Marie Laffont.

IUT (2009). Comprendre la Cybercriminalité: Guide pour les pays en développement. IUT (2009).

Jen W. Y., Chang W. et Chou S. (2006), Cybercrime in Taiwan – An analysis of suspect records. H. Chen et al. (Eds.): WISI 2006, LNCS 3917, pp. 38-48. Springer-Verlag Berlin Heidelberg 2006.

Jones, B. R. (2007), « Comment: Virtual neighborhood watch: Open source software and community policing against cybercrime », *Journal of Criminal Law & Criminology* 97(2), 601-629.

Joshi, V. (2009), Officials: Criminals cooperate better than police. The Boston Globe. http://www.www.boston.com/news/world/asia/articles/2009/10/12/officials_criminals_cooperate_better_than_police. Dernière consultation 12 juillet 2011.

Katyal, N. K. (2001), « Criminal law in cyberspace », *University of Pennsylvania Law Review* 149 (4), 1003-1114.

Kshetri, N. (2010), The Global Cybercrime Industry, DOI 10.1007/978-3-642-11522-6_2. Springer-Verlag Berlin Heidelberg.

Larsen, E., Lomi, A. (2002), « Representing change: A system model of organizational inertia and capabilities as dynamic accumulation processes», *Simulation Model Practice and Theory* 10 (5), 271-296.

Lavoie, P. (2008). Police et criminalité informatique. De réels problèmes à intervention dans L'univers virtuel. http://www.crimereg.com/police6226/rapports/police_et_cybercriminalite/cyberintro.html. Dernière consultation 7 août 2011.

Lebranchu, M., Hazan, A. (2007), « Répression n'est pas dissuasion » http://reformer.fr/. Dernière consultation 23/08/2011.

McAfee (2006), McAfee virtual criminology report. http://www.sigma.com.pl/pliki/albums/userpics/10007/Virtual_Criminology_Report_2006.pdf. Dernière consultation 23/08/2011.

Messmer, E. (2009), Malware flea market pays hackers to hijack PCs. The Industry Standard.http://www.computerworld.com.au/article/321201/malware_flea_market_pays_hackers_hijack_pcs/ . dernière consultation 19 août 2011.

Norton (2010), Rapport sur la cybercriminalité: l'impact sur les victimes. http://www.influencia.net/data/document/etude-norton.pdf. Dernière consultation 24/08/2011

Nykodym, N., Taylor, R., Vilela, J. (2005), Criminal profiling and insider cybercrime. *Computer Law & Security Report*, 408-414.

Poulsen, K. (2009), Superhacker max butler pleads guilty. http://www.wired.com/threatlevel/2009/06/. Dernière consultation le 25 juillet 2011.

Przyswa, E. (2010), Cybercriminalité et contrefaçon, Editions fyp,

Regan, K. (2006), FBI: Cybercrime causes financial pain for many businesses. TechNewsWorld. http://www.technewsworld.com/story/48417.html. dernière consultation le 25 juillet 2011.

Richtel, M. (1999), Federal cybercrime unit hunts for hackers. New York Times, A16.

Roman, J., Farrell, G. (2002), « Cost-benefit analysis for crime prevention: Opportunity costs, routine savings, and crime externalities » in N. Tilley (Ed.) Evaluation for Crime Prevention, Crime Prevention Studies, 14, 53-92.

Salu, A.O. (2004), « Online crimes and advance fee fraud in Nigeria – Are available legal remedies adequate? », *Journal of Money laundering Control* 8 (2), 159-167.

Sharma, B.B. (2011), « Analysis of the effect of cybercrime on teenagers » *International Referred Research Journal* 2 (18), 17-18.

Shavell, S. (1991), « Individual precautions to prevent theft: Private versus socially optimal behavior », *International Review of Law and Economics* 11 (2), 123-132.

Siegel, L.J. (1992), « *Criminology: Theory, Pattern and Typology* », St. Paul: West Pub. Co 4ème Edition.

Sullivan, B. (2007), Who's Behind Criminal Bot Networks ? April 10. http://news.bbc.co.uk/2/hi/technology/8279867.stm. dernière consultation 4 août 2011.

Sutherland, B. (2008), The Rise of Black Market Data ; Criminals who steal personal data often don't exploit it. Instead, they put it up for sale on one of the many vibrant online markets. Newsweek (International ed.), 152 (24).

Symantec (2008), Global Internet Security Threat Report 2007; Vol XIII.

Symantec (2010), Global Internet Security Threat Report 2009; Vol XV.

Van Dijk, J. (1992), « Understanding Crime Rates: On The Interaction Between Rational Choices of Victims and Offenders », *British Journal of Criminology* 34, 105-121.

Wall, D.S. (1998), « Catching cybercriminals: Policing the Internet », *International Review of Law* 12 (2), 201-218.

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