regards croisés sur l'économie

Compte-rendu de soirée-débat

Cybercriminalité: quels enjeux pour les économies souterraines ?

École normale supérieure
26 mars 2014

Regards croisés sur l'économie est une revue visant à combler le fossé entre la recherche académique et le débat public. Clairs et didactiques, ses articles rendent compte des dernières avancées des sciences sociales, en faisant appel à des spécialistes scientifiquement reconnus.

Cette soirée-débat a été organisée à l'occasion de la parution de son quatorzième numéro, *Lumière sur les économies souterraines*.

Site internet: rce-revue.com
Contact: redaction@rce-revue.com
Compte-rendu rédigé par Camille Dufour et Marine Duros (RCE).

A l'occasion de la sortie de son dernier numéro, *Lumières sur les économies souterraines*, la revue *Regards Croisés sur l'Économie* a organisé, le 26 mars dernier, une soirée-débat sur le thème de la cybercriminalité. Cette soirée a été l'occasion de présenter l'organisation et le fonctionnement des économies parallèles alimentées par les cybercriminels, encore peu connues et pourtant en pleine expansion.
Différentes questions ont été abordées : qui sont les acteurs en jeu dans les marchés de la cybercriminalité ? Quel est le coût de la cybercriminalité pour l'économie réelle ? En quoi son développement modifie les formes que prennent les économies souterraines pré-existantes ? La cybercriminalité a-t-elle fait émerger une forme spécifique d'économie souterraine? Quelles sont les mesures et les moyens disponibles pour lutter contre ces formes de cybercriminalité tout en préservant les libertés numériques individuelles ?

1 Jérôme Saiz, Information Security Analyst

Jérôme Saiz commence par une brève présentation de la place qu'a prise internet dans nos sociétés : plus d'un tiers de la population mondiale y a aujourd'hui accès, et en 2020, six fois plus d'objets que d'hommes seront connectés à Internet. **L'espace internet fournit ainsi un nouveau terrain favorable pour les activités criminelles.** La cybercriminalité représente un véritable marché mettant en jeu des agents spécifiques. Ces criminels de la toile créent des écosystèmes avec leurs propres règles, jargons et coutumes. Il distingue trois types d'acteurs sur ce marché :

1. **le pirate isolé** : il correspond à l'internaute qui se livre seul à une activité pirate (par exemple en profitant d'outils de piratage développés par d'autres, faciles d'accès et simples d'utilisation).

2. **les groupes criminels présents seulement sur le réseau internet** : ces groupes sont **très structurés et centralisés**, chacun de ses membres ayant une fonction bien précise. Il décrit les fonctions-clé suivantes: le codeur qui est en charge de faire "les codes malveillants" ; le hacker qui pénètre et vole les codes bancaires ; le cardeur qui revend les numéros de cartes bancaires ; la mule qui blanchit de l'argent. Enfin, le "manager" se charge de trouver des organisations de spécialistes et de recruter parmi eux. Ces membres n'interagissent entre eux que par internet, sans jamais se rencontrer physiquement. Certains de ces groupes sont suffisamment organisés pour **gérer toute la chaine de la cybercriminalité** (revente de biens illégaux, encaissement et blanchissement d'argent, etc).

3. **les groupes criminels traditionnels** : dans le contexte du développement d'internet, les groupes criminels traditionnels (mafias, gangs) ont récemment commencé à exploiter ce nouveau support pour mener leurs actions. **Ces groupes tirent différemment profit de cet outil, soit en recrutant en interne des spécialistes de la cybercriminalité, soit en "louant" des experts, ou encore en contraignant certains spécialistes à travailler pour eux par l'usage de la force.** Il cite l'exemple du Mexique où des pirates du Net ont été récemment kidnappés par ces groupes criminels traditionnels.

80% des infractions sur Internet sont commises par des groupes. Par ailleurs, Internet permet aux deux types de groupes cités précédemment de collaborer. En ce sens, on assiste à une reconfiguration des activités de l'économie souterraine.

Jérome Saiz fournit ensuite des exemples de pratiques concrètes d'activités cybercriminelles, les sites sur lesquels se déroulent ces activités et les biens qui s'y échangent. Ces activités se déroulent sur des **forums référencés sur Google** où des pirates tentent de proposer des biens ou des services illégaux, sur les *Internet Relay Chat*[1], ou encore **sur le marché noir en ligne non répertorié** par les moteurs de recherches traditionnels et seulement accessible grâce à des réseaux d'anonymisation. On peut citer l'exemple de ***Silk Road*** qui était un marché noir de produits illégaux qui utilise le réseau *Tor* pour assurer l'anonymat des acheteurs et vendeurs, ainsi qu'une monnaie électronique, le ***Bitcoin*** dont la possession n'est pas nominative. Sur ce marché, on peut y échanger des numéros de cartes bancaires (contenu intact de la piste magnétique de la carte bancaire), des comptes bancaires ou Paypal, etc. Les acheteurs de ces numéros vont ensuite répliquer les cartes en questions. **Ces marchés de la cybercriminalité sont très rentables**. Jérôme Saiz nous livre quelques estimations : selon l'United Nations Office on Drugs and Crime, le vol d'identité rapporterait à lui seul 1 milliards de dollars par an; selon le Center for Strategic and International Studies (étude de juillet 2013), la seule fraude en ligne chez les marchands représenterait 3,5 milliards de dollars et le poids du cybercrime se situerait entre 300 milliards et 600 milliards par an. Enfin une étude du Ponemon Institute sur un échantillon de 60 entreprises américaine publiée en 2013 évalue **le coût moyen du cyber-crime à 11,6 millions de dollars par an. Ces activités cybercriminelles représentent selon lui le plus grand transfert de ressources de tous les temps.**

2 Fabien Cozic, consultant en cybercriminalité

Fabien Cozic souligne une évolution des modes d'organisation cybercriminelle. Dans les années 1980, des cybercriminels isolés cherchaient la performance. Kevin Mitnik par exemple est très connu pour avoir piraté très jeune les réseaux de sociétés de télécommunications aux Etats-Unis. Aujourd'hui, on a plutôt affaire à des professionnels qui veulent faire prospérer leurs activités dans le temps long.

L'essentiel des victimes sont issues des petites et moyennes entreprises (PME) car ce sont les plus grandes détentrices de brevets et les plus grands fournisseurs de services. **Le hacker peut retirer de ses attaques un transfert monétaire immédiat mais aussi des savoir-faire ou de l'information sur les stratégies économiques des entreprises visées. Ces attaques relèvent alors de l'espionnage industriel.** Pour s'attaquer aux entreprises du CAC 40, les cybercriminels attaquent "par rebonds", c'est-à-dire qu'ils s'attaquent aux sous-traitants dans un premier temps. Ils y visent une personne stratégique en particulier, la surveillent et lui soutirent les informations qui leur permettront de remonter vers la grosse entreprise cible.
Fabien Cozic distingue différents types d'attaques :

[1]Protocole de communication textuelle sur internet

1. **le vol de données qui est opéré par des logiciels malveillants**. La récente attaque contre la troisième chaîne de distribution américaine "Target" est un cas d'école. Les attaquants ont installé des *malwares*[2] sur les terminaux de paiement, qui ont extrait les informations bancaires de la mémoire vive des caisses enregistreuses. Les substitutions de terminaux de paiement par des appareils identiques équipés d'un système d'émission par bluetooth et d'un *skimmer* qui capte les données bancaires sont de plus en plus courantes dans les commerces en France.

2. **l'usurpation d'identité** mise au point grâce à l'information recueillie sur les réseaux sociaux et dans les organigrammes mis en ligne. Le *phishing*[3] ou les arnaques aux faux ordres de virement en sont des exemples.

3. **le chantage** avec menace de mise à plat de serveur d'entreprise ou de parcelles de *data center* par un *malware* ou un *botnet*[4].

Comment s'en prémunir? Il faut se fournir en pare-feu et de sécuriser ses informations sur les réseaux sociaux. On parle d'"hygiène informatique". Et la métaphore ne s'arrête pas là puisque les épidémiologistes s'inspirent des modes de contamination informatique pour modéliser la propagation des maladies.

En conclusion, Fabien Cozic précise bien que la dimension technique de ces infractions n'est ni le mal ni le remède, c'est bien le facteur humain qui est à la racine de ces actes criminels.

3 Myriam Quenemer, magistrate

Myriam Quenemer commence par se livrer à un exercice de définition. La cybercriminalité recouvre tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent. La commission européenne y distingue trois formes d'infractions : les infractions propres aux réseaux électroniques de type piratage; les infractions qui reprennent les formes traditionnelles de criminalité et les infractions qui consistent à diffuser des contenus illicites (pédopornographie, racisme).
La délinquance se déplace en parallèle de l'action humaine : elle est devenue numérique. En réponse à cela, la justice doit se doter de nouveaux modes d'investigation. **Trois caractéristiques propres à la cybercriminalité posent problème : combattre ces infractions nécessite des compétences techniques, beaucoup d'infractions sont extraterritoriales, et enfin les délits se multiplient car le passage à l'acte est beaucoup plus facile dans un espace numérique qui distance l'agresseur de la victime.**
Quelle est la traduction juridique de ces modes opératoires **? La loi informatique et libertés de 1978 est la première à donner un cadre au traitement de données**

[2]Logiciels malveillants

[3] Arnaque visant à soutirer de l'argent à des particuliers en se faisant passer par mail pour un tiers de confiance (la banque de la victime par exemple).

[4]Réseau de programmes connectés à internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches

nominatives, en créant notamment la Commission Nationale de l'Informatique et des Libertés (CNIL). Sur ces questions, le droit pénal évolue ensuite sous l'impulsion du développement du crime organisé et du terrorisme. En 2001, la loi relative à la sécurité quotidienne permet de conserver les données de trafic jusqu'à un an, *i.e.* les données permettant d'identifier toute utilisation des réseaux de communication. Une série de lois votées en 2004 font des données informatiques un objet de réquisition et désignent des juridictions spécialisées. Enfin en 2011, la loi LOPSI II définit le délit d'usurpation d'identité sur internet au terme d'un long débat sur le *phishing* et permet d'intercepter le réseau internet dans le cadre d'une enquête. La convention de Budapest d'août 2011 est le premier traité international en matière de lutte contre la cybercriminalité. Son principal objectif, énoncé dans le préambule, est de poursuivre "une politique pénale commune destinée à protéger la société contre le cyber-crime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale".

Cependant, Myriam Quenemer regrette l'absence d'une réelle politique publique et pénale globale. **Des lacunes législatives subsistent : le vol d'éléments immatériels n'est pas explicitement traité dans la loi et certaines infractions déjà complexes à définir comme le blanchiment ou la traite des êtres humains sont complexes à caractériser lorsqu'elles sont commises via les réseaux numériques.** D'autre part, les données sur le phénomène sont encore approximatives. Une réelle coopération public / privé doit se mettre en place pour avoir une vue d'ensemble du phénomène.

4 Rodolphe Durand, professeur à HEC

Rodolphe Durand ouvre la discussion en proposant une **réflexion plus générale sur les organisations pirates**. Selon lui, leur essor est à relier aux évolutions du capitalisme moderne. Tout au long de l'histoire, ces organisations ont émergé en réaction à la volonté des Etats de détenir le monopole de certains territoires (monopole de ressources, dans la définition des normes, etc). Ces pirates ont alors cherché à conquérir de nouveaux espaces de libertés au sein même de ces territoires.

Il revient ainsi sur l'histoire des premiers pirates qui date de la découverte de l'Amérique : à cette époque, les monarchies européennes revendiquaient les routes maritimes commerciales qu'ils avaient "découvertes". Ainsi, certains marins alors exploités par la marine marchande ont cherché à s'organiser en s'unissant à des groupes établis sur les côtes américaines afin de récuser ce droit de propriété affirmé par les Etats européens. L'argument principal contre ces monopoles était la légitimité d'un commerce maritime ouvert à tous. Les Etats finissent par entendre cet argument en créant les eaux internationales. De nouvelles formes de pirateries se sont ensuite succédées, dans ces périodes de révolutions territoriales liées aux mutations du capitalisme : on peut penser aux radios pirates qui se sont opposées au monopole des ondes par la BBC au milieu du XXème siècle ; aujourd'hui, à la piraterie internet avec *Wikileaks*, *Anonymous*, *MegaUpload* qui contestent le pouvoir de marché de Google ou Microsoft ; ou encore la piraterie génétique avec le développement de sites comme *Do It Yourself Bio* gérés par des "biohackers" capables d'assembler des séquences d'ADN synthétiques. Rodolphe Durand explique qu'une piraterie de l'espace apparaîtra probablement.

Il opère ensuite une **distinction entre l'organisation pirate et l'organisation mafieuse**,

chacune d'entre elles ayant un rapport différent aux territoires, à un niveau local et global. En effet, l'organisation pirate est illégitime à un niveau local et prolifère plus la souveraineté étatique est forte puisque son but est d'entrer en contestation avec celle-ci. Toutefois, s'il existe ce qu'il appelle un "consensus normatif global" (au delà de l'échelle nationale), l'organisation périclite. A l'inverse, la mafia est illégale mais détient une certaine légitimité locale ; si la souveraineté locale est forte, la mafia périclite. L'organisation mafieuse, à l'inverse de l'organisation pirate, cherche davantage à s'infiltrer dans l'Etat.

Pour conclure, il évoque le complexe triptyque que forment l'Etat, les entreprises et les organisations pirates, chacun d'entre eux interagissant et ayant des frontières relativement floues. Le capitalisme marchand est profondément lié à la notion d'Etat souverain. **Selon lui, l'Etat crée des normes marchandes que les entreprises traditionnelles peuvent suivre pour s'implanter mais qui sont contestées par les pirates. Ainsi, ces derniers recréent toujours les frontières de l'Etat qui finit par prendre en compte ces revendications en adoptant de nouvelles lois sur le territoire en question.** Rodolphe Durand conclut en expliquant que les cyberpirates ne sont pas contre le capitalisme : ils luttent davantage contre les monopoles (d'entreprises, d'Etat) et sont en ce sens de fervents défenseurs de la concurrence et de la liberté économique sur des territoires considérés comme un bien commun.

5 Débat

Les intervenants notent un décloisonnement croissant des activités criminelles. Le blanchiment d'argent par le biais des monnaies virtuelles est typiquement utilisé par les trafiquants d'armes, de stupéfiants ou même par les terroristes. Les armes en pièces détachées sont échangées sur internet. Le trafic de données bancaires peut être lié au terrorisme. Les modes d'investigation doivent s'adapter en conséquence note Myriam Quenemer. Ainsi la collaboration des douanes, des sites internet et des postes est nécessaire.
La mobilisation contre la cybercriminalité se fait à plusieurs niveaux. Jérome Saiz signale que les banques rachètent parfois les codes volés de cartes bancaires aux criminels pour en comprendre les failles. Myriam Quenemer rappelle l'importance de la coopération internationale en soulignant la création récente du centre européen de lutte contre la cybercriminalité (EC3). Enfin Fabien Cozic nous parle de la "phishing initiative", plateforme sur laquelle les internautes sont invités à signaler les adresses de sites de *phishing*.
Concernant l'interception, Jérome Saiz et Myriam Quenemer insistent sur la différence entre le champ judiciaire et le champ administratif. Des logiciels permettent maintenant de faire des liens entre certaines transactions, certains appels ou échanges de données et des activités criminelles. En cela, la preuve sera de plus en plus numérique. Mais les interceptions judiciaires sont encadrées par les juges et sont soumises à des lois restrictives. Myriam Quenemer cite la loi sur la géolocalisation judiciaire du 1er mars 2014 à titre d'exemple. Les interceptions administratives sont elles gérées par une commission et leur réalisation est soumise à l'accord du Premier Ministre. La loi de programmation militaire votée en décembre dernier multiplie les intervenants capables de demander des accès administratifs aux données personnelles.

La loi qui permet de conserver les données de trafic jusqu'à un an a suscité

des réactions du public y voyant une violation des libertés individuelles. Myriam Quenemer répond que ces données ont permis de faire aboutir un certain nombre d'affaires et que la perquisition peut être en un sens plus "intrusive" que le bornage qui consiste à récupérer des données a posteriori et non en temps réel comme le fait la géolocalisation. C'est une question de modèle de société, il s'agit de trouver le bon équilibre entre une justice qui se donne les moyens d'investigation, y compris sur ces nouveaux champs, et une surveillance accrue et abusive des citoyens.

Pour aller plus loin

Durand R., Vergne J.-P. (2010), *L'organisation pirate : Essai sur l'évolution du capitalisme*, Editions Le Bord de l'eau.
Quenemer M., Charpenel Y. (2009), *Cybercriminalité, droit pénal appliqué*, Economica.
Quenemer M. (2013), *Cybersociété entre espoirs et risques*, L'harmattan.
Lumière sur les économies souterraines (2014), *Regards croisés sur l'économie*, 14, La Découverte.