doi: 10.14664/rcvs/244

L'intelligence criminale nel contrasto alla cybercriminalità: l'esempio francese della gendarmeria nazionale

Le renseignement criminel au service de la lutte contre la cybercriminalité : l'exemple français de la gendarmerie nationale

Criminal intelligence in the fight against cybercrime: the French example of the national gendarmerie

*Jérôme Barlatier**

Riassunto
Questo articolo propone un'analisi sintetica della cybercriminalità a partire dallo stato della minaccia cibernetica realizzato dalla gendarmeria nazionale. La portata di questa forma di delinquenza è oggi tale che l'azione degli investigatori e dei magistrati, caso per caso, in una logica procedurale di individualizzazione, non può, da sola, avere ragione di un fenomeno così esteso. Recentemente riformulata secondo la prospettiva dell'*intelligence-led policing* (ILP), l'*intelligence* criminale propone un nuovo approccio alla delinquenza, proattivo, orientato a una comprensione preliminare delle situazioni al fine di proporre soluzioni adeguate, diversificate e innovative. L'ecosistema digitale si presta particolarmente ai metodi di analisi e alle strategie proposte da tale approccio. L'individuazione e la comprensione delle minacce sono facilitate dalla cyber *threat intelligence* (CTI) e le soluzioni adottate dalle forze di sicurezza interna non si limitano più alla sola repressione penale, ma si avvalgono di dispositivi sempre più sofisticati.

Résumé
Cet article propose une analyse synthétique de la cybercriminalité au travers de l'état de la menace cyber réalisé par la gendarmerie nationale. L'ampleur de cette forme de délinquance est aujourd'hui telle que l'action des enquêteurs et des magistrats, au cas-par-cas, dans une logique procédurale d'individualisation, ne saurait, à elle seule, avoir raison d'un phénomène aussi massif. Récemment reformulé sous l'angle de l'*intelligence-led policing* (ILP), le renseignement criminel propose une nouvelle approche de la délinquance, proactive, orientée sur une compréhension préalable des situations afin de proposer des solutions adaptées, diversifiées et innovantes. L'écosystème cyber se prête particulièrement aux méthodes d'analyse et aux stratégies proposées par le renseignement criminel. La détection et la compréhension des menaces y sont autorisées par *la cyber threat intelligence* (CTI) et les solutions d'entrave pour les forces de sécurité intérieures ne se limitent plus à la répression pénale, mais font appel à des dispositifs toujours plus sophistiqués.

Abstract
This article carries out a synthetic analysis of cybercrime perceived in France through the state of the cyber threat carried out by the gendarmerie nationale. This form of criminality has today such a magnitude that the action of investigators and magistrates, on a case-by-case basis, in a procedural logic of individualization, cannot, on its own, overcome such a massive phenomenon. Recently reformulated from the perspective of intelligence-led policing (ILP), criminal intelligence offers a new approach to delinquency which is proactive and oriented on a prior understanding of the situations in order to propose some adapted, diversified and innovative solutions. The cyber ecosystem lends itself particularly well to the analytical methods and strategies proposed by criminal intelligence. The detection and understanding of threats are authorized by cyber threat intelligence (CTI) and the solutions for the law enforcement forces are no longer limited to criminal repression, but call on elaborate devices with increasing sophistication.

Key words: Internet, cybercriminalité, investigation, *intelligence*, gendarmerie

* Docteur en Criminologie. Chef de la division du renseignement, Service central de renseignement criminel de la Gendarmerie nationale.

1. Introduction

« La révolution de l'An 2000 sera celle de l'information pour tous ». C'est ainsi que débutait le peu clairvoyant rapport de Gérard Théry en 1994 au sujet de ce l'on nommait encore les « autoroutes de l'information » (Théry, 1994).

L'évolution et l'accélération des technologies est telle qu'il est difficile d'imaginer qu'il y a vingt ans à peine l'informatique en réseau et la téléphonie mobile n'en étaient qu'aux balbutiements. Les atteintes aux systèmes de traitement automatisés de données représentaient alors des actes isolés et à portée limitée, réprimés en vertu de la loi Godfrain n° 88-19 du 5 janvier 1988 relative à la fraude informatique.

La prise de conscience des bouleversements induits par la création de l'internet (Wall, 2007) a pour autant été très tôt anticipé par les États Occidentaux. Dans l'enceinte du Conseil de l'Europe, la convention de Budapest sur la cybercriminalité du 23 novembre 2001[1] envisageait une adaptation du droit pénal de fond et de la procédure. Ce texte témoignait d'une conscience et d'une prise en compte rapide des enjeux de délinquance liés à ce nouvel espace. La nécessité de maîtriser la vélocité de l'information et de pouvoir accéder aux traces numériques quels que soient leur lieu de stockage était bien perçue. Certains mésusages de l'internet comme support ou comme vecteur de délinquance étaient déjà identifiés.

Le scénario était écrit, le décor était planté, il ne restait plus qu'aux acteurs de jouer. Moins de deux décennies ont été suffisantes pour ériger la cybercriminalité en la menace criminelle majeure, alors que quarante ans ont été nécessaires au trafic de stupéfiants pour arriver à maturité[2].

Illustrant le lien étroit existant entre la criminalité et les activités humaines, l'essor sans précédent des technologies de communication a corrélé l'évolution des phénomènes cyberdélinquants avec notre addiction aux échanges virtuels. Le netaholisme de nos sociétés et de nos économies rend bien plus difficile la régulation des activités délinquantes, car elles ne se juxtaposent plus seulement aux activités légales. Elles les débordent et s'hybrident, leur volume et leur nature les rendant plus difficiles à identifier, à caractériser et à éradiquer. Elles nécessitent d'envisager des changement de paradigme pour appréhender les évolutions de cette délinquance (Linde, Aebi, 2020).

L'évolution radicale de ce contexte criminologique implique de repenser les modes de régulation qui s'y appliquent. La cybercriminalité est nouvelle et complexe. Elle invite à une démarche où la compréhension précède l'action, remettant en cause le caractère traditionnellement réactif de la répression de la délinquances. Il convient ainsi de s'interroger sur les apports du renseignement criminel, dans une approche issue des théorie de l'*intelligence-led policing* (ILP).

Issu d'une préoccupation ancienne, mais fruit d'une méthodologie nouvelle, le projet d'une police guidée par le renseignement peut être le support d'une réponse composite à la cybercriminalité dans une approche à la fois holistique et casuistique, préventive et répressive, publique et privée. L'ILP ambitionne une compréhension des phénomènes criminels recourant à Internet comme objet ou comme vecteur de délinquance. Elle est parallèlement animée par le souci de trouver des solutions concrètes et actionnables. Par la mise en

[1] Convention on Cybercrime (ETS No. 185), disponible en ligne (consultation le 10 novembre 2022) : https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[2] De la *french connection* au néo-banditisme ; voir, par exemple, l'évolution chez le même auteur : Lalam 2002 et 2017).

cohérence de l'intervention des acteurs publics et privés, une coordination est possible pour mettre en œuvre des techniques d'entrave diversifiées, destinées à apporter une solution stratégique ou opérationnelle à la cybercriminalité.

Au niveau stratégique, le renseignement criminel permet de disposer des éléments d'évaluation et de modélisation des phénomènes, des espaces et des groupes cybercriminels. Cette approche est indispensable pour envisager des moyens de remédiation déjà existants ou susceptibles d'être expérimentés dans une logique *What works ? What doesn't ? What's promising ?*

Au niveau opérationnel, il permet d'envisager des entraves préventives et répressives adaptées à chaque phénomène. Il cherche à cibler les cyber-groupes criminels, tels que les groupes APT, et conçoit des modalités de neutralisation spécifiques à chacun d'entre-eux.

Cette approche proactive constitue, à maints égards, un changement de paradigme en matière de lutte contre la délinquance. Il ne s'agit plus de penser en termes de répression et d'interdit pénal, mais en termes de gestion du risque et de menace. L'enquête n'est plus seulement une source de vérité judiciaire, mais un capteur de savoir au service du renseignement. La plainte formelle de la victime n'est plus le moteur de l'action publique : enrichit, synthétisé et analysé, un simple signalement permet de contribuer à la détection et à la caractérisation des phénomènes, préalables à la définition d'actions de remédiations pertinentes.

Coordonnant les administrations avec le secteur privé et le monde académique, cette approche par le renseignement est susceptible de permettre la compréhension d'un environnement complexe, d'anticiper l'évolution rapide des technologies et de proposer des solutions aussi diversifiées qu'adaptées. En ce sens, les forces de l'ordre se rappellent qu'il est nécessaire de savoir avant d'agir.

Le présent article est nourri par la double expérience de son auteur, praticien au sein des forces de l'ordre spécialisé dans l'exercice de la mission de police judiciaire, et chercheur, auteurs d'une thèse de doctorat interrogeant la performance des processus d'enquête (Barlatier, 2017). Ses constats sont ainsi autant d'ordre académiques qu'opérationnels. Réalisant dans un premier temps un état de la menace de la cybercriminalité (2), il envisage ensuite les conditions de sa régulation et les potentialités offertes par le renseignement criminel (3).

2. État de la menace

La cybercriminalité est souvent abordée de façon autonome par les spécialistes du numérique dans une approche technique et autocentrée qui ne permet pas de rendre compte fidèlement de sa nature. Afin de l'aborder dans ses réalités, il convient de la situer dans l'écosystème plus général de la délinquance.

La question des escroqueries dites « en ligne », par exemple, est souvent envisagée comme une catégorie à part-entière. L'analyse de ce phénomène démontre pourtant une réalité bien plus complexe que ce libellé ne le laisserait présumer : les trois quart des escroqueries intègrent aujourd'hui une composante numérique au sein de leur mode opératoire, que ce soit au niveau de la phase de contact de la victime, de celle de sa manipulation, ou de celle de son paiement[3]. Désormais, distinguer les infractions de l'univers physique et du monde

[3] D'après les analyse du service central de renseignement criminel de la gendarmerie nationale (SCRCGN), à partir d'un suivi permanent de la donnée sur l'ensemble des agrégats de la délinquance en zone de compétence gendarmerie (représentant 95% du territoire national et 52% de la population française).

virtuel constitue une opposition trompeuse. Le numérique se mêle à la vie de chaque citoyen. Il s'intègre à tous les degrés des activités humaines. La délinquance n'y fait pas exception. Son impact en est d'autant plus important.

Augmentant, depuis plus d'une décennie, de 20 points par an[4], la croissance exponentielle de la cybercriminalité est corrélative au développement des accès à l'internet et de l'économie numérique. Plusieurs études considèrent que les atteintes par le vecteur numérique dépassent désormais le volume des infractions constatées dans le monde physique (Europol, 2015 ; Loveday, 2018). Cette estimation est d'autant plus significative que la délinquance recourant au vecteur numérique s'est faite plus discrète pour les systèmes judiciaires. La propension des victimes à rapporter les infractions et celle des institutions à les révéler semble s'être émoussée au regard de la part importante des infractions à faible préjudice, de la technicité de ce contentieux, du faible espoir en termes d'élucidation et de répression, et de l'existence d'autres formes de compensation du préjudice (e.g., indemnisation) (Ghernaouti-Hélie, 2009, p. 59-62). Ainsi, en 2016 la gendarmerie et la police nationales françaises recensaient-elles moins de 10.000 plaintes de fraudes à la cartes bancaires pour plus de 1,9 millions de faits identifiés par les banques et le e-commerçants[5]. S'il mérite d'être adapté à la réalité de chaque phénomène, ce rapport d'une plainte pour 200 faits réellement commis est confirmé par une étude de la gendarmerie nationale évaluant le taux de plainte en matière de rançongiciels à un pour 257 faits commis (Dregoir, Klein, 2017). D'autres études affirment, en revanche, que le taux de reportabilité des infractions numériques serait de 20% environ (Margagliotti *et al.*, 2019 ; Kemp, 2020).

Le vecteur numérique semble ainsi avoir déplacé les opportunités criminelles (Koops, 2011). Il permet, en effet, d'accéder de façon massive à l'intimité des victimes, tout en restant à bonne distance au moyen de garanties d'anonymat, et donc d'impunité. La transmission des modes opératoires est facilitée par la logique de réseaux autorisant la création d'équipes animées par une communauté d'intérêt mais composées de membres se connaissant rarement (Leukfeldt, 2015). Souvent fondés sur la démultiplication de petits préjudices, les bénéfices criminels sont considérables et peu traçables.

Les rapports d'analyse de la gendarmerie nationale identifient le vecteur numérique comme la menace criminelle la plus importante sur les trois axes d'évaluation que sont les phénomènes (2.1), les groupes (2.2) et la géographie (2.3) criminels.

2.1. Les phénomènes cybercriminels

Internet a bouleversé la vie des populations et le fonctionnement de l'économie. Il constitue une rupture technologique décisive plaçant l'information au centre des valeurs. Au terme de vingt ans d'observation, il est possible d'affirmer que ces changements radicaux ont eu un effet considérable sur la délinquance.

Le Web est à la fois le vecteur et l'objet de la délinquance (Wall, 2007, p. 44 et s.) :

- le vecteur car, comme l'apparition de l'automobile en son temps a permis d'agir plus vite et plus loin, internet procure une surface d'attaque plus importante pour la commission d'infraction traditionnelles ;
- l'objet, car internet est composé d'acteurs et

[4] Source : SCRCGN.

[5] Analyse réalisée en 2016 par la SCRCGN lors de la mise en place de la plate-forme PERCEVAL de signalement des escroqueries en ligne à la carte bancaire. Source issues des données opérationnelles de la gendarmerie nationale et de ses partenaires dans le secteur bancaire et du e-commerce.

d'infrastructures eux-mêmes touchés par des infractions de nouvelle nature propres à cet écosystème si particulier.

Les nouvelles technologies de l'information et de la communication représentent donc tout à la fois la transposition d'une délinquance préexistante, l'amplification de celle-ci, et la création de nouvelles formes de criminalité qui n'existaient pas auparavant.

En France, la gendarmerie nationale positionne la cybercriminalité en tête de ses priorités opérationnelles. Son état de la menace cherche à comprendre son organisation, ses modes opératoires, ses dynamiques, ses motivations et son modèle économique. Un bref aperçu des principaux phénomènes peut être réalisé[6].

Intrusions dans un système informatique dans le but de vol, d'altération ou de piratage d'informations, les atteintes au système de traitement automatisé de données (ASTAD)[7] représentent un dixième des infractions constatées par les unités de la gendarmerie dans le cyberespace. Ce chiffre est cependant largement sous-estimé au regard de la faible reportabilité de ces délits auprès des forces de l'ordre, les volumes constatés par d'autres sources (observateurs privés ou publics, tels que le GIP ACYMA) étant bien plus importants[8].

Les rançongiciels (*ransomware*) sont la transposition de l'extorsion de fond traditionnelle par la prise en otage des données informatiques au préjudice des entreprises, mais aussi des personnes publiques et, désormais, des particuliers. Ne se limitant pas à bloquer le système informatique par le chiffrement des données, ce mode opératoire s'accompagne généralement du vol et du remploi des données de la victime, le *business plan* des malfaiteurs cherchant à rentabiliser l'acte par diverses sources de profit. Les procédés d'incitation au paiement sont radicaux et perfectionnés. Cumulant les frais de la rançon, les coûts d'exploitation et l'atteinte à la réputation, le préjudice est considérable et représente souvent un enjeu de survie pour une entreprise, voire une filière économique.

Destinées à neutraliser la disponibilité d'un système informatique, des communications ou d'un site internet par la saturation de ses capacités techniques, les attaques par déni de service (*Denial of Service Attack* - DOS) sont également très couteuses et reposent sur des infrastructures de délinquance évoluées.

D'autres manières d'opérer consistent à mettre à profit les failles informatiques, tel que le *swatting* (fausses alertes aux forces de l'ordre), le *jackpotting* (attaque informatique sur un distributeur automatisé de billet afin d'en retirer l'argent), le *mouse-jacking* (vol électronique de véhicules) ou les actions

[6] Tous les deux ans, la gendarmerie nationale française publie un rapport d'analyse relatif à la criminalité organisée (RACO) procédant à un état de la menace des tendances de la délinquance. Cette analyse constitue une aide à la décision au profit de son commandement et de ses partenaires.
Par ailleurs, un rapport d'analyse des cybermenaces a été publié cette année afin d'approfondir les constats du RACO dans le domaine plus spécifique des atteintes aux systèmes automatisés de données (ASTAD).
Ces rapports sont classifiés et accessibles qu'au regard du droit et du besoin d'en connaître. Toutefois, les éléments pouvant être communiqués au public sont évoqués dans cet article.

[7] Ces infractions sont prévues aux articles 321-1 à 321-8 du code pénal :
- accès, maintient frauduleux ayant, le cas échéant, entrainé la suppression ou la modification des données d'un STAD (art. 321-1 CP) ;
- entrave ou altération du fonctionnement d'un STAD (art. 321-2 CP) ;
- introduction frauduleuse de données dans un STAD, ou extraction, détention, reproduction, transmission, suppression, modification frauduleuse de données (art. 321-3 CP) ;
- détention, offre ou cession d'équipements, instrument, ou programme informatique destiné à commettre les infractions précitées (art. 323-3-1 CP) ;
- participation à un groupement en vue de la commission des infractions précitées (art. 323-4 CP).

[8] Pour le dernier rapport du GIP ACYMA : https://www.cybermalveillance.gouv.fr/medias/2022/03/cybermalveillance-rapport-activite-2021.pdf (consulté le 4 décembre 2022).

malveillantes sur la domotique (serrures électroniques, brouilleurs d'alarmes, *etc.*).

Si ces attaques techniques représentent des préjudices considérables, les trois quarts de la cybercriminalité constatée par les plaintes déposées auprès des unités de la gendarmerie nationale concernent néanmoins les escroqueries[9]. Celles-ci sont particulièrement hétérogènes au niveau de leur modes opératoires, de leur victimologie et de leur préjudice.

Une part importante d'entre-elles concernent les fraudes à la vente et à la livraison d'objets en ligne par des individus à faible capacité criminelle[10] profitant de l'anonymat et des opportunités offertes par la toile.

Les escroqueries dites « à la nigériane » commises par des populations situées en Afrique de l'Ouest représentent une forme plus structurée de délinquance. Commises depuis l'étranger, elles constituent un phénomène socio-économique où des populations pauvres ont une opportunité de gagner facilement de l'argent et contactant *via* internet des populations de pays plus riches. La communauté linguistique avec leur victime et la maîtrise d'un mode opératoire appris et perfectionné sur le tas sont les conditionnants de la réussite des escrocs. La typologie de modes d'action est particulièrement diversifiée, souvent standardisée, parfois innovante : lettre de Jérusalem (dites « *scam* 419 » consistant à solliciter de l'aide par message), fraudes aux sentiments, sextorsions, *pornscam*, fausses locations, fausses annonces, fausses offres d'emploi en ligne, *et cetera*. Ces escroqueries sont d'un faible préjudice économique, mais représentent un bénéfice cumulé important. Elles créent un sentiment d'insécurité chez des internautes vis-à-vis des services proposés sur la toile.

D'autres escroqueries à fort préjudice économique sont commises depuis la France et l'étranger selon des modes d'action bien plus perfectionnés. Qu'il s'agisse de faux ordre de virements internationaux (FOVI), de fausses commandes, de faux investissements, cette criminalité entrepreneuriale repose sur des processus et des modèles économiques planifiés et perfectionnés où le ciblage se fonde sur une collecte préalable des données (*leads*) et un démarchage actif (*via* des *call centers*), prolongé par une phase de manipulation (*social engineering*) et des opérations financières élaborées visant à brouiller les pistes et à blanchir les fonds indûment versés. Commises au préjudice des entreprises ou des particuliers, ces fraudes trouvent également des débouchés en matière de détournement des fonds publics comme cela a pu être observé lors de la captation frauduleuse des aides d'État durant la crise sanitaire (*i.e.*, chômage partiel, prêts garantis par l'État)[11], le détournement

[9] Sont considérées comme des escroqueries numériques l'ensemble des infractions dont au moins un des éléments du mode opératoire est perpétré dans le cyber-espace : identification de la victime (*via* les fuites de données, par exemple), prise de contact (*mail* frauduleux, *spam*, *etc.*), manipulations frauduleuses (procédés de tromperie, recours à des moyens d'anonymisation autorisés par le Web, par exemple) ou versement des sommes indues (virement en ligne ou utilisation de crypto-actifs, par exemple).

[10] La capacité criminelle s'entend du potentiel d'un individu à commettre des infractions d'une certaine gravité, au regard des prédispositions matérielles et psychologiques que celle-ci nécessitent de surmonter. Réaliser des détournements d'argent par ruse en l'absence d'une victime anonyme, par exemple, demande une moindre capacité criminelle que le vol avec violences physiques sur une personne vulnérable.

[11] Cette question a fait l'objet de nombreux écrits de la part des institutions internationales et nationales :

- Interpol : https://www.interpol.int/fr/Infractions/Cybercriminalite/Cybermenaces-liees-au-COVID-19 (consulté le 4 décembre 2022) ;
- Europol : https://www.europol.europa.eu/operations-services-and-innovation/staying-safe-during-covid-19-what-you-need-to-know (consulté le 4 décembre 2022) ;
- Institut des hautes études du ministère de l'intérieur (IHEMI) : https://www.ihemi.fr/articles/evolution-du-crime-et-du-cybercrime-durant-la-pandemie-de-coronavirus (consulté le 4 décembre 2022) ;
- Agence nationale de sécurité des systèmes d'information (ANSSI) : https://www.ssi.gouv.fr/actualite/lanssi-et-le-

du dispositif d'aide à la rénovation énergétique ou de comptes personnels de formation. Cette délinquance témoigne de l'articulation subtile d'actions dans le monde physique et numérique jouant sur l'ignorance ou la crédulités de certains acteurs combinée avec les vulnérabilités et les faiblesse juridiques ou économiques des entreprises et des administrations.

Cette hybridation du physique et du numérique est également bien présente dans les opportunités de trafics offertes à une vaste communauté d'internautes (Ablon *et al.*, 2014) : drogues, médicaments, tabac, armes, documents, données à caractère personnel, moyens de paiement, pièces détachées de véhicules, produits de contrefaçons ou de contrebande, *et cetera*. Ces denrées illicites sont déployées sur un marché libéralisé et anonyme, où l'offre est mise en lien avec la demande sans qu'une régulation spécifique ne soit opérée. Au-delà des échanges de biens illicites, internet facilite également les mouvements de capitaux, chacun se trouvant à un clic de sa banque ou d'un intermédiaire de transfert de fond. L'escroc n'a plus à recevoir le paiement des mains de la victime, les opérations de blanchiment n'emportent plus nécessairement le transport de valises de billets, les mouvements d'argent pouvant se réaliser de façon dispersés par des intermédiaires humains (*money mules*) ou techniques (crypto-actifs, *Non Fungible Token* - NFT) destinés à brouiller les pistes.

Internet crée donc un contexte favorable aux atteintes aux biens. Elle n'empêche pas davantage les atteintes aux personnes, en fournissant un cadre permettant de générer des contenus qui répondent à la curiosité, à la malveillance ou aux pulsions d'un large public d'anonymes (violences, exploitation et contrainte dans la production de contenus pornographiques, *etc.*) (pour une approche de l'influence des facteurs humains, auteur et victime, en termes de cybercriminalité : Leukfeldt, Holt, 2021). Parfois, l'être humain est considéré comme une marchandise dont la commercialisation est amplifiée par les réseaux en contrepartie d'importants profits (proxénétisme, trafic de migrants, atteintes sexuelles sur mineurs en ligne) (Yu, 2014). Brisant les barrières entre la proximité physique et la distance numérique, les réseaux sociaux se sont montrés propices aux violences morales (insultes, menaces, harcèlement), à la désinformation (délits de presse, *fake news*), aux atteintes à la réputation et à la vie privée (diffamation, atteinte au secret des correspondances, *sexting*, *revenge porn*)[12]. Si internet efface les distances, il restaure aussi parfois la proximité. Il existe, à ce titre, une « cyberdélinquance de proximité », où l'auteur agresse anonymement sa victime sur Internet alors même qu'il se situe dans son entourage proche (cyberharcèlement, pédopornographie).

Ces phénomènes accompagnent l'accroissement exponentiel des activités humaines et des enjeux économiques, politiques et sociaux de l'internet. Si la technicité de cet écosystème a impliqué une spécialisation de certains acteurs, la plupart de ces modes opératoires est réalisée par le report de la délinquance traditionnelle vers le *Web*.

2.2 Les acteurs de la cybercriminalité

Ensemble peu homogène, la cybercriminalité relève

bsi-alertent-sur-le-niveau-de-la-menace-cyber-en-france-et-en-allemagne-dans-le-contexte-de-la-crise-sanitaire/ (consulté le 4 décembre 2022).

[12] A cet effet, le service central de renseignement criminel (SCRC) de la gendarmerie participe à la mise en oeuvre d'un projet de recherche cherchant à comprendre et à entraver le cyberharcèlement (Dulaurans, Fedherbes, 2022). Dénommé CyberNe Tic, ce projet a mis en ligne un site internet destiné à informer le public sur ce phénomène : https://cyberneticproject.eu/projet (consulté le 4 décembre 2022).

d'un biotope d'acteurs diversifiés. A l'évidence, ce sont les groupes cybercriminels organisés qui ont le plus fort impact au regard de leurs actions directes ou indirectes (*i.e.* mise à disposition de services). Leur suivi le plus complet relève paradoxalement non des forces de sécurité intérieures, mais des démarches de renseignement du secteur privée, dénommées *cyber threats intelligence* (CTI). Une typologie générale de ces groupes établie par la gendarmerie nationale française distingue :

- les groupes appartenant à un État et œuvrant en lien avec les services de renseignement de celui-ci afin de mener des cyber-attaques dans un intérêt géopolitique (atteintes aux institutions et à l'économie, désinformation et déstabilisation ayant pour but d'atteindre le moral des populations ou d'influencer un scrutin électoral, *etc.*) ;
- les groupes soutenus ou tolérés par un État, ayant une part d'activités servant les intérêts de celui-ci et une part d'activités autonomes ;
- les groupes indépendants et structurés, à finalité uniquement criminelle et orientés sur le profit ou le pouvoir ;
- les groupes d'activistes en ligne (*hacktivistes*), orientés sur la défense d'une cause politique ;
- les groupes cyber-terroristes, utilisant internet comme vecteur de leur cause (apologie, recrutement, renseignement, communication, attaques informatiques, *etc.*) ;
- les réseaux criminels informels et peu structurés, constitués de membres ne se connaissant pas nécessairement, mais unis par la convergence de leurs actions (trafics de produits illicites, *money mules*, pédopornographie, *etc.*).

Les trois premières catégories sont souvent appelées « groupes APT » (par dérivation de la désignation de leurs attaques discrètes et planifiées, dites « *advanced persistant threats* ») et fait l'objet d'une nomenclature précise[13] permettant leur suivi dans la durée et la réalisation d'attribution en cas de cyber-attaques. Ainsi, le groupe russophone APT 28 (« *Fancy bear* ») est supposément lié aux services de renseignements russes et serait actif depuis 2004, orienté sur le cyber espionnage, la désinformation et la déstabilisation à l'encontre des pays de l'OTAN, des structures sportives internationales et de l'Ukraine. Le groupe russophone REvil est un groupe cybercriminel actif depuis 2019, probablement en reconversion de l'ancien groupe dissout GrandCrab, il utilise et propose en RaaS l'un des rançongiciels les plus utilisés : REvil/Sodinokibi. L'importance de ses actions (dont l'attaque de l'entreprise *colonial pipeline* en 2021) a incité les autorités américaines à avertir fermement leurs homologues russes, ce qui a eu pour effet d'entraîner la suspension des activités de ce groupe. A cet effet, la succession des groupes est courante et impose la réalisation de généalogies : le groupe Egregor a ainsi succédé au groupe Maze, soit par transfert des acteurs, soit par reprise des outils[14]. Paradoxalement, la géographie est fortement conditionnant de l'action de ces groupes dans le choix des cibles (*e.g.*, certains rançongiciels ne fonctionnement pas sur des systèmes d'exploitation en cyrilliques ou dans des langues de pays amis de la Russie) et dans la coopération entre malfaiteurs (la communauté linguistique est un fort conditionnant dans l'association entre développeurs, opérateurs, voire affiliés).

[13] Voir, par exemple, *e.g.,* https://attack.mitre.org/groups/ (consulté le 4 décembre 2022).
[14] *e.g.*, https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-012.pdf (consulté le 4 décembre 2022).

Agissant à grande échelle pour la commission de faits susceptibles de déstabiliser une économie ou des organisations, ces groupes cybercriminels sont bien structurés et disposent d'une aptitude à la coopération avec des entités tierces. Ils recourent à des modes d'action sophistiqués et à une forte capacité d'innovation. Leurs revenus sont particulièrement importants et leur donnent une capacité d'investissement susceptible de permettre le développement de leur activité. Le perfectionnement des *modus operandi* impose cependant une spécialisation progressive des acteurs sur le modèle de division du travail existant dans l'économie légale : développeurs, fournisseurs de solutions d'attaque (*initial access broker, loaders, services de test,* vendeurs de kits *webinject* ou de kits de hameçonnage, courtiers en données ou en informations), testeurs (test d'antivirus ou de la validité de données), fournisseurs de service (services criminels en ligne, ou CaaS), pourvoyeurs de solutions d'anonymisation (hébergement *bulletproof*, VPN, *proxy*), vendeurs de matériel physique nécessaire à la commission d'infractions (*skimmers*, dispositifs de détection de réseau, *etc.*), distributeurs (envois de *spams* sur les réseaux sociaux ou par *mail*, mise à disposition de sites piratés), groupes spécialisés dans la mise en oeuvre de certaines attaques (rançongiciels, DDOS), recruteurs (infiltration d'entreprises ou corruption de salariés), groupes utilisant les outils développés par les groupes cybercriminels (affiliés), intermédiaires de paiement (mules, blanchisseurs, mixeurs de cryptomonnaies), *et cetera* (Broadhurst *et al.*, 2014).

Au-delà de ces groupes structurés et disposant de capacités techniques particulières, la cybercriminalité concerne une grande diversité de profils délinquants, d'une criminalité entrepreneuriale (récupération de *leads*, contact avec les victimes par des *call centers* situés à l'étranger, paiements en ligne), à une criminalité sociale (*brouteurs*, *sakawas*, *yahooboys* ou *feymens* procédant par imitation dans les cybercafés d'Afrique de l'Ouest), de pirates informatiques (*hackers*, *script kiddies*) à des individus isolés ou œuvrant en réseau (accès gratuit aux bouquets numériques, téléchargement illégal, promoteurs de haine, producteurs ou collecteurs de contenus pédophiles). Bien moins compétente techniquement, cette catégorie de cyber-malfaiteurs bénéficie de la démocratisation et de la standardisation des outils et des modes opératoires mis en ligne dans le cadre du *crime-as-a-service* (CaaS).

2.3 La géographie et les cybermenaces

Les aspects géo-criminels des cybermenaces comportent plusieurs dimensions. Internet n'est pas seulement un espace dématérialisé. Ses modélisations (modèle OSI en 7 couches, ou modèle TCP/IP en 4 couches) rappellent que des infrastructures physiques et techniques particulièrement lourdes sont nécessaires pour permettre à l'internaute de pénétrer dans un univers d'apparence virtuelle. Le modèle le plus communément utilisé distingue la couche physique (système informatique et réseaux matériels et électromagnétiques), de la couche logique (logiciels permettant de fournir les services attendus), , de la couche applicative (interface démocratisant l'utilisation du Web) et de la couche sémantique (contenu du Web autorisant les interactions sociales) (Douzet, 2014). Entre *data center* et câbles sous-marins, il convient donc de garder à l'esprit les nombreuses vulnérabilités physiques de l'internet, quand bien même l'infrastructure répartie du réseau lui assure une certaine résilience.

La topographie d'internet impose aux individus de

se réorienter dans un écosystème dont les paramètres sont totalement différents du monde physique. Cet univers est, par ailleurs, en rapide mutation et a connu d'importants changements depuis vingt ans entre l'internet des sites (le Web 1.0) mis en œuvre par des acteurs spécialisés, l'internet des réseaux sociaux (le Web 2.0) où chacun est en mesure d'apporter son contenu, et l'Internet des objets (parfois désigné comme Web 3.0) où l'interaction offerte par le numérique investit tous les objets du quotidien.

A cela s'ajoute la plus ou moins grande accessibilité de l'information entre un web référencé et immédiatement accessible, régi par la traçabilité des connexions et le référencement des contenus (*clearweb*), le web non référencé uniquement réservé aux abonnés d'un réseau ou d'un site (*deepweb*), et le web non référencé organisé autour de protocoles destinés à garantir l'anonymat des utilisateurs par le chiffrement et l'intermédiation (*darkweb*) (Rudesill *et al.*, 2015).

Au sein de cette géographie, les acteurs (internautes, fournisseurs d'accès, gestionnaires de sites, *registrar* procurant les noms de domaine et hébergeurs fournissant les capacités de stockage) ont des positionnements et des rôles différents. Ils détiennent chacun une partie des traces nécessaires à l'identification des usagers du réseau.

Cette trop brève description de la géographie de l'internet souligne à quel point le cyberespace fournit des points de repère bien différents qui bouleversent les opportunités criminelles.

Du point de vue criminologique, le cyberespace constitue à maints égard une infrastructure favorable à la délinquance. Il met à disposition des contre-mesures particulièrement nombreuses qui permettent de compliquer l'exploitation des traces par les forces de sécurité intérieure et de favoriser l'anonymat : communications directes (*peer to peer* - P2P), intermédiées (*virtual personnal Network* - VPN, hébergeurs non coopératifs - *Bulletproof hosting*), parcellisées (*Botnet*, mixeurs) ou brouillées (chiffrement, *darkphones*, tels que *Encrochat* et *Sky ECC* ; *darknet*, tels que TOR ou I2P). L'affaiblissement et la mobilité des identités ainsi que les possibilités d'usurpation (pseudos, *dataleaks*, *typosquatting*, *spoofing*) viennent renforcer ces difficultés d'identification. Parallèlement, Internet offre un accès inédit aux victimes par le piratage, la collecte et la valorisation des données des particuliers et des entreprises (fuites de données, ou *dataleaks*). La capacité à prévoir l'action des malfaiteurs est réduite dans un espace ou le mouvement et l'innovation sont la règle : adaptation rapide des modes opératoires existant aux niveaux technique, managérial ou du modèle économique ; identification et exploitation de vulnérabilités techniques (*e.g.*, failles de type *zéro Day*) et humaines (*i.e.,* manipulation par *social engineering*) ; mise à profit de l'évolution technologique (Internet des objet, crypto-actifs, NFT, Métaverse, pour ne citer que ceux-ci).

Du point de vue criminalistique, le numérique renouvelle l'intérêt pour la trace et en transforme les paramètres de sa collecte et de son exploitation. Le principe de déperdition des preuves formulé par le criminaliste français Edmond Locard selon lequel « le temps qui passe, c'est la vérité qui s'enfuie » (Locard, 1934) pourrait être reformulé par « le temps qui passe, c'est la vérité qui persiste », voire même « le temps qui passe, c'est la vérité qui réapparaît ». Les traces laissées sur internet sont, en effet, d'une particulière résilience et présentent tout autant d'une valeur intrinsèque que d'une valeur collective quand la congruence des unes est mise en écho avec les autres. L'internet des objets (*Internet of*

Things - IoT) va accroître la disponibilité et la dispersion des traces, en lien avec le cadre de vie des populations et les habitudes des individus (multimédia, domotique, *smart cities*, véhicules connectés et gérés en flotte, *etc.*) (Bouchaud, 2021).

Du point de vue victimologique, internet bouleverse la façon dont se distribue la criminalité. Il modifie en cela la répartition géographique traditionnelle de la délinquance et la concentration de certains phénomènes dans les centres urbains, plus propices aux violences et aux activités de trafic. L'a-territorialité[15] du cyberespace fait évoluer les modèles de dispersion de la criminalité, les activités en ligne et les vulnérabilités informatiques semblant désormais constituer les variables essentielles. La répartition des infractions paraît ainsi guidée par un critère démographique, plus que géographique[16]. Ce constat est essentiel, car il permet d'envisager que certaines populations relativement épargnées par la délinquance de masse sont aujourd'hui rattrapées par celle-ci au regard des fenêtres numériques qui permettent d'accéder à leur intimité (smartphone, PC, *etc.*). Chaque classe d'âge est différemment exposée : cyberharcèlement et atteintes à la réputation pour les plus jeunes, escroqueries pour les classes d'âge intermédiaires, avec abus de faiblesse pour les plus âgés. La *summa divisio* entre les particuliers et les personnes morales est également pertinente, les typologies de délinquance étant relativement distinctes.

Au terme de cette brève analyse orientée sur les phénomènes, les auteurs et la géographie, la cybercriminalité apparaît comme un enjeu de sécurité essentiel. Son accroissement exponentiel et ses implications majeures en termes politique, économique et social implique de repenser la lutte contre cette menace prioritaire.

3. Réguler la cybercriminalité

Si la cybercriminalité a été anticipée par le législateur, une organisation et des mesures, les effets de ces dispositifs n'ont manifestement pas permis de limiter une forme de délinquance qui est devenue une menace majeure en 20 ans. Cela interroge l'efficacité des moyens de lutte traditionnels, fondés sur un schéma relativement classique consistant à normer (création d'un cadre juridique adapté au niveau national et international), à institutionnaliser (création d'unités et juridictions spécialisées destinées à prendre en charge un contentieux naissant), puis à démocratiser (recherche d'une décentralisation de compétences en vue de faire face à la croissance du contentieux). Cette approche des institutions publiques est essentiellement réactive. Elle ne cherche ni à comprendre, ni à entraver les causes même des phénomènes. Pour autant, aux côtés de cette action axée sur le traitement judiciaire, les acteurs de l'internet se sont souvent eux-mêmes organisés pour tenter de réguler les phénomènes selon des méthodes diversifiées (3.1). Accompagnant cette

[15] Terme évoqué lors d'un colloque au Conseil d'État organisé le 28 septembre 2016 : « L'a-territorialité du droit à l'ère numérique ».

[16] Les analyses du SCRCGN ont établi une typologie relative à la répartition spatiale des phénomènes criminels en fonction de la nature des opportunités criminelles :

- certains ont une répartition criminologique, en ce sens que les déplacement d'un délinquant ou d'une bande criminelle expliquent la localisation des infractions (*e.g.*, sur-représentation des vols avec violence en milieu urbain, vol de fret routier par des modes opératoires perfectionnés) ;
- d'autres ont une répartition géographique, car l'implantation des victimes conditionne la survenance des infractions (*e.g.*, atteintes aux entreprises ou à un secteur économique) ;
- d'autres phénomènes, enfin, ont une répartition démographique, car leur localisation est proportionnelle à l'implantation des populations sur un territoire (*e.g.*, homicides, violences intrafamiliales ou intrafamilières, mais aussi cybercriminalité dont la survenance n'est pas conditionnée par le lieu où se trouve la victime, mais par sa seule présence sur le Web et, parfois, par sa provenance linguistique).

Cette classification empirique est à mettre en lien avec la théorie des activités routinières (Cohen, Felson, 1979)

dynamique, les force de l'ordre ont tout intérêt à mettre en œuvre les principes d'une police guidée par le renseignement, fondée sur une meilleure compréhension de la délinquance (3.2) en vue d'une action plus efficiente (3.3).

3.1 Réprimer ou réguler ?

Le sociologue français Michel Crozier affirmait que, dans tout système, les acteurs investissent les zones indéfinies et utilisent cette incertitude à leur profit (Crozier, Friedberg, 1977). Internet est initialement conçu comme un espace d'échange et de liberté, une a-territorialité vierge et sans frontière qui a été investie diversement par les acteurs au niveau politique, économique, social et légal. Ses zones indéterminées sont particulièrement importantes et la régulation des acteurs privés a bien souvent pris le pas sur la normalisation des États. La tentative de la convention de Budapest de simplifier les échanges entre États afin de mieux prendre en compte un phénomène d'essence transnationale n'a pas produit les effets escomptés. Il est probable que le second protocole additionnel adopté en 2021 ne fasse pas grandement évoluer cette situation.

Orientés sur une logique traditionnelle d'interdit et de répression, les États recourent aux outils habituels offerts par leur arsenal répressif. Destinés à prouver le lien entre un fait infractionnel et son auteur sur la base de garanties procédurales fortes dans le but de répression d'un interdit pénal, ces outils ne sont pas forcément les instruments les plus adaptés pour lutter contre un phénomène massif et permanent. Au regard du faible taux d'élucidation et des difficultés à aborder au cas par cas une délinquance technique et massive, le volume des affaires judiciaires traitées avec succès est sans commune mesure avec l'ampleur du contentieux (Barlatier, 2020b). Elles débouchent sur des peines bien souvent assez peu dissuasives au regard des bénéfices que ces délits génèrent. Au demeurant, l'action judiciaire ne permet souvent qu'une neutralisation ponctuelle et superficielle, l'action policière se concentrant sur les maillons les plus visibles, mais aussi les plus interchangeables des réseaux, les donneurs d'ordre et les gestionnaires d'infrastructure de délinquance étant rarement inquiétés.

Ainsi, après les atteintes aux biens, la délinquance économique et financière et le trafic de stupéfiants, la cybercriminalité porte un nouveau soupçon sur la capacité du système pénal à représenter le seul, sinon le principal, sinon le plus légitime, moyen de lutte contre la délinquance (Barlatier, 2019 et 2020b).

Cette incapacité de soumettre l'internet au droit a très tôt été perçue par les acteurs publics et privés qui ont développé des dispositifs de régulation sectoriels pour instaurer des espaces de stabilité sur la toile.

Ces régulations sont, d'ailleurs, souvent devenues des enjeux de pouvoir et de profit. Le fonctionnement des GAFAM-T en est probablement le plus symbolique. Acteurs structurant du *Web*, ces multinationales sont incontournables et disposent d'une position dominante en termes d'infrastructures physiques et logicielles (Microsoft, Apple), de référencement (Google), de réseaux sociaux (Facebook, Twitter) ou de commerce (Amazon). Par la maîtrise de la donnée, ces acteurs bénéficient des attributs foucaldiens d'un savoir panoptique et d'un pouvoir sur le comportement de chacun au sein d'un espace de socialisation totalement tracé, auquel les individus sont devenus dépendants (Foucault, 1975). L'analyse des données permet tout à la fois la maîtrise du général (activité économique et des

populations) et du particulier (accès à la vie privée de chacun). Cumulant le tout et les parties dans une approche tout aussi holistique que casuistique, la puissance centralisatrice de ces multinationales privées est traditionnellement mise en lien avec le *soft power* américain que les autres puissances continentales tentent tardivement d'endiguer avec des mesures de protection (règlement général de protection des données - RGPD - au sein de l'Union européenne) ou de cloisonnement (création de barrières techniques isolant les internet russes et chinois). Révélatrice des équilibres géopolitiques, internet devrait être le témoin, dans les années à venir, du développement des BATX[17] et de la maîtrise la 5G qui accompagneront et faciliteront l'affirmation de la puissance politique et économique chinoise. La puissance de ces multinationales s'illustre particulièrement à l'égard du pouvoir traditionnel des États dans les enquêtes judiciaires conduites par les forces de sécurité intérieure. Généralement installées aux États-Unis, l'accès à leur données implique le processus lourd et complexe d'une demande d'entraide pénale internationale (DEPI). Toutefois, s'abstrayant du cloisonnement juridique des États, l'enquêteur peut tout aussi bien adresser directement sa demande auprès de l'opérateur privé dans le cadre d'une *legal request*. L'opérateur de l'internet examinera alors cette demande au regard de ses conditions générales d'utilisation (CGU) et acceptera de répondre aux enquêteurs si celles-ci sont enfreintes (*e.g.*, en cas de pédopornographie ou d'apologie du terrorisme). En l'espèce, le droit contractuel des opérateurs de l'internet s'avère d'une plus grande efficacité que les traités d'entraide judiciaire (*Mutual Legal Assistance Treaty* - MLAT).

Au-delà de la régulation des géants de l'internet, la toile fait l'objet de nombreuses initiatives d'acteurs privés cherchant à renforcer leur sécurité dans un cyberespace qui est source de risques comme de profits pour les entreprises. La sécurité des systèmes d'information (SSI) est ainsi devenue un marché autonome et fortement structuré, sous une forme internalisé aux entreprises ou sous celle de prestations de services. Par exemple, la création de CERT (*Computer Emergency Response Team*) illustre la volonté de centraliser les données et d'analyser les cyber menaces afin d'y apporter des parades appropriées. En France, l'agence nationale de sécurité des systèmes d'information (ANSSI) est un organisme public venant unifier ces initiatives éparses en apportant une vision d'ensemble. Ces dix dernières années la *cyber threat intelligence* (CTI) s'est développée comme méthode de ces organisations. Cette discipline structure le recueil et l'analyse des informations sur les cyber menaces. L'intention est de comprendre la nature des atteintes, le profil des cibles et des attaquants. L'objectif est d'anticiper, de détecter ou de parer aux attaques informatiques. Ces méthodes s'inspirent fortement des principes du renseignement et se fondent sur le recueil de données multi-sources (*e.g.*, sources humaines, ouvertes ou techniques), la détection des signaux faibles (*Indicators of Compromissio*n - IOC), un traitement et une analyse débouchant sur des mesures de remédiation diversifiées du niveau tactique au niveau stratégique (Kuerbis *et al.*, 2022).

Il convient également de ne pas négliger les initiatives citoyennes sur la toile. Particulièrement diversifiées, elles tendent à recréer un contrôle social en informant sur les menaces (sur les sites et réseaux sociaux), en organisant une vigilance (lanceurs d'alerte, signalement de contenus illicites), en constituant une aide à la détection (*e.g.*, site

[17] Acronyme désignant les quatre plus grandes entreprises technologiques chinoises : Baidu, Alibaba, Tencent et Xiaomi.

haveibeenpwned en matière de compromission d'identifiants) débouchant parfois sur une logique de milice (*e.g.*, action violente de certains traqueurs de pédophiles) (Hadjimatheou, 2019 ; Frampton, 2020). Dans ce même ordre d'idée, la viralité d'internet a favorisé le développement des fausses informations (*fake news*) que des initiatives de particuliers comme de professionnels, et notamment des entreprises de presse tentant de restaurer leur rôle, tentent de limiter par une démarche d'éclaircissement fondée sur une analyse critique (*debunking, hoaxbusting*) (Petratos, 2021).

Face à ces initiatives éparses et peu coordonnées, les administrations françaises se sont également organisées afin de répondre aux cyber menaces[18] par la création d'agences d'analyse et de remédiation, tels que l'ANSSI[19], destinée à la protection des organismes d'importance vitale (OIV), ou le GIP ACYMA[20], destiné aux particuliers et aux entreprises. Le système pénal s'est, quant à lui, articulé autour de compétences décentralisées (C-NTECH, ESI, NTECH[21], ICC[22]), d'unités d'enquête ou d'appui dédiées (EC3[23], C3N[24], OCLCTIC[25], BEFTI[26]) ou de juridictions spécialisées (*e.g.*, section J3 au tribunal judiciaire de Paris). Transposant son organisation territoriale à la problématique numérique, la gendarmerie nationale a, par ailleurs, créé en 2021 un commandement dans le cyberespace (ComCyberGend) et orienté la gestion de ses ressources humaines vers cette thématique (*e.g.*, création d'un recrutement destiné aux officiers scientifiques, intégration de compagnies de « cyber-gendarmes »). Ces services ne sont toutefois qu'une simple évocation de l'ensemble des administrations françaises impliquées dans la lutte contre les cyber menaces dans le cadre de la lutte contre la fraude (*e.g.*, CSCE[27]), du renseignement (*e.g.*, DGSI[28], DGSE[29], cyber douanes) ou de la défense nationale (COMCYBER[30]).

En vingt ans, les institutions publiques ont ainsi constamment évolué avec le droit pour lutter contre la cybercriminalité, tentant de répondre, souvent de façon réactive aux menaces avec des moyens techniques et des prérogatives juridiques adaptés. Sur la base de pouvoirs généraux ou de textes spécifiques, la procédure pénale s'est ainsi adaptée

[18] Pour une présentation et un organigramme des chaînes cyber (protection, défense, renseignement et judiciaire), disponible le site de l'IHEMI le 31 juillet 2022 : https://www.ihemi.fr/articles/organisation-france-europe-cybersecurite-cyberdefense-V2

[19] Agence nationale de sécurité des systèmes d'information (ANSSI), créée en 2009 et relevant d'un organisme rattaché au Premier ministre, le secrétariat général à la défense et à la sécurité nationale (SGDSN).

[20] Groupement d'intérêt public « Action de lutte contre la cybermalveillance » (ACYMA).

[21] La gendarmerie nationale dispose de correspondants N-TECH (C-NTECH) dans les unités territoriales, d'enquêteurs sur internet (ESI) dans les unités de recherche et des spécialistes nouvelles technologies (N-TECH) dans les unités d'appui, formant une communauté de 8.000 professionnel dénommée CYBERGEND.

[22] Enquêteurs en cybercriminalité (ICC) de la police nationale.

[23] European Cybercrime Center (EC3) de l'office européen de police (EUROPOL).

[24] Centre de lutte contre les criminalités numériques (C3N) de la gendarmerie nationale.

[25] Office central de lutte contre la criminalité liée au technologies de l'information et de la communication (OCLCTIC) rattaché à la police nationale.

[26] Brigade d'enquête sur les fraudes aux technologies de l'information et de la communication (BEFTI) de la préfecture de police de Paris.

[27] Centre de surveillance du commerce électronique (CSCE) relevant du service national des enquêtes (SNE) de la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF).

[28] Direction générale de la sécurité intérieure (DGSI), service de renseignement du ministère de l'intérieur chargé de la sécurité nationale et des intérêt fondamentaux de la Nation sur le territoire national.

[29] Direction générale de la sécurité extérieure (DGSE), service de renseignement du ministère des armées chargé de la recherche et de l'exploitation des renseignement intéressant la sécurité de la France, ainsi que de la détection et de l'entrave hors du territoire national, des activités d'espionnage dirigées contre les intérêts français.

[30] Commandement de la cyberdéfense (COMCYBER), rattaché au ministère des armées et réunissant, sous une direction opérationnelle unique et interarmes, les forces de cyberdéfense.

aux enjeux de la détection d'infractions et de la collecte de preuves : saisie et exploitation des supports numériques[31], accès aux données détenues par un tiers[32], enquêtes sous pseudonyme[33], interceptions de correspondance[34], perquisitions et saisie de données en ligne[35], captation de données à distance[36]. L'ensemble de ces pouvoirs trouvent leur équivalent dans le code de la sécurité intérieure[37] où est ajoutée, par ailleurs, la notion d'algorithme, ou « boîte noire », obligeant les fournisseurs d'accès à mettre à disposition des données de connexion à fin de traitement par les services de renseignement[38]. En revanche, le droit français refuse la mise en œuvre de procédés de lutte informatique offensive (LIO)[39] dans le cadre des missions d'enquête judiciaire.

S'adaptant au niveau tactique, les forces de l'ordre évoluent peu cependant dans leur stratégie, les dispositifs de lutte contre la délinquance continuant à recourir à un traitement individualisé et parcellisé du contentieux fondé sur la plainte de la victime. La mise en œuvre de plate-forme de recueil de signalement fait exception à cela. Sans souci de cohérence, celles-ci se sont démultipliées au sein des forces de l'ordre ces dernières années pour le signalement de contenus illicites (PHAROS)[40], le signalement d'escroqueries en ligne à la carte bancaire (PERCEVAL)[41], la plainte en ligne pour escroqueries (THESEE)[42] ou tout simplement la prise de contact en ligne avec les forces de l'ordre[43]. Mise en œuvre par la gendarmerie nationale, la plate-forme PERCEVAL[44] représente un changement de paradigme car elle ne fait plus de la plainte de la victime un préalable : le seul signalement de celle-ci est pris en compte, enrichi avec d'autres sources, rapproché en vue de générer des éléments permettant soit l'ouverture d'une enquête judiciaire, soit la recherche de solutions préventives avec les partenaires (Barlatier, 2020a). Cette approche apparaît comme un signe prometteur d'une nouvelle articulation entre la

[31] Art. 14, 66, 77-1 et 156 CPP et 230-1 suiv CPP pour la mise au clair de données chiffrées.
[32] Art. 14 CPP en sources ouvertes, art. 60-1, 77-1-1 et 99-3 CPP pour les données en sources fermées.
[33] Art. 230-46 CPP.
[34] Combinaison des art. 100 et 706-95 CPP pour l'interception du flux avec les art. 56 suiv, 76, 92 suiv, 706-95-1 CPP et la convention de Budapest pour l'exploitation des données en mémoire.
[35] Art. 56 suiv, 76 et 92 pour les perquisitions de jour, dont art. 57-1 pour les perquisitions à distance, art. 706-28, 706-35, 706-73, 706-89 et 706-91 CPP pour les perquisitions de nuit, convention de Budapest pour les données situées à l'étranger, art. 56 suiv, 76, 92, 94, et 96 CPP pour les saisies.
[36] Art. 706-102-1 CPP.
[37] Art. L851-1 CSI pour le recueil des données de connexion ; art. 851-2 CSI pour l'interception en temps réel des données de connexion, le géolocalisation en temps réel et les interceptions de correspondances par voie hertzienne ; art. L851-1-1 CSI pour les interceptions de sécurité ; art. L851-6 CSI pour l'identification d'un utilisateur par son appareil et le recueil de ses données de connexion ; art. L853-1 CSI pour la sonorisation et la captation d'images ; art. L853-2-1 CSI pour le recueil et la captation de données informatiques ; art. L853-3 CSI pour l'autorisation de pénétrer dans un véhicule ou un lieu privé pour la mise en oeuvre de ces techniques ; loi du 30 octobre 2017 prévoyant les visites domiciliaires, les assignations à résidence, ainsi que les mesures individuelles de contrôle administratif et de surveillance (MICAS - art L228-1 à L228-7 CSI), telles que l'interdiction d'entrer dans un périmètre géographique, l'obligation de se présenter périodiquement à un service de police ou à une unité de gendarmerie, celle de déclarer son lieu et ses changements de domicile, et le placement sous surveillance électronique.
[38] Art. 851-3 CSI.
[39] Introduction dans un système de traitement automatisé en vue d'en extraire, d'en altérer ou d'en neutraliser les données.

[40] La plate-forme PHAROS est accessible sous le lien suivant : https://www.internet-signalement.gouv.fr/PharosS1/ (consulté le 4 décembre 2022).
[41] La plate-forme PERCEVAL est accessible sous le lien suivant : https://www.service-public.fr/particuliers/vosdroits/R46526 (consulté le 4 décembre 2022).
[42] La plate-forme THESEE est accessible sous le lien suivant : https://www.moncommissariat.interieur.gouv.fr/fr/demarches/la-plainte-en-ligne-pour-les-arnaques-sur-internet-thesee (consulté le 4 décembre 2022).
[43] Issue de la récente fusion du site de la brigade numérique de la gendarmerie nationale et moncommissariat.fr de la police nationale, l'application ma sécurité est téléchargeable sous le lien suivant : https://play.google.com/store/apps/details?id=com.masecuriteapp&hl=fr&pli=1
[44] Dédiée aux escroqueries à la carte bancaire, la plate-forme PERCEVAL recueille en ligne les signalements des victimes sur la base d'une identification forte (*via* France Connect). Les informations ainsi collectées sont recoupées et enrichies avec les banques et e-commerçants afin de disposer de la masse critique d'informations nécessaires au développement de solutions de remédiation.

tradition judiciaire fondée sur la casuistique et la recherche de solutions nouvelles permettant une action à plus grande échelle.

Entre répression et régulation, les stratégies, souvent empiriques, choisies pour lutter contre la cybercriminalité se sont avérées insuffisantes et n'ont pas permis d'enrayer l'apparition d'une nouvelle dimension dans l'univers de la délinquance (Barlatier, 2019). De nouvelles méthodes en termes de compréhension et d'entrave pourraient ainsi être éprouvées. Elles invitent à présenter les apports du renseignement criminel.

3.2 Comprendre

Le renseignement criminel est une préoccupation ancienne et une méthode nouvelle. Il apparaît en France sous sa forme embryonnaire avec l'idée de « Haute police », où la préoccupation était de neutraliser les opposants politiques en les identifiant au sein de la population. Avec l'émergence de l'enquête en France, Vidocq importe cette préoccupation dans le champ criminel. Ancien condamné ayant construit sa réputation sur l'évasion, il acquiert une connaissance de la population criminelle au sein des bagnes, et met son savoir au service de la préfecture de police de Paris dans le cadre d'une action aussi efficace que contestée (Kalifa, 2013). Le renseignement criminel se fonde ainsi sur la logique de connaissance *a priori* des criminels. Cette vision sera contrebalancée quelques années plus tard par la promesse positiviste de solutionner le crime avec la science, inversant ainsi un schéma qui ne part plus des auteurs pour leur attribuer les faits qu'ils commettent, mais part des faits pour identifier les auteurs. La logique de l'enquête héritée de Vidocq restera néanmoins présente dans la culture et les méthodes des services de police judiciaire luttant contre la grande criminalité.

L'idée d'un savoir précédant l'action connait un renouveau avec l'émergence de l'*intelligence-led policing* (ILP), ou police guidée par le renseignement. Ce mouvement apparaît non pas dans le cadre d'une police scientifique portée par les sciences exactes, mais plutôt d'une approche scientifique de la police portée par les sciences humaines (Barlatier, 2020c). Partant du fameux « *Nothing Work's* » de Robert Martinson (Martinson, 1974), après des premiers constats inquiétants sur l'efficience réelle des modes d'action des forces de l'ordre[45], les chercheurs ont abouti au constat criminologique que les pratiques policières devaient être évaluées et sortir des seules approches empiriques ou managériales qu'elles avaient connu jusqu'à présent. Les criminologues ont ainsi, tour à tour, proposé la création d'une police fondée sur la proximité avec les populations (*Community Policing* - COP ; Skogan, Hartnett, 1977), puis d'une police de résolution de problème (*Problem-Oriented Policing* - POP ; Goldstein, 1990). L'ensemble de ces politiques policières proposent le passage d'une police bitnérienne, pyramidale, bureaucratique, militarisée, réactive et concentrée sur ses propres modalités de fonctionnement (Bitner, 1970) à une police plus proactive et recentrée sur sa mission. Si elles ont montré une certaine efficience qui leur valent depuis d'être, tout à tour, reprises sous diverses politique gouvernementales (la fameuse alternance en France entre police d'intervention et police de proximité), le COP et le POP se limitent à proposer une compréhension et des entraves se réduisant à un traitement local de la délinquance. A la fin des années 1990, avec l'ILP, le criminologue britannique

[45] Par exemple, la célèbre expérience de Kansas City pour l'efficacité des patrouilles des police (Harris, 1977) ou l'étude de la Rand Corporation relative à la performance des enquêtes judiciaires (Chaiken *et al*., 1977).

Jerry Ratcliffe propose d'améliorer la pertinence de l'action policière en agissant à plus grande échelle sur les phénomènes criminels à partir de leur compréhension préalable (Ratcliffe, 2016).

Intégrée dans la criminologie francophone sous le vocable de « renseignement criminel », l'ILP repose sur les postulats de quatre grande théories criminologique (Maillard, 2017) :

- celle des « *prolific offenders* » (Wolfgang, Figlio, Sellin, 1972), qui indique que la majorité des infractions sont commises par une minorité de délinquants chroniques (*prolific offenders*) ayant érigé la criminalité en un mode de vie. La connaissance de ces individus permet de concentrer l'action des forces de l'ordre sur la population délinquante utile ;
- celle des « activités routinières » (Cohen, Felson, 1979), avançant l'importance de la notion d'opportunité criminelle dans la commission du crime, fruit d'une activité de routine où se rencontrent des individus (l'auteur, la victime) et des occasions (dans un cadre espace-temps). La compréhension de ces circonstances permet d'identifier les modèles fondés sur les répétitions criminelles (Bradford, 2017) ;
- celle du « choix rationnel » (Felson, Clarke, 1998), où le délinquant s'adapte à son environnement immédiat en fonction d'un calcul en termes de risques et de bénéfices. La compréhension de la délinquance implique donc de se mettre à la place du criminel et de connaître les paramètres de son choix ;
- celle des « *patterns* » (Brantingham, Brantingham, 1994), à partir de laquelle il est possible d'analyser les répétitions et les anomalies dans la récurrence des faits afin de pouvoir établir les caractéristiques uniques d'un phénomène criminel. Par exemple, dans une approche géographique, le mouvement du *hot spotting* se fonde sur l'analyse des concentrations criminelles.

L'ILP propose trois focales d'analyse (Maillard, 2017) :

- le niveau stratégique, qui est une aide à la compréhension des phénomènes, de la géographie et des groupes criminels ;
- le niveau opérationnel (ou opératif), qui est une aide à la décision pour les autorités politiques, hiérarchiques, administratives ou judiciaires ;
- le niveau tactique, qui est une aide à l'enquêteur ou au patrouilleur pour l'accomplissement de sa mission.

Au sein de la gendarmerie nationale, la méthode du renseignement criminel a été formalisée à partir du cycle du renseignement (collecte-traitement-analyse-production) et de la logique de raffinage qui y est attachée (*Data-Information-Knowledge-Intelligence*, mieux connu sous la dénomination « DIKI »). Face au processus linéaire de l'enquête judiciaire fondé sur l'exploration des pistes, le renseignement propose ainsi un processus circulaire selon une boucle itérative et incrémentale qui repose sur quatre qualités :

- l'exhaustivité, car la phase habile de collecte des données ne se limite pas aux seuls éléments de l'activité des services d'enquête (qui transforment bien souvent leurs analyses en de simples bilans d'activité), mais exploite l'ensemble des sources disponibles (ouvertes ou fermées, d'origine humaine, financière, cyber, technologique, culturelles, *etc.*) ;

- la rigueur, car la phase souvent technique de traitement de l'information impose de classer, d'uniformiser, d'indexer et de visualiser des données de plus en plus volumineuses afin d'en tirer des informations utiles à la confrontation et à l'exploration des éléments collectés ;
- pertinente, car la phase intellectuelle d'analyse doit permettre d'élaborer un savoir fondé sur une pensée critique ou la logique, comme la capacité de conception et de confrontation des hypothèses permettent de comprendre ce qui se voit et d'envisager ce qui ne se voit pas (*i.e.*, *intelligence gap*) ;
- maîtrisée, car la phase persuasive de production du renseignement doit transformer ce savoir en action dans le cadre de constats, d'interprétations et de recommandations utiles au destinataire.

Cette méthode n'est pas spécifique au renseignement criminel. Elle est un processus de connaissance mis en œuvre, de façon plus générale, par les « travailleurs du savoir » (Bouchez, 2004). Dans le monde du numérique, elle est déjà mise en œuvre par les acteurs de la *cyber threat intelligence* (CTI) chargés de l'analyse des cyber menaces (Wagner et al., 2019). La CTI est destinée à élaborer une analyse de risque permettant de connaître les menaces et d'identifier les vulnérabilités. Elle envisage la compréhension technique et contextuelle :

- des outils utilisés, par l'inventaire et la retro-ingénierie des *malwares*, des logiciels et autres infrastructures techniques de délinquance ;
- des modes d'action, par la connaissance des pratiques sur l'ensemble du processus, de la recherche d'informations préalables à la reconnaissance, des techniques de pénétration, d'attaque, des modalités d'exploitation des bénéfices (paiement, blanchiment et remploi) ;
- des acteurs, orientées sur le recensement des groupes cybercriminels et de leur rôle, permettant une connaissance de leurs caractéristiques et de leurs capacités, un suivi historique et une anticipation de leur évolution, la compréhension et l'attribution de leurs actes.

Impliquant une coordination entre les acteurs publics et privés fondée sur la circulation de l'information, la CTI repose sur des méthodes et des modèles relativement standardisés, tels que les référentiels *Kill chain*[46] et Mitre[47], ou les classement YARA[48] et SIGMA[49]. L'objectif est le partage de signaux faibles (dont les IoC, *indicators of Compromise*, destinés à la détection des signes d'intrusion), des tactiques et des techniques d'attaque, et enfin des mesures de remédiation pouvant être adoptées. Les éléments ainsi collectés sont versés dans un *security information and event management* (SIEM) qui est destiné à établir les relations et les corrélations entre les événements enregistrés et les modèles connus.

Sommairement décrite, la CTI est compatible avec les finalités et les méthodes du renseignement criminel. Orientée sur les aspects les plus techniques, elle ne répond pas intégralement aux

[46] Pour une synthèse d'écrits sur le référentiel *Kill Chain* : https://www.sciencedirect.com/topics/computer-science/kill-chain (consulté le 4 décembre 2022).
[47] Pour accéder aux à la documentation Mitre : https://attack.mitre.org/techniques/enterprise/ (consulté le 4 décembre 2022).
[48] Pour accéder à la documentation Yara : https://yara.readthedocs.io/en/stable/index.html (consulté le 4 décembre 2022).
[49] Pour une synthèse de ces méthodes : https://www.threat-intelligence.eu/standards/ (consulté le 4 décembre 2022). Ce site contient également un certain nombre de références utiles en termes d'analyse.

attentes de compréhension de l'ensemble des phénomènes délinquants. Particulièrement utile en termes d'atteintes aux systèmes de traitement automatisé de données (ASTAD), la CTI est insuffisante pour aborder les atteintes aux biens (escroqueries et fraudes, notamment) et aux personnes (insultes, diffamation, harcèlement, pédopornographie, *etc.*) qui doivent faire l'objet d'une compréhension criminologique plus que technique. La CTI permet d'élaborer un renseignement d'intérêt cyber (RIC) qui ne doit pas être confondu avec le renseignement d'origine cyber (ROC ou *cyber intelligence* - CYBINT) qui aborde le numérique comme une source de renseignement (tel que le *Social Media Intelligence* - SOCMINT) et non comme un sujet d'analyse (Brun *et al.*, 2022).

A cet effet, si la CTI est une méthode adaptée et compatible avec le renseignement criminel, elle ne doit pas être sanctuarisée au risque de perdre de sa pertinence. L'analyste en renseignement criminel spécialisé dans les cybermenaces doit évoluer dans un écosystème plus large, entouré de ses collègues spécialistes en termes de trafics illicites, de traite des êtres humains, de violences aux personnes, de victimologie, d'infractions économiques et financières, de vols et de recel, de connaissance des groupes criminels ou de géographie criminelle. L'analyste cyber doit pouvoir bénéficier de l'écosystème de compréhension des autres domaines de la criminalité car, pas plus que l'utilisation de la voiture au début du XX^{ème} siècle n'était sécable de la délinquance de son époque, la cybercriminalité au début du XXI^{ème} siècle n'est pas une forme de délinquance à part entière. Elle reste, pour l'essentiel, un nouveau mode d'action des criminalités traditionnelles.

Destiné à réduire l'incertitude par une compréhension au plus près des réalités, le renseignement criminel est un savoir en vue d'une action réelle et concrète sur la délinquance. Il est ainsi en mesure de renouveler les solutions de lutte contre la cybercriminalité.

3.3 Agir

La compréhension préalable des phénomènes permet de faciliter la recherche de solution et la détermination des stratégies pour les mettre en œuvre. Le renseignement criminel s'inscrit dans un objectif performatif de remédiation (au sens étymologique de « porter remède »). Les solutions qu'il propose n'ont pas à être limitées à la recherche d'une réponse judiciaire sur l'infraction principale, mais envisage plus largement l'annihilation d'un mode opératoire ou d'un groupe criminel par tout moyen légal.

A cet effet, le champ de la réponse policière s'inscrit dans la dynamique « *What works? What doesn't? What's promising?* ». Diversifiant le champ des possibles, il repose tant sur une logique de *benchmark* et de retour d'expérience de solutions déjà éprouvées, que sur la capacité à concevoir de nouvelles solutions innovantes, et parfois audacieuses. En application de la matrice SWOT (*Strengths, Weaknesses, Opportunities, Threats*), les recommandations doivent être conçues à partir d'une analyse des paramètres internes (forces et des faiblesses) et externes (opportunités et des menaces). Dans leur mise en œuvre, elles doivent être précises, évaluables, réalistes, pertinentes et cohérentes dans le temps, conformément aux principes SMART (*Specific, Measurable, Attainable, Relevant, Time-based*).

Sur le socle de ces notions fondamentales, trois formes de remédiations sont généralement distinguées :

- l'entrave pénale, qui consiste à mettre en

évidence un interdit afin de faciliter la constatation des infractions, d'améliorer le recueil des preuves ou de faciliter l'identification des auteurs. Elle recherche le prononcé d'une décision judiciaire adaptée concernant l'infraction principale ou des infractions secondaires ou incidentes. Cela pourrait consister à obtenir l'incarcération d'un individu sur le simple constat du non-respect de ses obligations de contrôle judiciaire, par exemple ;

- l'entrave administrative, qui consiste à mettre à profit, de façon distincte ou combinée, les pouvoirs dont disposent les administrations en termes fiscal, de prestations sociales, de répression de fraudes, de droit douanier, de législation sur les étrangers, *et cetera*. La coordination avec les administrations de l'État et des collectivités locales revêt alors un aspect essentiel afin d'autoriser une réaction intégrée de l'autorité publique à la criminalité, fondée sur la détection de situations criminelles, la dissuasion, l'empêchement ou la neutralisation des auteurs. Cela peut consister à créer un environnement administratif hostile à l'égard d'un délinquant, ou à combler une vulnérabilité réglementaire qui profite à la fraude ;
- l'entrave partenariale, qui consiste à proposer des solutions préventives ou curatives avec la coopération d'acteurs privés. Souvent fondée sur une action portant sur les circonstances du crime, elle consiste, dans une logique de prévention situationnelle, à mieux informer les victimes, à mieux protéger les cibles, à réduire l'utilité du crime ou à accroître les risques de détection et d'identification pour les auteurs. Cela consiste, par exemple, à inciter un commerce à modifier ses processus de vente pour réduire les opportunités de vol.

Le renseignement criminel ouvre ainsi le champ des possibles en termes de modes d'action. Les forces de l'ordre ne sont plus tenues à des processus standardisés mis en œuvre dans le cadre d'une obligation de moyens. Le traitement judiciaire de la délinquance n'est plus l'unique réponse des forces de l'ordre. Cela permet d'échapper à l'involution des buts que représente une approche managériale du système pénal (Jean, 2008 ; Cliquennois *et al.*, 2015), où les flux de délinquance traités dépendent de la capacité des institutions à les assumer (prise de plainte, élucidation, poursuite, capacité d'audiencement, stock pénitentiaire, *etc.*). L'analyste en renseignement criminel doit être en mesure de proposer de nouveaux filons d'efficacité et de tenter d'enrayer les phénomènes le plus en amont possible. S'inscrivant dans une approche pragmatique et conséquentialiste, il doit pouvoir bénéficier de la diversité des outils offerts par la criminologie. Le policier devient le catalyseur des moyens de lutte contre la délinquance.

L'écosystème cyber est particulièrement propice à un tel décloisonnement des solutions. Les acteurs de sa régulation proposent déjà des mesures de remédiation recourant à une gestion du risque, avec des réponses graduées, loin de l'approche disjonctive entre le légal et l'illégal. Abordant les phénomènes de façon holistique et non casuistique, ces solutions recherchent le plus fort impact au moindre coût. Fondées sur l'analyse de données, elles mettent en oeuvre des stratégies inventives. D'une façon générale, les méthodes d'entrave sur le

Web reposent sur la cinématique détection - caractérisation - blocage - signalement. Tel est le cas des algorithmes de détection des transactions frauduleuses mis en œuvre par les e-commerçants et les banques à partir des *patterns* de fraude connus. Le signalement des fraudes en ligne par les internautes sur les forums et réseaux sociaux est également un moyen de rétablir un contrôle social dans cet espace d'anonymat par une information pertinente des victimes destinée à désamorcer les situations pré-criminelles.

Certains États sont en mesure de mettre en œuvre des stratégies bien plus élaborées. Ainsi, pourtant considéré comme garantissant l'anonymat de ses utilisateurs, le *darkweb* n'échappe-t-il pas à l'action des services de renseignement. La surveillance du téléchargement et de l'utilisation de TOR[50] permet, par exemple, de disposer de signaux faibles à l'égard d'internautes susceptibles d'avoir des activités clandestines. Ainsi, des stratégies offensives et audacieuses ont pu être développées à l'égard des *darkmarket*. En 2017, une opération combinée du *Federal Bureau of Investigation* (FBI) et de la police néerlandaise a ainsi permis de saisir les deux plus importantes *marketplace*[51] : laissant leurs homologues néerlandais prendre le contrôle du site *Hansa Market* par des techniques de lutte informatique offensive (LIO) auxquelles leurs services sont habilités, les fédéraux américains ont ensuite saisi le site *Alphabay*. Poussés par la nécessité de continuer leur activité marchande, les utilisateurs d'*Alphabay* se sont majoritairement réfugiés sur *Hansa Market*, autorisant ainsi leur identification par la police des Pays-Bas. Complétée par une opération de communication à destination des utilisateurs de ces plates-formes, ce dispositif opérationnel a recherché une entrave pénale à l'encontre des principaux vendeurs, une entrave technique à l'égard des sites et un effet psychologique à l'égard d'utilisateurs du *darkweb*, désormais conscients de ne plus pouvoir préserver leur anonymat en ce lieu où ils se sentaient libre d'agir en toute impunité. A l'issue de cette opération, l'*US attorney general* Jeff Session avertira les trafiquants « *You cannot hide* ». Pour déployer une opération de telle ampleur, les autorités américaines et néerlandaises ont dû préalablement réaliser un travail de renseignement sur les objectifs (quelles plates-formes cibler ? comment en prendre le contrôle ? quels trafiquants neutraliser ?), avant de planifier une stratégie coordonnée qui sera mise en œuvre avec succès en recourant à modes d'action techniques et juridiques correctement planifiés.

En août 2019, en coordination avec le FBI, la gendarmerie nationale neutralise le *Botnet*[52] Retadup hébergé sur un serveur en Île-de-France. Réalisée sur renseignement, cette opération a permis la désinfection de 850.000 ordinateurs piratés. Cette entrave technique a permis d'atteindre une infrastructure de délinquance active depuis 2016 et qui était en mesure de contrôler et commander les machines à distance en vue de la commission de rançongiciels, de vols de données ou d'attaques DDOS.

En juillet 2020, la gendarmerie nationale annonce le démantèlement du réseau de *darkphones* Encrochat. Actif depuis 2015, ce réseau de communication

[50] Acronyme de *The Onion Router*, le réseau TOR est tout à la fois un réseau décentralisé et un navigateur, dont le fonctionnement garanti l'anonymat des utilisateurs. Il est l'un des *darknet* qui permet d'accéder au *darkweb*.

[51] Situées sur le *darkweb*, les *marketplaces* sont des sites commerciaux sur lesquels sont échangés des biens et services illégaux : drogue, armes, services illicites en ligne, numéro de carte de crédits volés, produits pharmaceutiques, fausse monnaie, *et cetera*. L'anonymat des échanges est compensé par des dispositifs destinés à garantir les transactions (*e.g.*, le système d'*escrow* instaurant un intermédiaire de paiement). Celles-ci sont opérées en crypto-actifs.

[52] Un *Botnet* est un réseau d'ordinateurs infectés, dont chacun peut être contrôlé à distance pour conduire des attaques de type DDOS, ou encore procéder à des envois de *spam*.

chiffré et sécurisé était essentiellement utilisé par des groupes criminels organisés de haut niveau, notamment en matière de trafic de stupéfiants. Détectant ce réseau en 2017, les gendarmes ouvrent une enquête devant la juridiction interrégionales spécialisée (JIRS) de Lille en 2018 et parviennent à comprendre le fonctionnement de ce réseau pour parvenir à intercepter les communications en temps réel à compter de 2019. Une équipe commune d'enquête franco-néerlandaise « Emma 95 / 26 Lemont » est créée dans le cadre d'Europol, en partenariat avec plusieurs forces de police à l'étranger. 120 millions de communications impliquant près de 60.000 utilisateurs sont ainsi exploitées en temps réel en vue d'opérations de saisies de stupéfiants (dont 100 tonnes de cocaïne), de saisies d'avoirs criminels (330 millions d'Euros), de la découverte de 19 laboratoires de drogues synthétiques et de lieux de détention et de torture mis en place par les groupes criminels. Plus de 200 projets d'assassinats sont ainsi déjoués et 5800 criminels arrêtés dont certains étant des cibles de haut niveau recherchées de longue date par les États. Ces résultats édifiant démontrent l'intérêt du travail en renseignement et de la détermination de filons d'élucidation permettant disposer de leviers d'efficacité contre la criminalité de masse transitant par les réseaux. L'exploitation de ces sources a également permis de comprendre l'envers du décors de la criminalité organisée et d'identifier des cibles de haut niveau (HVT, ou *high value targets*) animant depuis l'étranger (Dubaï notamment) les trafics en France. En 2021, une opération similaire est conduite par les autorités belges, néerlandaises et françaises sur le réseau chiffré Sky ECC. D'autres États renouvelleront cette expérience de lutte contre un phénomène à grande échelle en permettant aux forces de l'ordre de transformer une infrastructure utilisée par les délinquants en un moyen de lutte contre les groupes criminels.

Le réseau de téléphone chiffré ANOM représente une stratégie de déception autrement plus ambitieuse de la part des autorités américaines. Dans le cadre de l'opération *Trojan Shield*, le FBI et l'*Australian Federal police* (AFP) ont mis en place, de 2018 à 2021, un réseau de cryptophones qui a été utilisé par de nombreux groupes criminels. Déclenchée le 8 juin 2021, l'opération a permis l'interpellation simultanée de 800 individus dans 16 pays et la saisie de 40 tonnes de drogues.

Ces quelques exemples illustrent l'efficacité de stratégies d'entrave guidées par le renseignement. Elles renversent le paradigme judiciaire classique quant aux modalités de détection des affaires et de détermination des solutions de remédiation.

4. Conclusion

Cet article tente de situer la cybercriminalité en soulignant les spécificités de son écosystème technique et criminologique. Il indique que ce phénomène a pris le pas sur les autres formes de délinquance et constitue une priorité pour les force de l'ordre.

Qu'elle considère internet comme objet ou comme vecteur, cette délinquance de masse tend, en effet, à réduire à l'impuissance les processus classiques de réaction pénale consistant à constater les infractions pour ensuite les élucider par la révélation de leurs causes, en vue de poursuites et de réponses judiciaires.

Le renseignement criminel est capable de modifier cette posture réactive des forces de l'ordre. L'entrave pénale est alors mise en œuvre, non comme la volonté de réguler, par des actes de détail, un contentieux massif et difficile à élucider, mais comme une solution orientée et gagnante, cherchant

à atteindre avec précision le cœur des réseaux.

L'action judiciaire s'intègre alors comme composante d'un processus de savoir et se trouve combinée et coordonnée à un ensemble d'autres solutions. Sans renier l'enquête judiciaire, cette approche la remet dans une position d'efficacité dans le cadre de dispositifs à la fois imaginatifs et légaux.

Savoir guidant l'action, le renseignement devient alors le moyen d'aborder avec plus d'efficience la cybercriminalité dans cet environnement incertain et peu régulé qu'est le cyber espace. Conscient des risques d'un *Far-West*, terre de promesse comme de non-droit, où la cavalerie arrive toujours en retard, le renseignement criminel tente de réguler les effets de la création d'un *Far-Web* par une action résolue et proactive où il marque de son empreinte les immensités d'un territoire virtuel.

Bibliographie

1. Ablon L., Libicki M., Golay, A. A., *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar*, Rand Corporation, 2014
2. Barlatier J., « Criminal Investigation and Criminal Intelligence: Example of Adaptation in the Prevention and Repression of Cybercrime », *Risks*, vol. 8, n. 3, 2020b.
3. Barlatier J., « De L'enquête au Renseignement, Changement de Paradigme Pour la Victime » Paris: AJ Penal, 2020a, pp. 17-20.
4. Barlatier J., « De l'enquête scientifique à l'approche scientifique de l'enquête », *Médecine légale du vivant*, vol. 14, n. 1, 2020c, pp. 1-11.
5. Barlatier J., « L'enquête judiciaire est-elle une réponse appropriée à la cybercriminalité? », *Revue de la Gendarmerie Nationale*, 4ème Trimestre, 2019, pp. 159-62.
6. Barlatier J., *Management de l'enquête et ingénierie judiciaire, recherche relative à l'évaluation des processus d'investigation criminelle*, Thèse de Doctorat en Criminologie. Lausanne: UNIL/École des Sciences Criminelles, 2017.
7. Bitner E., *The Functions of the Police in Modern Society: Review of Background Factors, Current Practices and Possible Role Model*, Oelgeshlager, Gunn & Hain. Cambridge, 1970.
8. Bouchaud F., *Analyse forensique des écosystèmes intelligents communicants de l'internet des objets*, Thèse de doctorat en Informatique et applications, sous la direction de Gilles Grimaud et de Thomas Vantroys, soutenue en 2021 à l'Université de Lille.
9. Bouchez J.P., Les nouveaux travailleurs du savoir, Éditions d'organisation, Paris, 2004.
10. Bradford W.R., *Routine Activity Theory and Cybercrime, A Theoretical Appraisal and Literature Review. Technocrime and Criminological Theory*, Routledge, London/New York, 2017.
11. Brantingham P.L., Brantingham, P.J., « La concentration spatiale relative de la criminalité et son analyse : vers un renouvellement de la criminologie environnementale », *Criminologie*, vol. 27, n. 1, 1994, pp. 81-97.
12. Broadhurst R., Graborvsky P., Alazab M., Bouhours B., « An Analysis of the Nature of Groups engaged in Cyber Crime », *International Journal of Cyber Criminology*, vol. 8, n. 1, 2014, pp. 1-20.
13. Brun F., Cohen Y., Craciuneac C., Grépin F., Mouchès G., Wisson C., *L'apport du cyber dans les techniques d'investigation. Rapport de l'école de guerre économique*. Disponible en ligne le 31 juillet 2022 : https://www.ege.fr/infoguerre/lapport-du-cyber-dans-les-techniques-dinvestigation
14. Chaiken J.M., Greenwood P., Petersilia J., *The criminal Investigation Process. A Summary Report*, The Rand Paper Series. The Rand Corporation, Santa Monica, 1976.
15. Cliquennois G., Bellebna H., Léonard, T., « Management et système pénal: Présentation du dossier », *Droit et société*, vol. 90, n. 2, 2015, pp. 243-252.
16. Cohen L.E., Felson M., « Social change and crime rate trends: A routine activity approach » (1979), in Andresen M., Kinney

B.., *Classics in environmental criminology*, Routledge, London, 2010, pp. 203-232.
17. Crozier M., Friedberg E., *L'acteur et le système*, Seuil, Paris, 1977.
18. Douzet F., « La géopolitique pour comprendre le cyberespace", *Herodote*, vol. 1, n. 152-153, 2014, pp. 3-21.
19. Dregoir M., Klein E., *L'effet Iceberg et la Cybercriminalité*, Étude Service Central de Renseignement Criminel de la Gendarmerie Nationale, Centre de recherche de l'école des officiers de la gendarmerie nationale, Melun, 2017.
20. Dulaurans M., Fedherbes J-C., *Cyberharcelement et communautes en ligne: les resiliences organisationnelles en jeu! Un monde de crises au prisme des communications organisationnelles*, Universite Catholique de Louvain [UCL], Mons, Belgique, 2022, hal-03655311
21. Europol, *Internet Organized Crime Threat Assessment (IOCTA)*, disponible à l'adresse suivante : https://www.europol.europa.eu/iocta/2015/resources/iocta-2015.pdf
22. Felson M., Clarke R.V., *Opportunity Makes the Thief. Police Research Series, Paper 98*, Policing and Reducing Crime Unit, Research, Development and Statistics Directorate, London, 1998.
23. Foucault M., *Surveiller et punir. Naissance de la prison*, Gallimard, Paris, 1975.
24. Frampton L., *The Hunters and the Hunted: Exploring Practitioner and Public Attitudes Towards Paedophile Hunting Groups and the Implications for Risk Management*, Thèse Université de Portsmouth, 2021. Disponible à l'adresse suivante: https://pure.port.ac.uk/ws/portalfiles/portal/27089150/The_Hunters_and_The_Hunted._Exploring_Practitioner_and_Public_Attitudes_Towards_Paedophile_Hunting_Groups_and_the_Implications_for_Risk_Management.pdf (consulté le 4 décembre 2022).
25. Ghernaouti-Hélie S., *La cybercriminalité, le visible et l'invisible*, Presses polytechniques et universitaires romandes, Lausanne, 2009.
26. Goldstein H., *Problem-Oriented Policing*, Temple University Press, Philadelphie, 1990.
27. Hadjimatheou K., « Citizen-led digital policing and democratic norms: The case of self-styled paedophile hunters », *Criminology & Criminal Justice*, vol. 21, n. 4, 2021, pp. 547-565.
28. Harris L.H. (1977), *Response Time Analysis*, Missouri Police Department, Kansas City MO, 1977.
29. Jean J.P., *Le système pénal*, La Découverte, Paris, 2008.
30. Kalifa D., *Histoire des détectives privés*, Nouveau Monde edition, Paris, 2013.
31. Kemp S., « Fraud reporting in Catalonia in the Internet era: Determinants and motives », *European Journal of Criminology*, 2020, pp. 1-22.
32. Koops B-J., « The Internet and it's opportunities for cybercrime », *Tilburg Law School Legal Studies Research Paper Series*, vol. 1. n. 09, 2011, pp. 735-754.
33. Kuerbis B., Badeie F., Grindal K., Mueller M., « Understanding transnational cyber attribution: Moving from "whodunit" to who did it », in Cavelty M., Wenger A., *Cyber Security ans Politics, Socio-Technological Transformations and Political Fragmentation*, Routledge, Londres/New York, 2022.
34. Lalam N., « L'argent de la drogue en France », *Après-demain*, vol. 4, n. 44, 2017, pp. 46-48.
35. Lalam N., « Le trafic de drogue : un activité économique ancrée et adaptative », *Studia Diplomatica*, vol. 55, n. 5/6, Géopolitique et nouvelles criminalités internationales : actes du colloque des 13 et 14 décembre 2002 (Palais d'Egmont, Bruxelles) 2002, pp. 51-63.
36. Leukfeldt E. R., « Organised Cybercrime and Social Opportunity Structures: A Proposal for Future Research Directions », *The European Review of Organised Crime*, vol. 2, n. 2, 2015, pp. 91-103.
37. Leukfeldt E. R., Holt T., J., *The human factor of cybercrime*, Routledge, Londres, 2021.
38. Linde A, Aebi, M., « La criminologie comparee a l'heure de la societe numerique : Les theories traditionnelles

peuvent-elles expliquer les tendances de la cyber-delinquance ? », *Revue Internationale de Criminologie et de Police Technique et Scientifique*, vol. 4, n. 20, 2020.
39. Locard E., *Manuel de technique policière*, Payot, Paris, 1934.
40. Loveday B., « The Shape of Things to Come. Reflections on the potential implications of the 2016 Oce of National Statistics Crime Survey for the Police Service of England and Wales », *Policing: A Journal of Policy and Practice*, vol. 12, pp. 398–409.
41. Maillard de C., *Le renseignement criminel dans les forces de police françaises, une étude de l'absent et de l'existant au prisme du modèle de police guidée par le renseignement*, Thèse de doctorat en criminologie, sous la direction de Olivier Ribaux, soutenue en 2017 à l'école des sciences criminelles de l'université de Lausanne.
42. Margagliotti G., Borisova B., Ajil A., Rossy Q., *Mon canton, ma sécurité: sentiment de sécurité physique et numérique et opinions sur la police neuchâteloise*, Ecole des Sciences Criminelles, Lausanne, 2019.
43. Martinson R., (1974), « What works? Questions and answers about prison reform », *Public Interest*, vol. 35, 1974, pp. 22-54.
44. Petratos P. N., « Misinformation, disinformation, and fake news: Cyber risks to business », *Business Horizons*, vol. 64, n. 6, 2021, pp. 763-774.
45. Ratcliffe J., Intelligence-led Policing, Willan, Cullompton, 2016.
46. Rudesill D., S., Caverlee J., Sui D., *The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box*, Woodrow Wilson International Center for Scholars, STIP 03, October 2015, Ohio State Public Law Working Paper No. 314.
47. Skogan W. G., Hartnett S. M., *Community policing*, Chicago style, Chicago, 1977.
48. Théry G., *Les autoroutes de l'information*, Rapport au premier ministre, La documentation française, Paris, 1994.
49. Wagner T. D., Mahbub K., Palomar E., Abdallah A. E., « Cyber threat intelligence sharing: Survey and research directions », *Computers & Security*, vol. 87, 2019, 101589.
50. Wall D., *Cybercrime*, Polity press, Cambridge, 2007.
51. Wolfgand M. E., Figlio R., Sellin T., *Delinquency in a Birth Cohort*, University of Chicago Press, Chicago, 1972.
52. Yu S., *Human trafficking and the internet. Combating Human Trafficking: A multidisciplinary approach*, CRC Press, Boca Raton, 2015.

Textes juridiques

1. Code de procédure pénale (CPP).
2. Code de la sécurité intérieure (CSI).
3. Convention du Conseil de l'Europe relative à la cybercriminalité signé à Budapest le 23 novembre 2001. Série des traités européen n° 185.
4. Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, adopté le 17 novembre 2021. Disponible en ligne le 31 juillet 2022 : https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4c
5. Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique, dite « Godfrain », NOR : JUSX8700198L, JORF du 6 janvier 1988.