# Projet de recherche n°7: Le crime organisé: nouvel acteur dominant dans le cyberespace?

## Contexte

**Deux milliards de dollars** : c'est le coût estimé de la cybercriminalité en 2019[1]. Le cyberespace est le **nouveau paradis des réseaux criminels**. Premièrement, le coût d'entrée est très faible, le risque de détection, de perturbation et de répression est faible, et les échappatoires réglementaires sont faciles à exploiter[2]. Même pour les **fraudes et les pirates informatiques**les plus complexes, les réseaux criminels n'ont besoin que d'une **connexion Internet**, d'un **ordinateur**et de logiciels ou **programmes malveillants** (virus) **à des prix de plus en plus attractifs**. La main-d'œuvre n'est pas non plus difficile à trouver, les **cyber-mercenaires** gagnent en réputation et se forgent une identité **en travaillant avec ou contre certains États**, pour certains **principes cyber-politiques** (neutralité de l'internet par exemple) ou en devenant des **cyber-filiales de grandes mafias**. La **location de capacités cyberoffensives** au plus offrant[3] et la**force de ces réseaux parapublics** entraînent une **imbrication croissante** de ces groupes criminels avec les États[4]. Cette coopération tend à renforcer considérablement la capacité de ces réseaux et la disponibilité de moyens techniques avancés dans le Darknet pour tous les réseaux criminels du monde, comme illustré par les virus **WannaCry** et **NotPetya**.

Outre la **sophistication des modes opératoires criminels**et le **renforcement de leurs structures**, la cybercriminalité offre la possibilité de générer de nouveaux profits en identifiant de **nouvelles opportunités d'enrichissement**, en proposant constamment de **nouveaux services innovants** et, si possible, en tirant parti de**sources de revenus faciles** [5]. La **numérisation des vices**de la société, notamment la prostitution et le jeu, les drogues synthétiques ou les armes, est une**source importante de revenus** pour les réseaux criminels.

## Cybermenaces émergentes

Aujourd'hui, la majorité de la cybercriminalité consiste encore en un**logiciel de rançon**, qui permet de **garder les données en otage** [6]. Jusqu'à présent, l'approche des réseaux criminels reposait sur le **volume d'opérations** souvent dispersées et à revenu relativement faible. Cependant, **98% des données sont maintenant numérisées dans le monde entier**et cette part continue d'augmenter. Le cyberespace est donc le moyen de transporter des données **de plus en plus précieuses**, mais c'est aussi un **vecteur de coercition**avec l'utilisation d'**attaques DDOS**(déni de service distribué), de virus de plus en plus sophistiqués (**Wannacry** par exemple) ou de **cyber-attaques de type StuxNet**. Par exemple[7], l'utilisation croissante des méthodes de paiement à distance, l'augmentation du nombre de transactions électroniques et la délocalisation de données offrent aux réseaux criminels de nouvelles possibilités de **monétiser les identifiants**, **les informations personnelles et les données provenant d'actifs immatériels** qu'ils extorquent, notamment en les vendant à des entreprises légitimes, au chantage de personnes les opérateurs[8].

Des cybercriminels ont récemment racheté des entités privées et publiques, telles que l'hôtel de ville d'Atlanta aux États-Unis, et ces prises d'otages ont entraîné une **augmentation significative du prix moyen facturé**pour le déverrouillage des données ou de l'accès au réseau. Le **ciblage** et la **construction de fraudes financières en ligne** se sont également améliorés, en particulier sous l'influence des **syndicats du crime nigérians**[9]. Le nombre d'attaques a également considérablement augmenté avec le **vol de données**, pouvant inclure des industries entières de l'**armement**, les données de **consommateurs** d'une entreprise, l'influence d'une **élection** ou toutes **les données de**

**santé publique d'un pays**. L'impact sur ces entreprises et institutions publiques (en termes de finances, d'opérations ou de réputation) et in fine sur la vie des citoyens peut être catastrophique.

En effet, le nombre d'**appareils en réseau** (50 000 milliards en 2040 selon certaines estimations), de **données collectées et enregistrées automatiquement** ou d'**infrastructures et d'industries automatisées** continuera à augmenter dans les années à venir. Toutes ces **données**, **empreintes digitales** et **signatures numériques** individuelles ou collectives, ou le contrôle de ces entités automatisées deviendront une **proie de choix pour les réseaux criminels**. Ces développements créent non seulement de **nouvelles vulnérabilités exploitables** en termes de **vol**et de **fraude**, mais également en termes de **pouvoir**. En effet, le**chantage** qu'un réseau criminel peut exercer sur un État, des multinationales ou des gouvernements sur la base de leur propriété ou du contrôle de leurs données numériques pourrait constituer une**cyber-puissance majeure**[10].

## Questions de recherche associées

Mener des études transversales, allant de la psychologie à l'ingénierie sociale et sociétale, et en particulier concernant le *modus operandi* des cybercriminels afin d'étudier leurs**profils**, leurs **chemins de recrutement et de guérison**, mais aussi d'identifier leurs **vulnérabilités**et les meilleurs moyens de les combattre.

La montée d'acteurs criminels dans la cyber-protection peut-elle contester la souveraineté des États et **modifier l'équilibre des pouvoirs** dans les relations internationales?

Les**mafias** pourraient-elles développer un nouveau **pouvoir d'intermédiation** entre les États et les populations à travers le cyberespace?

Le cyberespace confère-t-il**structurellement** un avantage plus important que l'expansion du pouvoir de la mafia sur tout autre acteur de la scène internationale?

Quels sont les exemples français du développement de **nouveaux foyers criminels** dans le cyberespace?

---

[1] Cockayne, James and Roth, Amanda (2017), "Crooked States: How organized crime and corruption will impact governance in 2050 and what states can – and should – do about it now", United Nations University.

[2] Baumard, Ph, "Comparing National Approaches and Doctrines in Cyber-Security", International Forum on Cyber-Security Cooperation. Garmisch 23/04/2013

[3] Champeyrache, Clotilde, "Crime Societies. A world tour of mafias", CNRS editions, Paris. Reissue in pocket format / new pocket edition: 2011.

[4] Gayraud Jean-François and Thual François, "Geostratégie du crime", Odile Jacob, Paris, 2012.

[5] Adeniyi, T. 2015, "Nigerian Cyber-crime in Nigeria hits $9.3bn annually", Daily Trust (online).

[6] Cockayne, J. (2016), "Hidden Power: the Strategic Logic of Organized Crime" ,Oxford University Press.

[7] Cockayne, James and Roth, Amanda (2017), "Crooked States: How organized crime and corruption will impact governance in 2050 and what states can – and should – do about it now",United Nations University.

[8]James Cockayne, "Chasing Shadows : Strategic Responses to Organised Crime in Conflict-Affected Situations", The RUSI Journal, vol.158, pages 10-24, 28 Avril 2013.

[9] James Burns, "The Insurance Industry: An Important Part of the Fight against Cybercrime", 16 mai 2018.

[10] Cockayne, James and Roth, Amanda (2017), "Crooked States: How organized crime and corruption will impact governance in 2050 and what states can – and should – do about it now", United Nations University.

https://esd.cnam.fr/projets-de-recherche-cooperation-scientifique/projets-de-recherche/projet-de-recherche-n-7-le-crim