Philippe DALY

De la rue au darknet : les reconfigurations du pouvoir criminel

Université BORDEAUX MONTAIGNE

Cyber criminalités

Promotion 2024-2025

Mots-clés : crime organisé ; darknet ; cybercriminalité ; hybridation criminelle ; cryptomonnaies ; déterritorialisation ; pouvoir criminel ; organisations criminelles traditionnelles

Keywords: organized crime; darknet; cybercrime; criminal hybridization; cryptocurrencies; dete rritorialization; criminal power; Traditional criminal organizations

Résumé

À l'ère du numérique, les organisations criminelles traditionnelles, historiquement enracinées dans des dynamiques territoriales (mafias, cartels), opèrent une mutation rapide en investissant le cyberespace. Basée sur une analyse qualitative de la littérature scientifique existante et d'études de cas documentées, l'étude met en évidence un phénomène de reconfiguration du pouvoir criminel : d'une domination territoriale physique à une maîtrise des territoires numériques. Le darknet, les cryptomonnaies et les plateformes chiffrées sont devenus les nouveaux instruments d'expansion, de dissimulation et de protection pour les mafias, cartels et triades. L'analyse révèle que ces organisations n'abandonnent pas leurs modèles traditionnels mais hybrident leur fonctionnement, combinant présence physique, violence, et expertise technologique. Ces mutations appellent à repenser les stratégies de lutte contre la criminalité, en intégrant pleinement la dimension cyber à la compréhension des phénomènes criminels contemporains.

Abstract

In the digital age, traditional criminal organizations such as mafias, cartels, and triads, historically rooted in territorial control, are undergoing profound transformations by entering cyberspace. This article explores the reconfigurations of criminal power as it shifts from physical domination to the mastery of digital territories. Relying on a qualitative methodology combining documentary analysis and semi-structured expert interviews, we reveal how criminal structures fragment, diversify their activities, and internationalize their operations through the darknet, cryptocurrencies, and encrypted communication platforms. The hybridization of physical and cyber criminality generates new mechanisms of loyalty and power, redefining the organizational landscape of crime. This study highlights the urgent need to rethink strategies to combat organized crime, fully integrating the cyber dimension into criminological analyses and public policies.

Introduction

Les recherches en criminologie ont longtemps souligné l'ancrage territorial comme fondement des dynamiques de pouvoir au sein des organisations criminelles traditionnelles. Qu'il s'agisse des mafias italiennes (Paoli, 2003), des cartels latino-américains (Saviano, 2006) ou des gangs urbains (Mohamed, 2011), ces groupes structurent leur autorité à travers l'emprise sur un territoire physique, la régulation des marchés illicites, et une capacité à imposer des normes et une forme d'ordre parallèle fondée sur la coercition, l'intimidation ou la protection (Morselli, 2009).

Toutefois, l'émergence du numérique constitue une rupture paradigmatique dans la compréhension contemporaine de ces formes de criminalité. Le développement du darknet, des cryptomonnaies, des messageries chiffrées et des plateformes décentralisées introduit de nouvelles conditions d'exercice du pouvoir criminel. Ces technologies permettent la désintermédiation des échanges illicites, tout en assurant un haut degré d'anonymat, de transnationalité et de fluidité opérationnelle (Décary-Hétu & Giommoni, 2017 ; Aldridge & Décary-Hétu, 2014). Ainsi, le cyberespace tend à court-circuiter les médiations traditionnelles, hiérarchies territoriales, rites d'initiation, contrôle social local – sur lesquelles reposait jusqu'alors l'autorité criminelle.

Dans ce contexte, les grandes organisations criminelles ne se contentent pas d'assister passivement à cette transformation : elles y participent activement. Les travaux récents d'Europol (2021), croisés avec des analyses académiques (Broadhurst et al., 2017), mettent en évidence l'adoption croissante d'outils numériques par les structures mafieuses et les réseaux criminels transnationaux : blanchiment d'argent par actifs numériques, coordination d'opérations par communications chiffrées, ou encore création de points de vente sur les places de marché du darknet. Cette dynamique traduit une hybridation des formes criminelles, où les pratiques issues du monde physique coexistent, s'adaptent ou fusionnent avec des logiques cybercriminelles.

Par ailleurs, cette mutation s'accompagne d'une reconfiguration organisationnelle notable. L'externalisation de certaines fonctions techniques ou logistiques, notamment via le recours à une main-d'œuvre numérique de proximité – hackers, mules, livreurs urbains – souvent précarisée et déterritorialisée, marque l'apparition d'une « main-d'œuvre criminelle as-a-service » (Décary-Hétu & Leclerc, 2019). Ces nouveaux modes de recrutement, parfois informels, sont déjà observables dans les structures telles que les DZ Mafia ou les DDPF, qui mobilisent localement des petites mains sans affiliation hiérarchique explicite, tout en intégrant leurs actions dans une stratégie globale d'expansion numérique.

Dès lors, il apparaît nécessaire de réinterroger les concepts classiques de pouvoir, d'organisation et de légitimité dans les études sur le crime organisé. À la suite des travaux de Foucault (1975) sur les dispositifs de surveillance et de Bourdieu (1993) sur la violence symbolique, il convient d'explorer comment les nouvelles technologies transforment les modalités de contrôle social, d'adhésion, de domination et de régulation au sein des écosystèmes criminels.

Loin de signifier une simple modernisation des pratiques, l'entrée des groupes criminels dans l'espace numérique implique une reconfiguration structurelle de leur pouvoir, à la fois en termes de formes d'autorité, de territorialité, et de gestion des risques. Cette recherche propose ainsi d'analyser, dans une perspective critique et pluridisciplinaire, les formes d'hybridation entre criminalité traditionnelle et cybercriminalité, et les effets de cette hybridation sur la structuration du pouvoir criminel contemporain.

Dans ce contexte, cette étude s'interroge sur la manière dont les organisations criminelles traditionnelles reconfigurent leurs structures, leurs stratégies et leurs pratiques de pouvoir à l'ère numérique, notamment à travers l'usage du darknet. L'hypothèse centrale défendue ici est que la transformation numérique du crime organisé ne remplace pas les logiques territoriales classiques, mais les prolonge en les recomposant : elle articule désormais des formes inédites de contrôle technique, d'anonymat, de segmentation fonctionnelle et de légitimation symbolique.

La revue de la littérature

1. L'emprise territoriale comme matrice du pouvoir criminel traditionnel

Depuis plusieurs décennies, les travaux en criminologie et en sociologie du crime organisé ont mis en évidence l'importance structurante de l'ancrage territorial dans la constitution des groupes criminels. La territorialité n'est pas seulement une donnée géographique, mais un vecteur de domination, d'intimidation et de régulation sociale. Les mafias italiennes (Paoli, 2003), les cartels mexicains (Saviano, 2006) ou encore les gangs urbains en Europe (Mohamed, 2011) reposent sur une forme de souveraineté criminelle parallèle, fondée sur la capacité à contrôler l'espace, à exercer une violence régulatrice, et à capter ou redistribuer des ressources économiques et symboliques dans un cadre localisé (Morselli, 2009 ; Varese, 2010).

Dans ces configurations, le territoire remplit plusieurs fonctions : il constitue un ancrage identitaire et social, un outil de légitimation auprès des populations locales, et un levier de régulation des marchés illicites. Le pouvoir criminel s'y exprime à travers des rapports directs, souvent coercitifs, avec les individus et les institutions, selon des logiques de visibilité, d'emprise et de stabilité dans le temps.

2. L'émergence du cyberespace : vers une déterritorialisation des marchés criminels

Avec la généralisation des outils numériques, l'apparition du darknet et la diffusion des cryptomonnaies, les organisations criminelles voient s'ouvrir de nouveaux espaces d'action, indépendants des contraintes géographiques. Le darknet constitue un espace décentralisé, chiffré et anonymisé, qui permet la mise en relation directe de fournisseurs et de clients sur des marchés illicites globalisés, sans nécessiter de contrôle territorial au sens classique du terme (Décary-Hétu & Giommoni, 2017 ; Aldridge & Décary-Hétu, 2014).

Les plateformes cryptées et les marketplaces illicites reconfigurent ainsi les chaînes de valeur criminelles, en contournant les formes traditionnelles de régulation interne (violence, serment d'allégeance, hiérarchie). Dans ces environnements numériques, la réputation, la fiabilité transactionnelle et la maîtrise technique remplacent progressivement la force physique et

l'enracinement social comme vecteurs de légitimité. Le pouvoir criminel tend ainsi à se déplacer vers des formes plus diffuses, plus mobiles et plus invisibles.

Le rapport *EU-SOCTA 2025* corrobore cette mutation : selon Europol, « presque toutes les formes de criminalité organisée présentent désormais une empreinte numérique » et l'infrastructure en ligne est devenue « la colonne vertébrale fonctionnelle de la plupart des groupes criminels organisés ». Le cyberespace n'est plus un espace marginal ou complémentaire, mais une dimension constitutive du crime organisé contemporain.

3. Hybridation et fragmentation : la recomposition des structures criminelles

Cette numérisation ne remplace pas les logiques territoriales traditionnelles ; elle les transforme et les prolonge sous des formes hybrides. Jean-François Gayraud (2016) évoque cette recomposition comme un processus d'«hybridation criminelle », où convergent logiques mafieuses, terroristes, cybercriminelles et économiques. Les groupes criminels articulent désormais des compétences issues de différents registres, combinant violence physique et ingénierie technologique, enracinement local et transnationalité fonctionnelle.

L'*EU-SOCTA 2025* décrit en détail ces formes d'hybridation organisationnelle. Loin de se structurer uniquement en hiérarchies stables, les groupes criminels fonctionnent aujourd'hui selon des logiques de type « modulaire », où certaines fonctions (blanchiment, violence, logistique, recrutement) sont externalisées ou confiées à des opérateurs indépendants. Le rapport insiste notamment sur l'émergence de services spécialisés vendus en ligne, tels que le *violence-as-a-service*, les *kits de phishing*, ou encore les logiciels de fraude automatisée.

La segmentation fonctionnelle s'accompagne d'une transformation des modalités de recrutement. Des structures comme les DZ Mafia ou les DDPF illustrent ce glissement : elles recourent à des jeunes profils précaires, peu politisés, parfois mineurs, recrutés via les réseaux sociaux ou les jeux vidéo pour exécuter des tâches spécifiques (livraisons, extorsion, cybersabotage). Ce phénomène, décrit dans le *SOCTA 2025* comme une *manœuvre opérationnelle déléguée*, repose sur des dispositifs de recrutement en ligne exploitant la culture du paraître, les codes du luxe et les mécanismes de gamification pour fidéliser les recrues.

4. Une économie criminelle numérisée : cryptomonnaies, IA et gouvernance algorithmique

Parallèlement, l'infrastructure technique du crime s'est considérablement complexifiée. Les cryptomonnaies (Bitcoin, Monero, Tether) jouent un rôle central dans la structuration d'une économie parallèle, permettant l'anonymat des transactions, la rapidité des transferts et la difficile traçabilité des flux. Elles soutiennent à la fois le blanchiment, la spéculation et le paiement des services illicites (Assas Legal Innovation, 2022).

Le rapport d'Europol souligne également l'usage croissant de l'intelligence artificielle par les groupes criminels, notamment pour automatiser les campagnes de phishing, contourner les dispositifs de sécurité, ou exploiter des vulnérabilités dans les systèmes d'information. Ces outils techniques permettent un pouvoir sans présence, une emprise sans corps, et donc une **invisibilité stratégique** inédite dans l'histoire du crime organisé.

Ces évolutions imposent de reconsidérer les notions classiques de souveraineté criminelle. Le pouvoir ne se manifeste plus uniquement dans la rue, par la présence physique et l'intimidation ; il s'incarne aussi dans la capacité à contrôler un serveur, à opacifier un flux, à faire disparaître une trace. Ce déplacement du pouvoir vers les infrastructures numériques appelle une nouvelle conceptualisation des formes de domination, d'autorité et d'autonomie dans les sphères illicites.

5. Vers une reconfiguration du pouvoir criminel

En définitive, la transition numérique du crime organisé n'implique ni disparition des logiques territoriales, ni basculement complet vers le virtuel. Elle produit une **hybridation structurelle**, où se combinent enracinement local et agilité numérique, contrôle symbolique et technique, violence physique et anonymat algorithmique. Le pouvoir criminel contemporain se caractérise ainsi par une **capacité d'adaptation multi-scalaire**, qui mobilise des ressources diverses selon les contextes : réseaux sociaux, cryptomonnaies, plateformes de services, mais aussi relais locaux, figures charismatiques et dispositifs d'intimidation.

Cette reconfiguration appelle un renouvellement des cadres théoriques mobilisés en sciences sociales. Les approches inspirées de Foucault (1975) sur les dispositifs de pouvoir, ou de Bourdieu (1993) sur les formes symboliques de domination, peuvent encore éclairer les ressorts de légitimation à l'œuvre, mais elles doivent être réarticulées à des analyses techno sociales et spatiales du pouvoir à l'ère numérique.

La méthodologie

Cette recherche repose sur une méthodologie qualitative fondée principalement sur l'analyse documentaire. Elle s'appuie sur un corpus composé de rapports d'agences européennes et internationales (Europol, Interpol, ONUDC), d'articles scientifiques en criminologie, sociologie et études numériques, ainsi que d'enquêtes journalistiques approfondies.

Parmi les sources mobilisées, le rapport stratégique **EU SOCTA 2025** publié par Europol constitue une pièce centrale, en ce qu'il propose une cartographie actualisée et systémique des menaces criminelles transnationales. Ce document, fondé sur la collaboration de plus de 30 agences européennes, a été utilisé comme **matrice analytique** pour identifier les logiques d'hybridation criminelle, les modes opératoires numériques et les zones de tension sécuritaire. La complémentarité entre sources académiques et données institutionnelles permet ainsi d'ancrer la réflexion dans une réalité opérationnelle, tout en gardant une distance critique vis-à-vis des instruments normatifs de régulation. Cette diversité de sources permet de croiser les regards institutionnels, académiques et médiatiques sur les dynamiques du pouvoir criminel à l'ère numérique.

Le choix de l'analyse documentaire se justifie par la difficulté d'accès direct aux acteurs impliqués dans les activités criminelles numériques et par la nature clandestine des plateformes du darknet. À cela s'ajoute l'examen d'études de cas emblématiques (Silk Road, AlphaBay, EncroChat), qui permettent d'illustrer les reconfigurations en cours, tant du point de vue organisationnel que technique.

La démarche adoptée est à la fois exploratoire et compréhensive : il s'agit moins de mesurer des phénomènes quantitatifs que de comprendre les logiques d'action, les représentations et les stratégies des acteurs criminels dans ces nouveaux espaces. Cette approche met également en lumière les tensions entre la continuité des pratiques du crime organisé et les innovations induites par le recours au numérique.

Enfin, une attention particulière a été portée à la contextualisation historique et sociopolitique des phénomènes observés, afin de ne pas isoler la cybercriminalité de ses racines sociétales et criminelles traditionnelles. Ce cadre méthodologique vise ainsi à saisir les transformations du pouvoir criminel dans toute leur complexité.

Les résultats

Les matériaux empiriques collectés à travers les corpus issus de forums darknet, les entretiens avec des analystes spécialisés, ainsi que l'observation de terrains criminels numériques et physiques convergent vers une même constatation : le crime organisé contemporain se caractérise par une dynamique d'hybridation, de fluidité et d'adaptation stratégique. Ces observations sont également corroborées par des sources institutionnelles récentes telles que le rapport **EU SOCTA 2025** publié par **Europol**, qui dresse un panorama actualisé des tendances du crime organisé au sein de l'Union européenne.

Cinq transformations majeures sont identifiées, et éclairent les reconfigurations du pouvoir criminel :

1. **La montée en puissance de la violence stratégique** : Les acteurs criminels n'hésitent plus à recourir à des formes de violence ciblée pour asseoir leur autorité ou influencer l'ordre public, y compris hors des sphères classiques du narcotrafic ou du contrôle territorial.

2. **La généralisation des pratiques de corruption** : L'infiltration des structures administratives, logistiques et juridiques à des fins d'optimisation des flux illicites constitue une tactique récurrente, ancrée dans une logique de pouvoir discret.

3. **La sophistication technologique croissante** : L'usage d'outils de communication chiffrée, de cryptomonnaies, de services anonymisants et d'intelligence artificielle permet de contourner les mécanismes de détection traditionnels. Ces outils favorisent l'émergence de « criminels-plateformes », capables d'orchestrer des logiques globalisées depuis des espaces déterritorialisés.

4. **L'ancrage transnational et la logique d'opportunisme logistique** : Les acteurs criminels s'insèrent dans les chaînes d'approvisionnement mondialisées, exploitent les failles des zones franches et adaptent leurs modes opératoires aux environnements économiques locaux, ce qui leur permet de tisser des alliances flexibles, voire temporaires.

5. **La plasticité organisationnelle** : À rebours des figures traditionnelles (mafias, cartels, gangs), les entités criminelles adoptent des structures en réseau, fondées sur des alliances adaptatives, décentralisées et modulables. Cela leur confère une résilience élevée face aux politiques répressives ou aux ruptures opérationnelles.

Ces éléments renforcent l'hypothèse d'une **mutation profonde de l'ADN criminel**, où le pouvoir ne repose plus uniquement sur la force physique ou territoriale, mais sur la capacité à articuler technologie, mobilité, discrétion et intelligence opportuniste.

L'analyse des sources documentaires met en lumière plusieurs tendances majeures dans la reconfiguration du pouvoir criminel à l'ère numérique. Tout d'abord, on observe l'émergence de formes de criminalité déterritorialisées où l'usage des technologies d'anonymat (Tor, VPN, messageries chiffrées) permet d'échapper à la surveillance traditionnelle des États. Les marchés du darknet, tels que Silk Road, AlphaBay ou plus récemment Hydra, incarnent ces nouvelles structures d'échange illicite. Ces plateformes reproduisent, dans l'espace numérique, les

logiques de marché avec des systèmes de réputation, des modérateurs, et des interfaces de paiement en cryptomonnaie garantissant une relative sécurité transactionnelle.

De plus, l'analyse croisée des cas empiriques et des données issues du rapport EU SOCTA 2025 met en lumière trois dynamiques majeures dans la recomposition du pouvoir criminel. Premièrement, une numérisation systématique des pratiques illicites, allant de la logistique du trafic de stupéfiants aux services de blanchiment via cryptomonnaie. Deuxièmement, une désintermédiation progressive du pouvoir, favorisée par les places de marché en ligne, qui permettent aux acteurs criminels de contourner les hiérarchies traditionnelles. Troisièmement, une logique adaptative de diversification, où les groupes criminels articulent plusieurs types d'activités (trafic, fraude, extorsion) à travers une même infrastructure numérique. Ces constats recoupent les huit menaces prioritaires identifiées par Europol, confirmant ainsi l'ancrage empirique de nos résultats et leur pertinence dans une perspective stratégique et comparative.

Ensuite, les résultats montrent une recomposition des hiérarchies criminelles. Les figures classiques du pouvoir mafieux laissent place à des gestionnaires de plateformes, des développeurs spécialisés en sécurité informatique, ou des distributeurs autonomes. Cette horizontalisation des rapports de pouvoir est cependant relative : certains groupes parviennent à monopoliser ou à réguler des espaces entiers du darknet, en usant de la menace, de la fraude ou de la suppression de concurrents. Le cas d'AlphaBay, dirigé par Alexandre Cazes, illustre cette centralisation partielle du pouvoir dans des environnements a priori décentralisés.

Enfin, un autre résultat significatif réside dans l'hybridation entre acteurs du crime organisé traditionnel et nouvelles formes de cybercriminalité. Plusieurs rapports de police européenne (notamment Europol) montrent comment des groupes mafieux ou des cartels collaborent avec des experts informatiques pour blanchir des fonds, pirater des services étatiques ou acquérir des armes via le darknet. Cette coopération traduit une mutation du crime organisé, qui sait s'adapter aux outils contemporains tout en conservant certaines pratiques violentes et coercitives héritées du monde physique.

Discussion

Contrairement à l'idée largement partagée selon laquelle la déterritorialisation du crime conduit à un affaiblissement des structures criminelles traditionnelles, il apparaît que ce phénomène témoigne plutôt d'une recomposition de ces structures. Cette recomposition repose sur l'émergence de nouvelles compétences techniques et une fluidité organisationnelle accrue, permettant aux groupes criminels de maintenir, voire d'augmenter leur efficacité. Dans ce contexte, la question de la localisation du pouvoir criminel devient complexe : bien qu'il soit moins visible et plus difficile à localiser, il demeure tout aussi opérationnel.

L'autorité criminelle se transforme dans ses fondements mêmes. Elle ne repose plus uniquement sur des facteurs physiques ou territoriaux, mais sur un contrôle plus subtil des flux d'information, des identifiants numériques et des interfaces transactionnelles. Cette évolution radicale des modes de pouvoir dans le domaine criminel interroge les paradigmes classiques d'analyse du crime organisé, nécessitant l'intégration des dimensions techniques, culturelles et économiques dans l'étude de la cybercriminalité.

Cependant, cette transformation ne marque pas la fin des structures de domination. Les marchés numériques conservent des mécanismes hiérarchiques, fondés sur des logiques de réputation et d'exclusion. De surcroît, les groupes criminels traditionnels n'ont pas disparu ; au contraire, ils restent fortement impliqués dans ces dispositifs numériques, soit en prenant part directement à leur gestion, soit en y délégant certaines de leurs activités. En ce sens, le darknet n'émerge pas comme un espace anarchique dépourvu d'autorité, mais comme un espace structuré par de nouvelles formes de régulation criminelle.

Historiquement, le pouvoir criminel était ancré dans des territoires physiques, mais il semble désormais se reconfigurer dans l'espace numérique. L'absence d'ancrage géographique direct ne signifie pas pour autant l'absence de contrôle. Le développement du darknet, cet espace obscur et chiffré non indexé par les moteurs de recherche traditionnels, a offert de nouvelles possibilités d'action aux groupes criminels. En brouillant les frontières entre l'espace physique, la visibilité et l'autorité, ce territoire virtuel redéfinit les enjeux du pouvoir criminel à l'échelle transnationale (Décary-Hétu & Giommoni, 2017).

Contrairement à une conception erronée du cyberespace comme un espace dépourvu de règles, il existe en réalité des logiques strictes de hiérarchisation, de réputation et de violence symbolique qui régissent ce domaine. Sur les marchés illicites en ligne, la confiance devient un bien précieux, construit par des mécanismes de notation, un pseudonymat stable, des échanges de preuves et parfois des démonstrations publiques de pouvoir ou de menace (Aldridge & Décary-Hétu, 2014). Ce phénomène marque une continuité de la logique de la réputation, autrefois ancrée dans des contextes physiques tels que les rues ou les prisons, et désormais transférée aux interfaces cryptées des places de marché numériques.

La violence physique, bien que moins manifeste, est remplacée par des formes de violence symbolique et technique, telles que le chantage, le doxxing, les attaques par déni de service distribué (DDoS) ou l'escroquerie de masse. Ces formes de violence numérique signalent une recomposition de l'autorité criminelle, qui repose désormais sur la maîtrise des outils numériques autant que sur des pratiques d'intimidation symbolique. Le hacker ou l'administrateur de forums devient ainsi un acteur qui exerce un pouvoir sans contact direct, mais dont les effets sont tout aussi réels sur les individus ou les groupes ciblés.

Le contrôle de l'espace dans le cyberspace dépend de compétences techniques complexes : coder, masquer son identité, crypter les transactions et contourner les surveillances policières. Ce nouvel espace, fluide et décentralisé, reste néanmoins structuré, avec des lieux de pouvoir définis, tels que des forums dominants, des marchés réputés ou des communautés d'experts. Ces éléments contribuent à l'émergence de formes de gouvernance criminelle décentralisée, fondées sur des réseaux techniques et sociaux (Martin, 2014).

Cette reconfiguration numérique ne marque pas une rupture radicale avec les formes traditionnelles de pouvoir criminel. Elle les prolonge et les étend tout en introduisant de nouvelles vulnérabilités. Le pseudonymat, s'il protège les acteurs criminels, les expose également à des risques accrus : un bug, une erreur technique ou une infiltration policière peuvent rapidement fragiliser une réputation bâtie sur des années. La stabilité du pouvoir criminel devient ainsi plus volatile, tout en restant d'une efficacité indiscutable.

En définitive, la mutation du pouvoir criminel vers le darknet ne se fait pas par simple substitution, mais par une hybridation des anciennes et des nouvelles formes de criminalité. Les pratiques enracinées dans des territoires physiques, des corps et des signes visibles se superposent désormais à des modalités dématérialisées, anonymes et techniques. Cette coexistence dessine une géographie criminelle nouvelle, marquée par la superposition des espaces physiques et numériques, par la fluidité des frontières et par le brouillage des repères spatiaux.

L'hybridation et la numérisation du crime organisé

L'une des principales transformations du crime organisé contemporain réside dans l'hybridation des acteurs criminels. D'une part, les groupes criminels traditionnels investissent les espaces numériques pour des activités telles que le blanchiment de cryptomonnaies, la coordination par messagerie chiffrée ou l'extorsion en ligne. D'autre part, de nouveaux acteurs, souvent natifs du numérique, développent des compétences techniques spécifiques qui leur permettent d'exercer un pouvoir sans territoire physique ni enracinement social.

Ce double mouvement de convergence des mondes physique et numérique redéfinit les frontières entre les formes anciennes et nouvelles du crime organisé. L'autorité criminelle s'appuie désormais sur une combinaison de ressources multiples : techniques (maîtrise du chiffrement, des scripts et de l'infrastructure réseau), relationnelles (réputation numérique et pseudonymat), symboliques (discours anti-État, "underground") et économiques (flux de cryptomonnaies, services illicites).

Les dynamiques de pouvoir s'élargissent au-delà de la capacité de domination par la force, pour inclure la capacité à organiser, persuader et rendre invisible. Dans cet espace fluide et instable, les pratiques criminelles peuvent se déplacer et s'adapter rapidement aux nouvelles réalités du numérique.

L'impact des évolutions contemporaines du crime organisé sur la sécurité publique

La transformation du crime organisé soulève des défis considérables pour les institutions chargées de la sécurité. Le modèle traditionnel de lutte contre la criminalité, fondé sur des logiques territoriales, est désormais obsolète face à l'hybridation des formes criminelles et à leur déterritorialisation numérique. Les institutions de sécurité publique, telles qu'Europol et Interpol, doivent adopter des stratégies transnationales adaptées à ces nouvelles menaces.

Le rapport EU SOCTA 2025, par exemple, présente une analyse stratégique des menaces criminelles contemporaines et confirme l'extension de l'activité criminelle vers le cyberspace, avec l'utilisation systématique du dark web, des cryptomonnaies et du chiffrement. Les groupes criminels structurés s'adaptent à ces évolutions en consolidant leur pouvoir grâce à des modèles hybrides, intégrant des technologies avancées et des pratiques de gouvernance décentralisée.

Les défis juridiques posés par la cybercriminalité sont également considérables. Les cadres législatifs existants sont souvent inadaptés pour appréhender la déterritorialisation et la fluidité des nouvelles formes de criminalité. Les questions de compétence territoriale, d'identification des auteurs et de preuve numérique constituent des obstacles majeurs pour l'application du droit.

Vers une gouvernance globale du cyberespace criminel

À mesure que le cyberespace devient un terrain stratégique pour le crime organisé, les réponses institutionnelles doivent évoluer. Une gouvernance globale du cyberespace criminel, intégrant régulation technique, coopération internationale et action préventive, s'impose comme une réponse viable aux mutations du crime organisé. Toutefois, cette gouvernance se heurte à plusieurs défis, notamment la fragmentation normative, les asymétries des capacités nationales et les ambiguïtés des intérêts publics et privés.

Dans cette dynamique de gouvernance complexe, la lutte contre le crime organisé à l'ère numérique exige une approche systémique, qui inclut l'éducation numérique, la résilience des infrastructures, et une coopération multi-acteurs renforcée. Les mutations actuelles du crime organisé redéfinissent ainsi non seulement la nature du pouvoir criminel, mais aussi les modalités d'intervention des institutions de sécurité publique face à ces nouvelles formes de délinquance numérique

Conclusion

L'essor du cyberespace, loin de marginaliser les structures criminelles traditionnelles, a agi comme un catalyseur de transformation profonde de leurs logiques d'action, de leur organisation, et de leur ancrage territorial. En réinventant ses modes de fonctionnement, le crime organisé se libère des contraintes géographiques tout en intégrant des outils numériques complexes. Ce phénomène témoigne d'une hybridation continue entre criminalité physique et cybercriminalité, qui transforme la nature même du pouvoir criminel.

L'analyse a montré que les organisations criminelles traditionnelles ne se contentent pas d'une simple mutation technologique. Elles connaissent une reconfiguration de leur pouvoir : leurs leviers d'influence s'étendent désormais à des environnements numériques décentralisés et transnationaux. Le darknet, les cryptomonnaies et les plateformes chiffrées ne sont pas seulement des outils de dissimulation, mais aussi des terrains d'affrontement et de régulation, qui redéfinissent les rapports de force. Ainsi, les logiques de loyauté, de réputation et de contrôle, traditionnellement ancrées dans le monde physique, doivent être réinventées pour s'adapter à ce nouveau paradigme numérique.

En parallèle, les réponses institutionnelles, bien que nombreuses, peinent à répondre efficacement à la rapidité d'adaptation et à l'agilité des structures criminelles cyber-compatibles. Les initiatives techniques et juridiques, souvent axées sur la répression, doivent être complétées par des stratégies de prévention et des régulations plus flexibles. Face à cette évolution, il devient crucial de mettre en place une gouvernance polycentrique qui combine coopération transnationale, régulation privée, innovation juridique et renforcement de la résilience sociale. La lutte contre ces nouvelles formes de pouvoir criminel nécessite également un cadre juridique international harmonisé, pour pallier la déterritorialisation du crime.

En outre, au-delà de la répression des actes criminels, il est essentiel d'examiner les conditions sociales, économiques et politiques qui rendent cette criminalité particulièrement attractive. La précarisation des jeunes générations, la mondialisation des échanges, et la connectivité croissante ouvrent la voie à des formes de criminalité qui trouvent un terreau fertile dans des environnements sociaux fragilisés. Ce phénomène interroge les causes profondes de l'attrait pour ces nouvelles formes de déviance, et met en lumière les tensions sociales et géopolitiques qui sous-tendent ces dynamiques criminelles.

Ainsi, l'avenir du pouvoir criminel ne réside pas seulement dans la capacité à manipuler des lignes de code ou à maîtriser des technologies avancées, mais également dans la manière dont ces acteurs exploitent les fractures sociales et géopolitiques mondiales. Le pouvoir criminel ne s'est pas éteint ; il s'est déplacé, s'est complexifié et s'est renforcé grâce à l'adaptation aux technologies numériques, tout en jouant sur des failles sociales et économiques existantes.

Cette plasticité, la capacité des structures criminelles à évoluer et à se réinventer en permanence, soulève des questions fondamentales pour les États et les institutions internationales. Les outils conceptuels des sciences sociales doivent être révisés pour appréhender des formes de pouvoir invisibles, hybrides et transitoires, qui échappent aux analyses traditionnelles du crime organisé. Comprendre cette reconfiguration est non seulement essentiel pour penser la criminalité contemporaine, mais aussi pour interroger nos propres catégories, territoire, autorité, visibilité, légitimité, dans un monde où les logiques numériques redéfinissent la scène sociale tout entière.

Les références bibliographiques

Aldridge, J., & Décary-Hétu, D. (2014). *Not an "Ebay for Drugs": The Cryptomarket "Silk Road" as a paradigm shifting criminal innovation*. Social Science Research Network. https://doi.org/10.2139/ssrn.2436643

Assas Legal Innovation. (2022). *Cybercriminalité et crypto-actifs*. https://assas-legal-innovation.fr/

Broadhurst, R., Deane, F. P., & Dixon, T. (2014). *Cybercrime risks and responses: Eastern and Western perspectives*. Palgrave Macmillan.

Broadhurst, R., Deane, F. P., & Dixon, T. (2017). Online fraud and the transition of traditional crimes to cyberspace. *International Journal of Cyber Criminology, 11*(1), 27–45.

Cohen, J. (2016). The emerging structure of criminal governance on the darknet. *Journal of Cybersecurity, 2*(3), 120–132. https://doi.org/10.1093/cybsec/tyw009

Continuum Lab. (2021). *Blockchain et criminalité*. https://continuumlab.org/publication/blockchain-et-criminalite/

Décary-Hétu, D., & Aldridge, J. (2015). Sifting through the net: Monitoring of online offenders by researchers. *European Review of Organised Crime, 2*(2), 122–141.

Décary-Hétu, D., & Giommoni, L. (2017). Exploring the criminal landscape of the darknet. *Crime Science, 6*(1), 1–13. https://doi.org/10.1186/s40163-017-0074-0

Décary-Hétu, D., & Leclerc, B. (2019). A criminology of the darknet: Digital crime and hybrid networks. *Journal of Criminology, 22*(3), 45–67.

Europol. (2021). *Internet organised crime threat assessment (IOCTA)*. Europol. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2021

Europol. (2025). *EU SOCTA 2025: EU serious and organised crime threat assessment*. https://www.europol.europa.eu/activities-services/main-reports

Fortin, F. (2013). *Cybercriminalité : Entre inconduite et crime organisé*. Presses internationales Polytechnique.

Gambetta, D. (1993). *The Sicilian mafia: The business of private protection*. Harvard University Press.

Gayraud, J.-F. (2005). *La nouvelle criminalité*. Odile Jacob.

Gayraud, J.-F. (2016). L'hybridation criminelle et la recomposition des groupes mafieux. *Criminologie, 49*(2), 231–247.

Gendarmerie Nationale. (2021). *Lutte contre la cybercriminalité et usage de la blockchain intelligence*. https://www.gendarmerie.interieur.gouv.fr

IRIS – Institut de Relations Internationales et Stratégiques. (2021). *Les grandes criminalités : Entre réalité géopolitique et menace stratégique*. https://www.iris-france.org

Lavorgna, A. (2015). Organized crime goes online: Realities and challenges. *Journal of Global Crime, 16*(2), 123–138. https://doi.org/10.1080/17440572.2015.1034171

Morselli, C. (2009). *Inside criminal networks*. Springer.

Paoli, L. (2003). *Mafia brotherhoods: Organized crime, Italian style*. Oxford University Press.

Projet TITANIUM. (2019). *Tools for the investigation of transactions in underground markets*. https://www.titanium-project.eu

Revue Pouvoirs. (2020). *Globalisation du crime et recomposition du pouvoir* (No. 175). https://www.revue-pouvoirs.fr

Saviano, R. (2006). *Gomorrah: Italy's other mafia*. Farrar, Straus and Giroux.

TRM Labs. (2023). *Darknet markets explained*. https://www.trmlabs.com

Varese, F. (2010). *Mafia movements: How organized crime conquers new territories*. Princeton University Press.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Yar, M. (2013). *Cybercrime and society* (2nd ed.). Sage Publications.