doi: 10.14664/rcvs/245

Cybercriminalità e pluralizzazione del policing: alcune riflessioni sulla cyber threat intelligence

Cybercriminalité et pluralisation du policing : la cyber threat intelligence en question

Cybercrime and pluralization of policing: questioning the cyber threat intelligence

Camille Guisset et Giorgia Macilotti***

Riassunto
Il presente contributo si pone l'obiettivo di analizzare il ruolo svolto dal settore privato nel contrasto alla cybercriminalità, con particolare riferimento all'emergere di nuove strategie fondate su modalità d'azione proattive finalizzate alla raccolta di informazioni. L'attenzione sarà focalizzata in particolare sulla *cyber threat intelligence* (CTI), un'espressione utilizzata per descrivere un processo *e* un risultato basati sulla raccolta, l'elaborazione e l'interpretazione di differenti tipi di dati con l'obiettivo di fornire conoscenze che consentano di valutare la natura e le caratteristiche delle «minacce» di natura informatica. Particolarmente sviluppata dagli attori privati della cybersicurezza, la CTI è uno strumento di supporto decisionale che solleva diversi interrogativi in merito alla sua definizione, alla metodologia utilizzata e alla portata dei risultati ottenuti.

Résumé
Cet article vise à interroger le rôle joué par le secteur privé dans la lutte contre la cybercriminalité, en se focalisant notamment sur l'émergence de nouvelles stratégies fondées sur des modes d'action proactifs visant à la collecte de renseignements. Une attention particulière sera accordée à la *cyber threat intelligence* (CTI), une expression utilisée pour décrire un processus *et* un produit résultant de la collecte, l'analyse et l'interprétation de différents types de données dans l'objectif de fournir des connaissances permettant d'évaluer la nature et les caractéristiques des « cybermenaces ». Particulièrement développée par les acteurs privés de la cybersécurité, la CTI est un outil d'aide à la décision qui soulève plusieurs questions quant à sa définition, à la méthodologie utilisée et à la portée des résultats obtenus.

Abstract
This article aims to examine the role played by the private sector in the policing of cybercrime, focusing particularly on the emergence of new strategies based on proactive methods designed for collecting intelligence.
Particular attention will be paid to cyber threat intelligence (CTI), an expression used to describe a process *and* a product resulting from the collection, the analysis and the interpretation of different types of data in order to provide knowledge for assessing the nature and characteristics of cyber threats. Particularly developed by private cybersecurity actors, the CTI is a decision support tool that raises several questions about its definition, its methodology and the relevance of the results obtained.

Key words : cybercriminalité, cybersécurité, *policing*, *cyber threat intelligence*, acteurs privés

* Diplômée du master 2 Relations Internationales et Politiques de Sécurité et de Défense (Université de Toulouse Capitole), analyste en *cyber threat intelligence* et consultante en gestion de crise.
** Enseignante-chercheuse en sociologie, membre de l'Institut de Cybersécurité de l'Occitanie, chercheuse associée à l'Institut du Droit de l'Espace, des Territoires, de la Culture et de la Communication (Université de Toulouse Capitole).

1. Introduction[1]

Internet, cyberespace, réseaux, objets connectés, intelligence artificielle, *blockchain* sont plus que jamais des termes incontournables pour penser quelques-unes des principales transformations sociales en cours. Puisant leurs origines dans une époque post-industrielle caractérisée par le passage à une économie de services immatériels et par des profonds changements dans les rapports et les rôles sociaux (Bell, 1973), Internet et les technologies numériques figurent parmi les principaux vecteurs des mutations sociales auxquelles nos sociétés sont confrontées depuis la fin du siècle dernier. Les potentiels fournis par la numérisation et l'échange rapide des données couplés à la restructuration globale du capitalisme, à la mondialisation et à la « logique de réseau » ont contribué au renouvellement des modèles sociaux, culturels et politico-économiques au centre desquels se trouvent l'échange et le traitement de l'information (Castells, 2001).

Toutefois, ces technologies porteuses de progrès génèrent aussi de nouvelles vulnérabilités qui peuvent être exploitées à des fins criminelles. Des attaques par rançongiciels[2] aux atteintes sexuelles envers les mineurs en passant par l'usurpation de l'identité numérique, les formes de délinquance tirant profit des opportunités offertes par le numérique ne cessent de se diversifier et se multiplier (Décary-Hétu, Bérubé, 2018 ; Yar, Steinmetz, 2019 ; Fortin, 2020). Malgré les limites méthodologiques et interprétatives des statistiques sur la cybercriminalité (Côté *et al.*, 2016 ; Macilotti, 2018a ; Dupont, 2021), les données élaborées par les acteurs publics de la sécurité identifient plusieurs tendances utiles pour comprendre l'évolution actuelle des criminalités numériques, en lien notamment avec les effets de la crise sanitaire (ralentissement des activités économiques, diffusion du télétravail, pénurie de certains biens de première nécessité, etc.). Selon l'*Internet Crime Complaint Center* du FBI (IC3, 2022), par exemple, les plaintes pour des faits de cybercriminalité ont presque triplé aux États-Unis entre 2017 et 2021 (respectivement 301 580 et 847 376 plaintes enregistrées). En France, en 2020, le nombre de signalements liés à des rançongiciels traités par l'Agence Nationale de la Sécurité des Systèmes d'Information a été multiplié par quatre par rapport à l'année 2019 (respectivement 191 et 54 faits constatés ; ANSSI, 2021), avec une progression observée également en 2021 (203 signalements traités ; ANSSI, 2022). L'augmentation des cyberattaques ciblant des infrastructures critiques et basées, entre autres[3], sur l'utilisation de rançongiciels a été soulignée également par la police italienne des communications[4], avec 5 434 épisodes traités en 2021 (*Polizia Postale e delle Comunicazioni*, 2022) contre 507 en 2020 et 239 en 2019 (*Polizia Postale e delle Comunicazioni*, 2021).

[1] Bien que l'article soit le fruit d'une réflexion commune des auteures, il faut attribuer plus spécifiquement les sections 1, 2, 4 et 5 à Giorgia Macilotti et les sections 3.1, 3.2 et 3.3 à Camille Guisset.

[2] Selon l'agence nationale française en charge de la cybersécurité (ANSSI), une attaque par rançongiciel (en anglais *ransomware)* « consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement », https://www.ssi.gouv.fr/entreprise/principales-menaces/cybercriminalite/rancongiciel/

[3] Parmi les attaques contre les infrastructures critiques constatées par la *Polizia Postale e delle Comunicazioni* (2021 et 2022), on retrouve celles basées sur l'utilisation de rançongiciels, mais aussi celles liées à d'autres modes opératoires comme les attaques par déni de service, les accès frauduleux à un système informatique, les campagnes de phishing ou de type APT (*Advanced Persistent Threats*).

[4] Une réorganisation des services de cybersécurité et de lutte contre la cybercriminalité est actuellement en cours en Italie. Pour plus d'informations, voir l'article de Maurizio Tonellotto présenté dans ce même numéro de la revue.

Qu'il s'agisse de l'augmentation exponentielle des infractions *constatées*[5] par les services de police, de la professionnalisation des groupes criminels, de l'émergence de formes de cybercriminalité constituant des « menaces » graves pour les infrastructures essentielles des États et la sécurité nationale, il ne fait aucun doute que la délinquance numérique représente aujourd'hui « l'un des défis les plus complexes auxquels se heurtent les organisations policières » (Dupont, 2021, p. 55) et, de manière plus générale, les systèmes de contrôle social. Si depuis la fin des années 1990 les pouvoirs publics européens et nord-américains ont adopté plusieurs réformes visant à améliorer la prise en charge des phénomènes de cybercriminalité (introduction de nouvelles infractions, création d'unités de police spécialisées dans l'investigation numérique, mise en place de nouvelles stratégies d'enquête, etc.) (Jewkes, Yar, 2008 ; Bryant, Bryant, 2014 ; Macilotti, 2018b ; Yar, Steinmetz, 2019 ; Dupont, 2021), nombre de travaux soulignent à quel point la réponse publique en la matière s'avère encore particulièrement complexe. La sophistication croissante des conduites criminelles bénéficiant des évolutions rapides du monde numérique, les problèmes relatifs à l'augmentation exponentielle du volume des données à traiter, les difficultés des organisations et des « cultures » policières à s'adapter aux défis posés par l'environnement numérique, les problèmes de coopération internationale en matière judiciaire, sont autant d'aspects illustrant les problématiques auxquelles sont confrontés les professionnels des institutions pénales (Wall, 2007 ; Jewkes, 2012 ; Wall, Williams, 2014 ; Goodison *et al.*, 2015 ; Vincze, 2016 ; Holt *et al.*, 2015 ; Macilotti, 2018b ; Dupont, 2021 ; De Paoli *et al.*, 2021).

Il en ressort ainsi que l'évolution des criminalités numériques et les difficultés liées à la prévention et répression de ces phénomènes rendent urgente une réflexion approfondie non seulement sur la place et l'action des forces de police (voir, par exemple, Dupont, 2021), mais aussi sur l'émergence de modes de régulation faisant intervenir un ensemble plus diversifié d'intervenants (publics, privés, hybrides, voire citoyens). C'est ce que rappelait déjà en 2008 Michèle Alliot Marie, ancienne ministre française de l'Intérieur, à l'occasion d'une allocution portant sur l'amélioration des réponses aux criminalités numériques : « la lutte contre la cybercriminalité fait partie d'une chaîne, comme toute action en matière de sécurité. La police et la gendarmerie en sont des acteurs essentiels, mais ils ne sont pas les seuls »[6].

La prévention et la répression de la délinquance numérique renvoient en effet à un large éventail d'intervenants et de mécanismes de régulation, parmi lesquels un rôle non négligeable est joué par les acteurs privés de la sécurité (Wall, 2007 ; Dupont, 2016 ; Yar, Steinmetz, 2019). À partir de l'analyse de la littérature grise et des études les plus récentes sur le sujet, cet article propose alors de s'intéresser plus spécifiquement aux formes de contrôle social émanant de ce secteur, en se focalisant notamment sur les modes d'action « proactifs » visant à la collecte d'informations et à la production de renseignements. Pour ce faire, nous aborderons dans un premier temps le mouvement de pluralisation du *policing*, une notion

[5] Il n'est jamais inutile de rappeler que les statistiques produites par les services publics, que ce soit au niveau du ministère de la Justice ou de l'Intérieur, ne doivent pas être considérées comme des outils permettant de fournir une image exhaustive de l'état général de la délinquance. Elles sont avant tout les chiffres de l'activité policière ou judiciaire : une photographie à un moment donné de leurs actions en la matière (voir, notamment, Robert, Zauberman, 2011).

[6] http://www.interieur.gouv.fr/fr/Archives/Archives-de-Michele-Alliot-Marie-2007-2009/Interventions/14.02.2008-Lutte-contre-la-cybercriminalite

qui s'avère particulièrement utile pour illustrer les changements à l'œuvre dans le champ des réactions aux phénomènes de cybercriminalité (2). L'attention sera ensuite focalisée sur une méthode d'analyse de l'information, dénommée *cyber threat intelligence* (CTI), qui vise à fournir des connaissances permettant de mieux évaluer la nature et les caractéristiques des faits de cybercriminalité (3). Bien qu'elle ne soit pas limitée au secteur privé, la CTI figure parmi les principales solutions de sécurité proposées par les entreprises de cybersécurité et de services numériques. Cet outil d'aide à la décision soulève toutefois plusieurs interrogations quant à sa définition, à ses approches méthodologiques et à la portée des résultats obtenus (4).

2. La cybercriminalité et les manifestations d'un *policing* pluralisé

2.1 À propos de la pluralisation du *policing*

Le fait que différents types d'acteurs participent à la régulation des comportements déviants et délinquants ne constitue pas une nouveauté. Comme le soulignait déjà Robert Castel à la fin des années 1980, circonscrire « les régulations normativantes des comportements à l'action de l'appareil d'État » montre toutes ses limites, d'autant plus que « les formes les plus modernes de contrôle [fonctionnent] sur un mode capillaire en économisant le plus souvent la coercition directe » (1988, p. 74). L'émergence et la consolidation d'un secteur marchandisé de la sécurité (Ocqueteau, Warfman, 2011), la mobilisation de « pacificateurs indigènes » dans les quartiers populaires paupérisés (Boucher, 2015), l'émergence de services de sécurité mi-publics mi-privés dans les transports publics et dans le secteur de l'habitat social (Malochet, 2022), constituent quelques exemples du mouvement de « multilatéralisation » (Bayley, Shearing, 2001) ou de « pluralisation » du *policing* (Jones, Newburn, 1998 ; Crawford, 2008).

Globalement prise, la notion de *policing* « se réfère aux *activités*[7] qui sont déployées pour assurer la régulation sociale et à l'application des lois pénales » (Brodeur, 1995, p. 127), elle se rapporte « à toutes les activités de surveillance et de sécurisation visant à garantir la protection des personnes, des biens, et le respect des lois » (Malochet, 2022, p. 2). Le terme « pluralisation », quant à lui, a été utilisé par les spécialistes des organisations policières pour rendre compte de certaines évolutions majeures du champ du *policing*, à savoir le rôle progressivement plus important des acteurs non-policiers, et notamment de la sécurité privée (Shearing, Stenning, 1983), ainsi que la variété des organismes publics, privés et bénévoles mobilisés dans la régulation des phénomènes déviants et délinquants (Wakefield, Fleming, 2009). Ainsi définie, la pluralisation du *policing* désigne un processus caractérisé « par un partage accru de la fonction policière (…), une diversification des parties prenantes, ainsi qu'une restructuration des rapports entre le niveau central et le niveau local, la sphère publique et le secteur privé » (Malochet, 2017, p. 2). Ce « nouveau *policing* » (McLaughlin, 2007) mobilise un ensemble très diversifié d'intervenants qui présentent une grande variété de statuts, d'identités et d'« habitus » professionnels (Macilotti, Boucher, 2022).

Ce processus est particulièrement évident quand on interroge les réponses à la cybercriminalité, une notion désignant de manière générale[8] « toutes les infractions pénales tentées ou commises à

[7] Italique de l'auteur.

[8] La notion de cybercriminalité fait l'objet de plusieurs débats dans la littérature (voir notamment Bergeron *et al.*, 2020). Dans un souci de synthèse, nous employons ce terme selon la définition « pédagogique » proposée par le Groupe de travail interministériel français sur la lutte contre la cybercriminalité (Robert, 2014).

l'encontre ou au moyen d'un système d'information et de communication » (Robert, 2014, p. 12). C'est ce que rappellent notamment David Wall (1998, 2007), Yvonne Jewkes (2012), Majid Yar (2019) et Benoît Dupont (2016) lorsqu'ils montrent que la prise en charge des criminalités numériques n'est plus l'apanage exclusif des organisations policières, si tant est qu'elle l'ait jamais été. À l'instar des problèmes concernant « l'espace physique », la prévention et la répression des faits de cybercriminalité impliquent un large éventail d'acteurs qui, à différents niveaux et selon différentes modalités, interviennent dans la tentative de régulation du cyberespace.

Nous pouvons rappeler, par exemple, les initiatives citoyennes comme les *netizen* groupes ou les *cyber angels* dont l'objectif est d'améliorer la sensibilisation et la prévention en matière de criminalités numériques à travers l'implication directe des internautes[9] (voir, par exemple, Wall, 1998). Il s'agit de communautés ou plateformes en ligne, plus ou moins structurées, qui mettent à disposition différents types de contenus (guides, vidéos, *serious games*, …) portant sur les principales formes de cybercriminalité et les bons réflexes à adopter, tout en proposant des outils pour signaler des comportements illicites et pour échanger alertes, conseils et bonnes pratiques entre les usagers. La participation citoyenne à la lutte contre la cybercriminalité peut glisser parfois vers des actions revêtant un caractère punitif, comme dans le cas du vigilantisme numérique (Yar, Steinmetz, 2019). Cette pratique consiste « non seulement [à] alerter les autorités ou l'opinion publique, mais également [à] "se faire justice soi-même" en engageant des formes actives de surveillance, de répression ou de dissuasion ciblées » (Loveluck, 2016, p. 128). Le vigilantisme en ligne peut prendre différentes formes allant des groupes d'internautes qui s'organisent pour aider les forces de police à résoudre une enquête (Huey *et al.*, 2012) jusqu'aux communautés numériques qui se spécialisent dans l'identification de certains types de délinquants, comme les auteurs d'escroqueries en ligne ou d'abus sexuels à l'égard des mineurs (Yar, Steinmetz, 2019).

D'autres réponses aux criminalités numériques ont vu le jour grâce à la mobilisation d'organisations sans but lucratif en partenariat avec les acteurs du Net et les pouvoirs publics. Au Royaume-Uni, par exemple, un organisme nommé *Internet Watch Foundation* (IWT)[10] a été créé en 1996 afin d'améliorer la veille sur Internet et le retrait des contenus illicites. Il s'agit d'une organisation caritative établie par l'industrie du numérique en partenariat avec le gouvernement britannique dont l'objectif est de surveiller les échanges et les communications en ligne, tout en facilitant le signalement des faits de cybercriminalité par le biais d'une *hotline* spécifique. En France, l'Association des Prestataires de l'Internet (AFPI) a créé en 1998 la plateforme Point de Contact qui, outre à fournir des informations en matière de prévention et bonne hygiène numérique, propose un service en ligne permettant à tout internaute de notifier un contenu potentiellement illicite rencontré lors de sa navigation[11]. Des plateformes similaires ont été mises en place dans d'autres pays et peuvent être coordonnées par des organismes comme l'Internet Hotline Providers in Europe[12] (INHOPE), une organisation qui réunit une cinquantaine de *hotlines* et vise à fournir un soutien pour simplifier les procédures de notification des contenus illicites en ligne (Macilotti, 2020).

[9] https://www.cyberangels.org/

[10] https://www.iwf.org.uk/

[11] http://www.pointdecontact.net/

[12] https://www.inhope.org/EN

Au-delà des initiatives relatives à ces plateformes de signalement, les entreprises du numérique et le secteur des activités privées de sécurité jouent un rôle important dans d'autres domaines de la lutte contre la cybercriminalité. Ces acteurs peuvent collaborer directement avec les forces de police en fournissant, par exemple, des logiciels permettant d'améliorer l'analyse des données informatiques, le traitement des dossiers d'enquête ou la détection des contenus illégaux (Macilotti, 2018b). Cependant, leur contribution se concrétise en particulier à travers le développement d'une offre de biens et de services dédiés à la sécurité numérique et à la protection des données. Cela se traduit non seulement par la création de départements en charge de la sécurité des systèmes d'information au sein des entreprises, mais surtout par l'émergence de sociétés de services spécialisées en cybersécurité (Bradshaw, 2017 ; Yar, Steinmetz, 2019 ; Button, 2020), ainsi que par l'implication des industriels historiques de la défense dans la mise à disposition de solutions de sécurité pour un panel plus large de clients (D'Elia, 2015).

La régulation des faits de cybercriminalité a été également impulsée par l'action de plusieurs organisations internationales. Le Conseil de l'Europe, par exemple, a adopté le premier traité multilatéral sur le sujet : la Convention sur la Cybercriminalité (et ses protocoles) signée à Budapest le 23 novembre 2001[13]. L'ONU, quant à elle, non seulement a voté plusieurs résolutions en matière de cybersécurité, mais elle a établi des groupes d'experts gouvernementaux (GGE) chargés d'examiner les risques qui se posent ou pourraient se poser dans le cyberspace et les éventuelles mesures de coopération pour y faire face[14]. S'agissant de l'Union Européenne, un certain nombre de mesures ont été adoptées afin d'améliorer la lutte contre la cybercriminalité et la promotion d'un Internet de confiance. Cela passe également par la création de structures *ad hoc*, comme par exemple l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA)[15], pour renforcer la réponse communautaire en matière de cybersécurité et la coopération entre les États membres de l'UE.

Bien qu'elle se décline différemment en fonction des pays, des contextes et des périodes considérés, cette pluralisation des réponses à la cybercriminalité s'explique en raison de plusieurs facteurs.

Outre les difficultés précédemment évoquées relatives à la réponse policière, une autre raison tient à l'histoire et au développement d'Internet[16]. Depuis sa création, son fonctionnement dépend de l'intervention d'une grande variété d'acteurs et, par conséquent, sa régulation est tributaire d'une pluralité d'initiatives. Bien que des mesures législatives aient été introduites par les pouvoirs publics, elles ne constituent en effet qu'une partie des règles qui encadrent le fonctionnement du « réseau des réseaux » et les usages numériques. Les formes d'autorégulation proposées par certaines

[13] ETS 185, Convention sur la Cybercriminalité, 23 novembre 2001, disponible à l'adresse suivante : https://rm.coe.int/168008156d

[14] https://www.un.org/disarmament/fr/informatique-et-telematique/

[15] https://www.enisa.europa.eu/media/enisa-en-francais

[16] La naissance et le développement d'Internet sont le résultat de l'intervention de plusieurs acteurs : le champ de la *défense étatsunienne* qui, à la fin des années 1950, soutient le création du premier réseau d'ordinateurs interconnectés à distance (ARPANET) dans le but d'assurer les communications en cas d'attaque nucléaire ; la *communauté scientifique* américaine qui collabore avec le monde militaire pour le développement de ce premier réseau ; le milieu de la *contre-culture* des années 1960-1970 dans lequel évoluent les concepteurs d'Internet et les communautés d'informaticiens ; la tradition du *service public européen* qui a largement influencé les concepteurs du World Wide Web ; les *acteurs privés* du numérique qui ont participé au développement de la structure actuelle d'Internet grâce notamment aux solutions introduites pour la recherche et le référencement des contenus et à la création des plateformes de réseautage (Curran, 2012 ; Lallement, 2015 ; Boullier, 2016).

communautés afin de préserver les valeurs fondatrices d'Internet (libre circulation de l'information, transparence, refus de toute forme de censure et d'« interférence » étatique, etc.), les standards, les spécifications et les référentiels introduits par des organismes techniques comme l'ICANN[17], l'ISO[18] et l'IEFT[19], les codes de conduite imposés par les principales plateformes numériques, en constituent d'autres exemples (Freyssinet, 2012 ; Yar, Steinmetz, 2019).

Pour comprendre cette dynamique, il faut également l'inscrire dans le mouvement plus général de pluralisation du *policing*. À cet égard, plusieurs facteurs sont conjointement mis en avant par la littérature : les changements profonds liés à la diffusion de la « culture du contrôle » (Garland, 2001) et du « risque » (Beck, 2001), l'inflation des préoccupations sécuritaires, la remise en question de l'efficacité de l'État dans la traitement de la délinquance, la crise de légitimité des organisations policières (Malochet, 2017 ; O'Neill, Fyfe, 2017), l'émergence de nouvelles échelles d'action (au niveau local, européen, international, transnational), le contexte de crise des finances publiques, l'échec des politiques interventionnistes de l'État-providence (Lascoumes, Le Galès, 2012), les mouvements de décentralisation et de privatisation caractérisant l'action de l'État dans un vaste ensemble de domaines (Dieu, 2016).

2.2 La cybercriminalité et le secteur des activités privées de sécurité

Dans ce panorama de réponses à la cybercriminalité, un rôle non négligeable est joué par le secteur des activités privées de sécurité, notamment pour ce qui concerne l'offre de *cybersécurité*.

Si la notion de cybercriminalité renvoie aux infractions pénales commises à *l'encontre* ou au *moyen* d'un système d'information (Robert, 2014), celle de cybersécurité désigne, de manière générale[20], l'ensemble des technologies, des processus et des mesures visant à protéger les données numériques et à préserver les infrastructures servant à stocker et à transmettre ces données (voir, par exemple, ANSSI[21] ; Centre Canadien pour la Cybersécurité, 2022). En suivant cette perspective, la sécurité numérique peut être alors pensée comme l'une des activités participant à la régulation de la cybercriminalité.

Bien que le champ de la cybersécurité mobilise un large éventail d'intervenants à la fois publics et privés (Nye, 2014 ; Dupont, 2016 ; Bradshaw, 2017 ; Yar, Steinmetz, 2019), l'offre de biens et services proposés par les entreprises spécialisées dans la sécurité numérique s'avère actuellement très importante, notamment en raison du chiffre d'affaires qu'elle génère (Yar, Steinmetz, 2019 ; Button, 2020). Assurer l'intégrité, la confidentialité et le bon fonctionnement des systèmes d'information et des données, contrôler l'accès aux systèmes informatiques, protéger le contenu des données contre la manipulation, le vol et la divulgation non autorisée, accompagner les organisations dans les processus de transformation numérique, sont autant d'exemples illustrant les besoins adressés par l'offre commerciale des sociétés de cybersécurité. Cela passe par le développement d'une large gamme de solutions, telles que la conception et la fourniture de logiciels de différente nature (contrôle des accès, antivirus,

[17] *Internet Corporation for Assigned Names and Numbers*.
[18] Organisation internationale de normalisation.
[19] *Internet Engineering Task Force*.

[20] À l'instar de la notion de cybercriminalité, la conceptualisation du terme cybersécurité soulève encore plusieurs débats dans la littérature (voir, par exemple, Dupont, Whelan, 2021).
[21] Glossaire de l'ANSSI disponible à l'adresse suivante : https://www.ssi.gouv.fr/entreprise/glossaire/c/

protection des données, chiffrement des contenus et des transactions sensibles, etc.), l'élaboration de stratégies de cybersécurité et d'architectures sécurisées, la mise en conformité avec la réglementation et les référentiels de sécurité, la gestion des crise, la réponse à incident, sans oublier les activités de sensibilisation sur les criminalités numériques à destination des organisations et de leurs employés (Grabosky, Smith, 2001; Nugent, Raisinghani, 2002 ; Yar, Steinmetz, 2019).

Parmi les multiples services proposés, l'analyse des formes de cybercriminalité *considérées* comme des *menaces* à la cybersécurité constitue un domaine de plus en plus investi par ces acteurs privés, avec un chiffre d'affaires au niveau mondial qui devrait passer de 5,3 milliards de dollars en 2018 à 12,9 milliards en 2023 (Oosthoek, Doerr, 2021). L'activité porte en particulier sur l'analyse des caractéristiques et des évolutions des « cybermenaces », c'est-à-dire des conduites visant « à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité d'un système ou de l'information qu'il contient» (Centre Canadien pour la Cybersécurité, 2022, p. 2).

Puisant ses origines dans le domaine militaire et le champ du renseignement, la notion de cybermenace mérite toutefois quelques précisions car sa définition ne s'impose pas d'elle-même[22]. Plusieurs approches théoriques allant de l'interactionnisme symbolique (Becker, 1966) à la théorie sur la sécuritisation (Buzan *et al.*, 1997) en passant par la sociologie de l'action publique (Lascoumes, Le Galès, 2012 ; Neveau, 2015) montrent à quel point la définition d'une situation comme étant problématique ou menaçante ne va pas de soi, mais procède d'un travail collectif basé sur des activités concurrentielles de qualification et de mise en récit (Borraz, 2008 ; Milet, 2022).

Ainsi, la notion de cybermenace sera ici utilisée selon la signification générale qui lui est attribuée par la doctrine de sécurité française. D'après cette perspective, nous rappelle Jean-Paul Brodeur (2006), « il faut distinguer les risques qui ne sont pas le fruit d'une intention humaine – les risques naturels et matériels – et les risques, auxquels on réserve le terme de "menace", qui sont le produit d'une intention humaine malveillante » (p. 491). Selon cette approche, la notion de cybermenace renvoie donc aux risques numériques résultant d'une intention humaine malveillante et englobe notamment les actes d'espionnage (étatique ou industriel), de déstabilisation, de sabotage, ainsi que les formes de cybercriminalité susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des systèmes d'information[23]. Plusieurs travaux ont en effet souligné à quel point le panorama des menaces associées aux usages numériques a évolué au cours des quinze dernières années, le cyberespace étant tantôt utilisé à des fins d'influence et de confrontations géopolitiques, tantôt à des fins lucratives ou même de revendications sociales et politiques (pour une synthèse, Taillat *et al.*, 2018 ; Yar, Steinmetz, 2019).

C'est précisément dans ce contexte que s'inscrit le développement de nouvelles stratégies visant à améliorer la détection et le traitement des criminalités numériques à travers la mise en œuvre de modes d'action proactifs orientés vers la collecte d'informations (Wagner *et al.*, 2019 ; Basheer, Alkhab, 2021). Le référence est en particulier à la

[22] Pour une analyse plus approfondie, voir l'ouvrage de Marc Milet (2022) ; pour un approfondissement sur la notion de menace dans le contexte de la cybercriminalité et de la cybersécurité, voir l'article de Benoit Dupont et Chad Whelan (2021).

[23] Il s'agit notamment de la perspective adoptée par l'agence nationale française en charge de la cybersécurité (ANSSI) : https://www.ssi.gouv.fr/entreprise/principales-menaces/

cyber threat intelligence (CTI), une expression utilisée pour décrire à la fois un processus *et* un produit résultant de la collecte, de l'analyse et de l'interprétation de différents types de données dans l'objectif de fournir des connaissances permettant d'évaluer la nature et les caractéristiques des cybermenaces.

3. Répondre aux défis posés par la cybercriminalité : quel rôle pour la *cyber threat intelligence* ?[24]

3.1 Qu'est-ce que la *cyber threat intelligence* ?

Depuis une dizaine d'années, la *cyber threat intelligence* fait partie non seulement des stratégies d'action adoptées par les acteurs de la sécurité publique[25], mais aussi des solutions de sécurité proposées par le secteur privé. La CTI, aussi appelée « renseignement d'intérêt cyber »[26], tente d'appréhender les contours des différentes cybermenaces en les étudiant de manière globale afin de permettre une compréhension holistique du contexte dans lequel se déroule une cyberattaque donnée. Ainsi, elle peut être pensée comme une « discipline » permettant de collecter, capitaliser, contextualiser, exploiter et diffuser le renseignement relatif aux cybermenaces.

De manière générale, la *cyber threat intelligence* peut être définie comme un outil d'aide à la décision basé sur des techniques empruntées au champ du renseignement et dont l'objectif est de fournir une évaluation de la nature et des caractéristiques des menaces numériques (émergentes ou existantes). Il s'agit d'un « système d'information qui fournit des connaissances factuelles sur les cybermenaces » (Basheer, Alkhatib, 2021, p. 1) à partir d'un ensemble d'activités « de recueil, d'étude et de partage d'informations liées à des attaques informatiques » (ANSSI, en ligne)[27]. Les connaissances ainsi produites permettent de mieux comprendre les caractéristiques des cyberattaques et des modes opératoires adoptés par les auteurs, tout en fournissant des informations utiles pour la définition des mesures de sécurité les plus appropriées pour prévenir les cyberattaques et pour faire face à leurs conséquences (Friedman, Bouchard, 2015 ; Wagner *et al.*, 2019 ; Basheer, Alkhatib, 2021).

Bien que sa méthode s'inspire à des approches analytiques ayant déjà montré leur efficacité, la *cyber threat intelligence* se trouve finalement être une discipline complexe, faisant appel à des champs de compétences variées et nécessitant de faire l'objet d'une stratégie prédéfinie afin de servir son principal objectif : « disposer d'une évaluation précise et permanente de la menace cyber » (Germain, Massart, 2017, p. 57). Cette évaluation doit elle-même servir un but précis, étant celui de fournir des analyses de risques basées sur la menace étudiée et permettant de prendre des décisions face à celle-ci (Moinet, 2019). La dimension de la *finalité* est en effet au cœur de la majorité des approches développées sur le sujet. La CTI n'est jamais une fin en soi, elle ne vise pas le savoir pour le savoir : c'est

[24] Outre que par les résultats des études sur le sujet, cette partie est nourrie également par l'expérience professionnelle d'une des auteures en tant qu'analyste en *cyber threat intelligence*.

[25] En France, par exemple, un rôle fondamental en matière de CTI est joué par l'ANSSI, l'agence nationale en charge de la cybersécurité. Cet organisme publie régulièrement des rapports sur l'actualité des cybermenaces, des bulletins présentant les nouvelles vulnérabilités détectées, ainsi que des travaux de synthèse. Voir par exemple : https://www.ssi.gouv.fr/entreprise/principales-menaces/analyse-de-la-menace/

[26] Il importe toutefois de préciser que la définition du mot renseignement diffère quelque peu par rapport à celle du mot *intelligence*. Ce dernier « s'emploie dans des domaines variés comme l'économie, le commerce, l'enquête policière, etc., puisqu'il s'entend dans un sens plus étendu d'information et de système d'information ». La définition du terme renseignement est plus restreinte et renvoie généralement à la dimension « gouvernementale » ou « politique », à l'activité des services de l'État spécialisés dans la surveillance et la collecte d'informations (Chopin, Oudet, 2016, pp. 39-40).

[27] https://www.ssi.gouv.fr/entreprise/principales-menaces/analyse-de-la-menace/

une méthode d'analyse produisant une information utile à quelqu'un qui l'a demandée dans une perspective précise. Il s'agit d'un outil d'aide à la décision qui met en avant « des connaissances qualifiées et adaptées à de multiples destinataires souhaitant protéger des systèmes numériques : le niveau stratégique oriente les décideurs, le niveau opérationnel (TTPs) aide à la priorisation des projets de sécurisation alors que le niveau technique (IOCs) alimente les outils de détection et de recherche de compromission » (ANSSI, en ligne)[28].

3.2 La démarche d'analyse

Cet objectif de connaissance fine des cybermenaces se décline tout d'abord en fonction de la temporalité d'une cyberattaque :

- en amont d'une cyberattaque afin d'*anticiper* la menace cyber. La CTI est mobilisée dans l'objectif de développer des connaissances sur les outils technologiques et le type de menaces en « temps de paix » ;
- au cours d'une cyberattaque afin de *détecter* la conduite illicite et y *répondre*. La CTI est alors utilisée pour mieux identifier et catégoriser la menace ainsi que sa criticité en « temps de guerre » ;
- en aval d'une cyberattaque afin de *remédier* à l'attaque subie. La CTI est sollicitée dans l'objectif de définir les modalités pour rétablir les fonctionnalités des systèmes d'information et assurer le retour au « temps de paix ».

Ainsi, pour pouvoir être pleinement utilisée à chacune de ces temporalités, la *cyber threat intelligence* doit être pensée « en temps de paix », c'est-à-dire quand les efforts ne sont pas dirigés vers la réponse immédiate à une cyberattaque donnée. La construction de renseignement doit même être envisagée comme une stratégie sur le long-terme, passant par la création de savoir-faire et réflexes des analystes CTI (Moinet, 2019).

Cette construction, initialement réfléchie par de nombreux acteurs de la communauté cyber comme une tâche principalement technique, est aujourd'hui de plus en plus appréhendée de manière globale (Taillat *et al.*, 2018) et tend à progressivement impliquer de nouvelles disciplines. Effectivement, l'obtention d'*intelligence* pérenne et viable nécessite :

1) d'être pensée sur le long-terme par des personnes issues de formations managériales et capables de mettre en place une stratégie de collecte, exploitation et diffusion du renseignement pertinente ;
2) de faire appel à des personnes issues du monde de l'ingénierie informatique capables d'identifier et analyser les données techniques relevées sur la menace ;
3) de remettre en contexte les données techniques par des personnes issues de formations fonctionnelles telles que les études de sécurité ou les relations internationales afin d'analyser les données liées à la menace numérique en fonction du cadre dans lequel celle-ci évolue (contexte politique et géopolitique, économique et démographique, historique, social et culturel).

La conjonction de chacun de ces pans de compétences permet alors d'obtenir une évaluation fine de la menace numérique, celle-ci se basant sur un cadre d'étude complet, sollicitant l'ensemble du contexte dans lequel un évènement cyber se produit.

[28] https://www.ssi.gouv.fr/entreprise/principales-menaces/analyse-de-la-menace/

La mise en place de cette stratégie d'analyse n'est généralement pas arbitraire, mais elle s'appuie sur les éléments constitutifs d'une cyberattaque afin de cartographier l'ensemble de ce contexte. Dans cette perspective, la communauté internationale de *cyber threat intelligence* fait généralement appel à trois sources d'informations majeures : 1) celles relatives aux groupes d'attaquants, 2) celles portant sur les modes opératoires et 3) celles concernant les outils et les infrastructures d'attaques (voir, par exemple, Friedman, Bouchard, 2015).

Les *groupes d'attaquants* sont généralement classés en différentes catégories en fonction des intentions qui les animent, de leurs capacités techniques ainsi que des impacts potentiels générés par leurs attaques. La CTI cherche à caractériser le degré de sophistication et ainsi le risque que représente le groupe en lui-même. S'agissant des *modes opératoires*, l'attention est focalisée sur les stratégies adoptées par les acteurs et sur l'existence de modèles d'action récurrents, chaque groupe d'attaquants développant un schéma opératoire précis, rarement modifié au regard des habitudes que ces derniers établissent. Parmi les techniques les plus utilisées, nous pouvons rappeler la mise en place de mécanismes de persistance ou d'évasion sur le système victime ou encore l'exploitation de vulnérabilités techniques ou humaines plus ou moins rodées. L'analyse de la manière dont les acteurs organisent, exécutent et gèrent les cyberattaques est résumée par l'expression « Tactiques, Techniques et Procédures » (TTPs)[29], un terme développé par la communauté de CTI pour indiquer les « modèles d'activités et les méthodes associés à un acteur ou à un groupe d'acteurs spécifiques de la menace »[30] (Friedman, Bouchard, 2015, p. 62). L'examen de ces informations permet aux analystes de contextualiser la cyberattaque et d'appréhender le niveau de réflexion apporté à son séquencement. Enfin, l'attention est focalisée sur les *outils* et les *infrastructures d'attaques*, chaque groupe d'acteurs reposant sur un arsenal numérique plus ou moins sophistiqué et intelligemment utilisé pour mener chaque étape de leurs attaques. Généralement, ces groupes s'appuient sur des logiciels malveillants programmés pour exécuter des actions prédéfinies à chaque phase de l'attaque. Ils s'appuient également sur des infrastructures numériques, physiques ou non, afin de communiquer avec l'environnement ciblé. La CTI vient ici identifier le fonctionnement technique de ces outils et infrastructures ainsi que leur niveau de complexité.

À partir de l'analyse de ces éléments, qui par ailleurs ne relèvent pas toujours nécessairement de la sphère numérique, la CTI contribue à approfondir les connaissances sur les formes de cybercriminalité touchant les organisations tant publiques que privées. Pour ce faire, elle fait appel à une méthodologie bien connue par les services publics de sécurité et également reprise par le secteur privé : le cycle du renseignement. En effet, la *cyber threat intelligence* est plus que la simple collecte d'informations : elle couvre un panel d'activités liées entre elles.

Classiquement adopté par les institutions publiques pour mener leurs activités d'*intelligence* sur toute menace à la Nation, le cycle du renseignement consiste à réaliser en continu, et selon des besoins bien définis, des étapes permettant *in fine* de transformer une donnée en information stratégique

[29] Les TTPs sont modélisées au sein de la Matrice Mitre ATT&CK, qui correspond à une classification de l'ensemble des techniques et tactiques d'attaques utilisées par des opérateurs malveillants et dont l'enchevêtrement permet de générer des modes opératoires d'attaques associés à des groupes d'attaquants précis. Pour plus d'informations, voir https://attack.mitre.org

[30] Notre traduction : « Patterns of activities and methods associated with specific threat actors or groups of threat actors ».

(Chopin, Oudet, 2016 ; Moinet, 2019). Nous parlons alors de renseignement actionnable, c'est-à-dire d'une information dont l'analyse permet de prendre des décisions quant à la prévention ou réaction à un évènement. En effet, « le renseignement repose (...) sur l'idée que les germes de l'action future se trouvent dans la connaissance du présent et du passé » (Roubelat, 2019, p. 7).

Appliqué à la CTI, le cycle du renseignement répond au même objectif en l'adaptant à la menace évoluant au sein du cyberespace (Pech, 2019). Il s'agit donc d'étayer la connaissance disponible sur les cybermenaces afin de mieux anticiper, détecter, répondre et remédier aux actions de celles-ci. Pour se faire, les analystes CTI reposent sur les étapes classiques du cycle du renseignement, à savoir l'orientation, le recueil, le traitement, l'analyse et la dissémination[31].

L'*orientation* se matérialise par une expression de besoin d'informations, techniques ou de contexte, sur une menace donnée. Cette orientation peut évoluer à tout moment et nécessiter une adaptation des recherches effectuées (Moinet, 2019). L'étape du *recueil*, quant à elle, se base sur des activités de veille, menées au moyen de recherches ainsi que de recueil d'informations pertinentes et fiables. Cette opération est généralement effectuée par de la veille active (réalisée par l'analyste lui-même) et passive (s'appuyant sur des flux d'informations intégrés automatiquement au sein de plateformes de CTI) sur la cybermenace. Ces informations peuvent provenir de sources publiques, disponibles pour l'ensemble des utilisateurs de l'Internet en clair, comme de sources privées reposant sur la mise en place de partenariats privilégiés avec des éditeurs de cybersécurité (Pech, 2019). Dans la phase du *traitement*, il s'agit tout d'abord de capitaliser l'information recueillie au sein des plateformes de CTI d'agrégation et de management des données (Tounsi, 2019), puis de la contextualiser, notamment par la mise en perspective de celle-ci avec une multitude de facteurs techniques, opérationnels et stratégiques entourant la cybermenace. L'étape de l'*analyse* renvoie au « double processus de déstructuration (analyse) et de création (synthèse) » (Moinet, 2019, p. 17). En effet, le renseignement obtenu au moyen de l'exploitation de l'information nécessite une étude critique, partiale et stratégique, permettant *in fine* de le rendre actionnable et donc exploitable lors de la prise de décision finale, en prévention ou en réaction à une menace pesant sur les systèmes d'information. Cette étape, essentielle, permet d'évaluer les risques qu'une conduite donnée représente ainsi que ses potentiels impacts. La dernière phase, celle de la *dissémination* du renseignement, est pensée et adaptée au destinataire de celui-ci, le renseignement diffusé pouvant porter tant sur les outils techniques que sur les méthodes utilisées ou même encore sur les cibles et les impacts des faits étudiés.

Si ces étapes sont présentées ici de manière linéaire, il est à noter qu'il « s'agit bien d'un cycle puisque les renseignements ainsi obtenus permettent de réorienter les besoins et d'en découvrir de nouveaux » (Moinet, 2019, p. 14) et que tout renseignement diffusé est pensé selon l'auditoire final, la CTI se nivelant en différents versants tout aussi importants dans l'anticipation, la détection et la réaction aux menaces numériques.

[31] D'autres termes peuvent être utilisés pour indiquer les étapes du cycle du renseignement. Par exemple, le Pentagone emploie l'expression « diffusion et intégration » au lieu de « dissémination » et ajoute l'étape de l'« évaluation et feedback »; le FBI ajoute après la « dissémination » l'étape de la « demande » (voir Chopin, Oudet, 2016).

3.3 Les niveaux d'analyse

L'analyse des menaces et des incidents informatiques permet de fournir des connaissances qualifiées et adaptées à de multiples destinataires souhaitant protéger leurs systèmes d'information. Dans cette perspective, la communauté internationale de la *cyber threat intelligence* identifie trois niveaux d'analyse en fonction du public et des résultats ciblés (Abu *et al.*, 2018 ; Basheer, Alkhatib, 2021 ; Oosthoek, Doerr, 2021).

La CTI dite *stratégique* vise à orienter les décideurs. Ce premier niveau repose sur un renseignement dit de « haut niveau » et a pour but « d'aider les stratèges à comprendre les risques actuels et à identifier d'autres risques dont ils ne sont pas encore conscients » (Tounsi, 2019, p. 13). Ainsi, la CTI stratégique s'adresse principalement au personnel exécutif afin de lui fournir un panorama global sur la menace et l'orienter dans la prise de décisions opérationnelles, la gestion des ressources et des stratégies organisationnelles. Pour ce faire, elle fournit des informations concernant les groupes d'attaquants, leurs motivations, les secteurs d'activités et les zones géographiques ciblés ainsi que les impacts des opérations réalisées.

La CTI dite *opérationnelle* aide à la priorisation des projets de sécurisation. Ce second niveau, d'ores et déjà plus technique, s'attache à identifier « la manière dont les acteurs de la menace mènent leurs attaques » (Tounsi, 2019, p. 13). Elle s'appuie ainsi sur la compréhension des modes opératoires (TTPs), des logiciels malveillants et de la temporalité dans la réalisation technique de l'attaque. La CTI opérationnelle s'adresse aux dirigeants des équipes de protection afin d'orienter au mieux les stratégies de sécurité et de remédiation.

Enfin, la CTI dite *tactique* vient en appui à la détection des cyberattaques et permet de contextualiser les évènements de sécurité au moyen d'indicateurs techniques (IoCs - Indicateurs de Compromission) associés à des attaquants ou à des logiciels malveillants connus. Ce niveau de CTI intéresse généralement les analystes de détection de la menace et de réponse à incident. Prisée par la communauté cyber, la CTI tactique « est immédiatement exploitable et est plus facilement quantifiable par rapport aux autres sous-catégories de CTI » (Tounsi, 2019, p. 4).

Ces différents niveaux de CTI traduisent ainsi un besoin en renseignement de diverse nature, tantôt stratégique, méthodologique ou technique.

4. Enjeux et défis de la *cyber threat intelligence*

La *cyber threat intelligence* constitue un champ d'expertise particulièrement prometteur en raison des opportunités qu'elle offre pour le développement de solutions permettant d'améliorer la protection des systèmes d'information et la lutte contre la cybercriminalité (Wagner *et al.*, 2019 ; Basheer, Alkhatib, 2021 ; Paliotta, 2022). Au fil des années, des « communautés de pratiques » (Wenger, 1998) se sont aussi constituées autour du partage d'alertes, d'informations, de données techniques et de modèles d'analyse. Bien que selon des modalités et des temporalités différentes en fonction des contextes et des secteurs considerés, le « renseignement d'intérêt cyber » s'inscrit dans un réseau de collaborations et de configurations hybrides où interviennent des organismes publics de sécurité, des chercheurs indépendants, des analystes du secteur marchandisé de la sécurité et des entreprises de cybersécurité (Wagner *et al.*, 2019). Toutefois, un examen de la littérature et des travaux produits par la communauté elle-même permet de souligner plusieurs aspects problématiques

concernant tant les approches développées, que la portée des résultats obtenus (voir aussi Abu *et al.*, 2018 ; Basheer, Alkhatib, 2021 ; Oosthoek, Doerr, 2021).

Un premier élément concerne la notion de *cyber threat intelligence* dont la définition peut varier parfois de façon significative. Ce terme peut être en effet utilisé tantôt pour désigner le *processus* permettant d'obtenir des connaissances sur les cybermenaces, tantôt pour indiquer le *résultat* d'un tel processus d'analyse ; ou bien, il peut être mobilisé pour décrire les deux. Selon l'agence nationale française en charge de la cybersécurité, par exemple, l'« analyse de la menace, ou Cyber Threat Intelligence (CTI), implique *l'ensemble des activités*[32] de recueil, d'étude et de partage d'informations liées à des attaques informatiques » (ANSSI, en ligne)[33]. Kurt Baker, au contraire, utilise cette notion pour indiquer « les *données*[34] collectées, traitées et analysées afin de comprendre les motivations, les cibles et les stratégies de l'auteur de la menace » (2022, en ligne)[35]. Robert Lee, quant à lui, définit la CTI comme « le *processus* et le *produit*[36] résultant de la transformation des données brutes en informations répondant à une exigence spécifique, [c'est-à-dire] concernant des adversaires ayant l'intention, l'occasion et la capacité de nuire » (2016, en ligne)[37].

La CTI est donc une expression qui présente au moins deux acceptions : une acception intellectuelle (une connaissance, un savoir), une autre processuelle (l'ensemble des activités réalisées). Cela n'est pas sans rappeler les travaux sur la notion de renseignement, bien que dans ce cas il y ait également une acception institutionnelle liée à l'organisation produisant ce type de connaissances (les services de renseignement) (Chopin, Oudet, 2016).

Les approches peuvent également varier en fonction de la manière d'opérationnaliser la notion de CTI. D'après la société Gartner, par exemple, la *threat intelligence* renvoie aux « connaissances fondées sur des données probantes, y compris le contexte, les mécanismes, les indicateurs, les implications et les conseils actionnables, au sujet d'une menace existante ou émergente (…) qui peuvent être utilisées pour éclairer les décisions concernant la réponse du sujet à cette menace ou à ce danger » (McMillan, 2013, en ligne)[38]. Si cette définition met l'accent sur le type de données utilisées pour produire les connaissances, l'approche proposée par l'une des guide les plus citées en la matière insiste plutôt sur les motivations et les stratégies mises en œuvre par les acteurs malveillants : « la cyber threat intelligence est la connaissance des adversaires et de leurs motivations, intentions et méthodes qui est recueillie, analysée et diffusée afin d'aider le personnel de sécurité et les employés à tous les niveaux à protéger les actifs essentiels de l'entreprise »[39] (Friedman, Bouchard, 2015, p. 6).

[32] Notre italique.
[33] https://www.ssi.gouv.fr/entreprise/principales-menaces/analyse-de-la-menace/
[34] Notre italique.
[35] Notre traduction : « Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors », https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
[36] Notre italique.
[37] Notre traduction : « The process and product resulting from the interpretation of raw data into information that meets a requirement as it relates to the adversaries that have the intent, opportunity and capability to do harm », https://www.robertmlee.org/intelligence-defined-and-its-impact-on-cyber-threat-intelligence/
[38] Notre traduction : « Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard », https://www.gartner.com/en/documents/2487216
[39] Notre traduction : « Cyber threat intelligence is knowledge about adversaries and their motivations, intentions, and methods that is collected, analyzed, and disseminated in ways that help security and business staff at all levels protect the critical assets of the enterprise ».

Le cadre méthodologique du « renseignement d'intérêt cyber » constitue un autre domaine qui mérite d'être interrogé. Dans cette perspective, un premier aspect à aborder concerne les données utilisées dans le cadre des activités de CTI. Celles-ci sont en effet alimentées par des sources de nature variée allant des processus de détection interne aux entreprises jusqu'aux services proposés par les éditeurs de cybersécurité, en passant par les informations diffusées par les organismes publics ou partagées librement au sein des communautés de CTI (pour une synthèse Wagner *et al.*, 2019).

Cette richesse d'informations entraîne toutefois une augmentation croissante du volume de données qui nécessitent d'être traitées, contextualisées et interprétées (Friedman, Bouchard, 2015 ; Abu *et al.*, 2018 ; Oosthoek, Doerr, 2021). Cela demande une mobilisation de ressources et de compétences qui ne sont pas toujours à la portée des équipes techniques. C'est ce que révèle, par exemple, une enquête par questionnaire réalisée auprès d'un échantillon de près de 1000 professionnels du secteur de la cybersécurité : 56% des répondants déclarent que les données à traiter dans le cadre d'une stratégie de CTI sont trop volumineuses ou complexes pour pouvoir fournir des renseignements exploitables (Institut Ponemon, 2021).

Si le volume des données à analyser soulève plusieurs problèmes, l'absence et le retard de partage des contenus s'avèrent également problématiques. À cet égard, certains travaux montrent que les informations diffusées au sein de la communauté de CTI offrent des renseignements dont la valeur est parfois difficile à estimer, les données pouvant être incomplètes ou publiées des mois après la détection de la cyberattaque ou de la vulnérabilité informatique (Oosthoek, Doerr, 2021). Selon Samantha Bradshaw (2017), par exemple, l'émergence du secteur marchandisé de la cybersécurité contribue à expliquer ces aspects, la vente de certains types d'informations étant particulièrement rentable (ex. failles *zero-day*). De plus, nombre d'organisations hésitent à partager les données relatives aux faits dont elles ont été victimes en raison des dommages potentiels à leur réputation, la cyberattaque pouvant dévoiler une vulnérabilité technique ou de sécurité (Macilotti, 2019). Il ne faut pas non plus oublier que dans le cadre de la *cyber threat intelligence* sont mobilisées des données dont le partage n'est pas toujours autorisé ou est juridiquement encadré[40].

L'utilisation de données de faible qualité est un autre aspect mis en avant par les travaux sur le sujet. D'après l'étude réalisée par l'Institut Ponemon (2021), par exemple, 60% des personnes interviewées considèrent que les données dont ils disposent dans le cadre des analyses ne permettent pas d'obtenir des informations ayant valeur stratégique. Cela s'explique aussi en raison des pratiques de certains éditeurs consistant à présenter des éléments techniques, tels que les adresses IP, les noms domaine, les *hash* des fichiers, comme des renseignements. Or, la connaissance sur l'état de la menace n'est pas une information qui existe déjà à « l'état brut » : elle est toujours le résultat d'un processus délibéré de collecte, d'analyse, de contextualisation et d'interprétation d'un ensemble de données.

Un dernier aspect à souligner concerne les modèles développés par les acteurs et les plateformes de CTI pour définir et caractériser les menaces numériques. Si d'une part ces approches ont contribué à faire évoluer les méthodes d'analyse, de l'autre le manque

[40] Nous pensons, par exemple, au Règlement général sur la protection des données (RGPD, règlement UE 2016/679 du Parlement européen et du Conseil du 27 avril 2016) qui encadre le traitement des données personnelles sur le territoire de l'Union européenne.

de standardisation dû à l'utilisation de plusieurs modèles peut empêcher le partage des informations et l'efficacité des analyses réalisées (Abu *et al.*, 2018 ; Oosthoek, Doerr, 2021).

5. Pour conclure

Qu'il s'agisse des communautés d'internautes, des fournisseurs de services numériques, des organisations internationales, des acteurs de la sécurité privée ou du milieu associatif, la prise en charge des criminalités numériques mobilise un large éventail d'intervenants, tout en impliquant un changement d'échelle dans la mise à l'agenda et la structuration des réponses adoptées. Cette dynamique vient ainsi non seulement démentir l'hypothèse d'un déficit de régulation en matière de cybercriminalité (souvent évoqué à propos du « Far West numérique »), mais témoigne d'une nouvelle « architecture du *policing* globalisé » basée sur des assemblages hybrides de sécurité et des configurations collaboratives assez originales (Dupont, 2016, p. 96).

Un exemple à cet égard est offert par l'analyse de la littérature grise et scientifique sur la *cyber threat intelligence*. Inspirés par les approches développées par les services gouvernementaux de renseignement, les travaux sur « l'état de la menace cyber » ont contribué à l'émergence de communautés de pratiques composées d'éditeurs de solutions de cybersécurité, d'analystes du secteur marchandisé de la sécurité, de chercheurs indépendants ainsi que d'acteurs de la sécurité publique. Dans ce contexte, la CTI a contribué à une meilleure compréhension des criminalités numériques, en permettant notamment « de structurer des modélisations assez complètes des modes opératoires utilisés par les attaquants » (Salamon, 2020, p. 1615).

Toutefois, la revue des travaux sur le sujet montre à quel point le champ de la *cyber threat intelligence* est encore « dans son enfance » (Oosthoek, Doerr, 2021 p. 303). Tout d'abord, il n'existe pas de définition communément admise de la notion de CTI, les acteurs tendant à la définir en fonction de leur domaine d'expertise et de leur environnement de travail (voir aussi Abu *et al.*, 2018). De plus, plusieurs problèmes d'ordre méthodologique émergent lorsque l'on interroge les approches développées en la matière. C'est ainsi que certains auteurs affirment que « la CTI est un produit sans processus » (Oosthoek, Doerr, 2021 p. 302), en référence notamment aux problèmes liés à la nature des données utilisées, aux conceptualisations de qualité variable et à l'absence de standardisation.

Malgré ces difficultés, le « renseignement d'intérêt cyber » est un domaine émergent qui présente un potentiel significatif pour la protection des systèmes d'information et les réponses, tant publiques que privées, à la cybercriminalité. C'est notamment ce que souligne l'étude de l'Institut Ponemon (2021) précédemment citée : 79% des professionnels interviewés affirment que la CTI est « essentielle pour obtenir une posture de cybersécurité solide » (p. 1). Il s'agit d'une perspective partagée également par plusieurs organismes de sécurité numérique, tels que l'ENISA[41] au niveau européen ou l'ANSSI en France, qui sont par ailleurs particulièrement mobilisés dans la mise en œuvre de solutions[42] visant à mieux structurer les informations relatives aux cybermenaces et à répondre aux principaux problèmes méthodologiques existants.

[41] Depuis plus de 10 ans, l'ENISA est un acteur central dans l'évaluation des cybermenaces et des activités de CTI : https://www.enisa.europa.eu/topics/cyber-threats

[42] Nous rappelons, par exemple, le projet OpenCTI (Open Cyber Threat Intelligence) développé par l'ANSSI en partenariat avec le CERT-EU : https://www.ssi.gouv.fr/actualite/opencti-la-solution-libre-pour-traiter-et-partager-la-connaissance-de-la-cybermenace/

Références

1. Abu S., Selamat S. R., Ariffin A., Robiah Yusof R., « Cyber Threat Intelligence – Issue and Challenges », *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 10, n. 1, 2018, pp. 371-379.
2. Basheer R., Alkhatib B., « Threats from the Dark: A Review over Dark Web Investigation Research for Cyber Threat Intelligence », *Journal of Computer Networks and Communications*, ID 1302999, 2021, pp. 1-21.
3. Bayley D., Shearing C., *The New Structure of Policing*, National Institute of Justice, Washington, 2001.
4. Beck U., *La société du risque*, Aubier, Paris, 2001.
5. Becker H., *Social Problems: A Modern Approach*. New York: John Wyler, New York, 1966.
6. Bell D. (1976), *The coming of the post-industrial society: a venture in social forecasting*, Basic Books, New York, 1976.
7. Bergeron A., Pamar M., Paquette S., « Introduction et définitions de la cybercriminalité », in Fortin F., *Cybercrimes et enjeux technologiques*, Presses internationales Polytechnique, Montréal, 2020, pp. 1-20.
8. Borraz O., *Les politiques du risque*, Presses de Sciences Po, Paris, 2008
9. Boucher M., *Sociologie des turbulences. Penser les désordres des inégalités*, Paris, L'Harmattan, 2015.
10. Boullier D., *Sociologie du numérique*, Armand Colin, Paris, 2016.
11. Bradshaw S., « Combatting cyber threats: CSIRTS and fostering international cooperation on cyber security », in Global Commission on Internet Governance, *Cybersecrutiy in a volatile world*, Centre for International Governance Innovation, 2017, disponible à l'adresse : https://www.jstor.org/stable/resrep05239.13
12. Brodeur J.-P., « Le contrôle social : privatisation et technocratie », in *Déviance et Société*, vol. 19, n. 2, 1995, pp. 127-147.
13. Brodeur J.-P., « Le risque et la menace », *Canadian Journal of Criminology and Criminal Justice*, vol. 48, n. 3, 2006, pp. 491-498.
14. Brun P., Denécé É., *Renseignement et espionnage pendant l'Antiquité et le Moyen-Âge*, Ellipses, Paris, 2019.
15. Burrus G., Howell C. J., Bossler A., Holt T., « Self-perceptions of English and Welsh constables and sergeants preparedness for online crime: a latent class analysis », *Policing: An International Journal*, vol. 43, n. 1, 2019, pp. 105-119.
16. Button M. « The "New" Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions », *Journal of Contemporary Criminal Justice*, vol. 36, n. 1, 2020, pp. 39-55.
17. Buzan B., Weaver O., De Wilde J., *Security : A New Framework for Analysis,* Lynne Rienner Publishers, London, 1997.
18. Castel R., « De l'intégration sociale a l'éclatement du social : l'émergence, l'apogée et le départ à la retraite du contrôle social », in *International Review of Community Development / Revue Internationale d'Action Communautaire*, n. 20, 1988, pp. 67-78.
19. Castells M, *La société en réseaux*, Fayard, Paris, 2001(1ère édition originale 1996).
20. Chopin O., Oudet B., *Renseignement et sécurité*, Armand Colin, Paris, 2016.
21. Côté A. M., Bérubé M., Dupont B., « Statistiques et menaces numériques. Comment les organisations de sécurité quantifient la cybercriminalité », *Réseaux*, vol. 3., n. 197-198, 2016 p. 203-224.
22. Crawford A., « The pattern of policing in the UK: policing beyond the police », Newburn T. *The handbook of policing*, Willan, Cullompton, 2008, pp. 147-182.
23. Curran J., « Reinterpreting Internet history », in Jewkes Y., Yar M. (ed.), *Handbook of Internet crime*, Willan, Cullompton, 2012, pp. 17-37.
24. D'Elia D., « La cybersécurité : de la représentation d'un bien public à la nécessité d'une offre souveraine », *Sécurité et stratégie*, vol. 19, n. 2, 2015, pp. 72-80.
25. De Paoli S., Johnstone J., Coull N., Ferguson I., Sinclair G., Tomkins P., Brown M., Martin R., « A Qualitative

Exploratory Study of the Knowledge, Forensic, and Legal Challenges from the Perspective of Police Cybercrime Specialists », *Policing: A Journal of Policy and Practice*, vol. 15, n. 2, 2021, pp. 1429-1445.
26. Décary-Hétu D., Bérubé M. (dir.), *Délinquance et innovation*, Presses de l'Université de Montréal, Montréal, 2018.
27. Dieu F., *Réponses à la délinquance*, L'Harmattan, Paris, 2016.
28. Dupont B., « La gouvernance polycentrique du cybercrime : les réseaux fragmentés de la coopération internationale », in *Cultures & Conflits*, n. 102, 2016, p. 95-120.
29. Dupont B., « La police et la prévention de la cybercriminalité », in Amicelle A., Boivin R., Dupont B., Fortin F., Tanner S., *L'avenir du travail* policier, Les Presses de l'Université de Montréal – Édition Kindle, Montréal, 2021, pp. 50-93.
30. Dupont B., Whelan C., « Enhancing relationships between criminology and cybersecurity », *Journal of Criminology*, vol. 54, n. 1, 2021, pp. 1-17.
31. Fortin F. (dir.), *Cybercrimes et enjeux technologiques*, Presses internationales Polytechnique, Montréal, 2020.
32. Freyssinet E., *La cybercriminalité en mouvement*, Hermes, Paris, 2012.
33. Friedman J., Bouchard M., *Definitive guide to cyber threat intelligence*, CyberEdge, Annapolis, 2015.
34. Garland D., *The Culture of Control*, Oxford University Press, Oxford, 2001.
35. Germain G., Massart P., « Souveraineté Numérique », *Études*, vol. 10, n. 10, 2017, pp. 45-58
36. Gill P., Phythian M., *Intelligence in an Insecure World*, Polity Press, Malden, 2012.
37. Goodison S., Davis R., Jackson B., *Digital Evidence and the U.S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*, RAND Corporation, Santa Monica, 2015.
38. Grabosky P., Smith R., « Telecommunication fraud in the digital age: The convergence of technologies », in Wall D. S. (dir.), *Crime and the Internet*, Routledge, London, 2001, pp. 29-43.
39. Holt T., Burruss G., Bossler A., *Policing Cybercrime and Cyberterror*, Carolina Academic Press, Durham, 2015.
40. Huey L., Nhan J., Broll R., « 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime », *Criminology & Criminal Justice*, vol. 13 n. 1, 2012, p. 81-97.
41. Jewkes Y., Yar M., « Policing cybercrime: emerging trends and future challenges », in Newburn T., *Handbook of policing*, Willan, Cullompton, 2008, pp. 580-605.
42. Jewkes, Y., « Public policing and internet crime », in Jewkes Y., Yar M. (dir.), *Handbook of Internet Crime*, Routledge, Oxon, 2012, pp. 525-545.
43. Jones T., Newburn, T., *Private security and public policing*, Clarendon Press, Oxford, 1998.
44. Lallement M., *L'Âge du faire. Hacking, travail, anarchie*, Seuil, Paris, 2015.
45. Lascoumes P., Le Galès P., *Sociologie de l'action publique*, Armand Colin, Paris, 2012.
46. Levi M., Doig A., Gundur R., Wall D., Williams M., *The Implications of Economic Cybercrime for Policing*, City of London Police, London, 2015.
47. Loveluck B., « Le vigilantisme numérique, entre dénonciation et sanction. Auto-justice en ligne et agencements de la visibilité », *Politix*, vol. 115, n. 3, 2016, pp. 127-153.
48. Macilotti G., « Studiare la cybercriminalità: alcune riflessioni metodologiche », *Rivista di Criminologia, Vittimologia e Sicurezza*, vol. 12, n. 1, 2018a, pp. 51-80.
49. Macilotti G., *Pedopornografia e tecnologie dell'informazione. Devianza e controllo sociale nella realtà italiana e francese*, FrancoAngeli, Milano, 2018b.
50. Macilotti G., « Cybercriminalità », in Balloni A., Bisi R., Sette R. (dir.), *Criminologia applicata. Criminalità, controllo, sicurezza*, Wolters Kluwer-Cedam, Milano, 2019, pp. 311-350.
51. Macilotti G., « Online Child Pornography: Conceptual Issues and Law Enforcement Challenges », in Balloni A., Sette R. (dir.), *Handbook of Research on Trends and Issues in Crime Prevention, Rehabilitation, and Victim*

Support, IGI Global, Hershey, PA, 2020, pp. 226-247.
52. Macilotti G., Boucher M., dossier *Les professionnels de la déviance et de la délinquance : quels enjeux d'hybridation ? Pratiques des acteurs, lieux d'intervention et logiques professionnelles*, *Sciences & Actions Sociales*, vol. 16, n. 1, 2022, pp. 1-14.
53. Malochet V., « Contours et positionnement d'une forme hybride de policing résidentiel », in *Champ pénal/Penal field* [En ligne], vol. 14, 2017, pp. 1-2.
54. Malochet V., « La pluralisation du policing en France. Logiques d'hybridation, effets de tropisme et enjeux d'articulation », *Sciences & Actions Sociales*, vol. 16, n. 1, 2022, pp. 53-67.
55. McLaughlin E., *The new policing*, Sage, London, 2007.
56. Milet M., *Sociologie politique de la menace et du risque*, Armand Colin – Édition Kindle, Paris, 2022.
57. Moinet N., « Le renseignement au prisme du couple agilité-paralysie », *Prospective et stratégie*, vol. 10, n. 1, 2019, pp. 13-27.
58. Neveu E., *Sociologie politique des problèmes publics*, Armand Colin, Paris, 2015.
59. Nugent J., Raisinghani M., « The information technology and telecommunications security imperative: Important issues and drivers », *Journal of Electronic Commerce Research*, vol. 3, n. 1, 2002, pp. 1-14.
60. Nye J., *The Regime Complex for Managing Global Cyber Activities*, Global Commission on Internet Governance, Paper Series No. 1., Waterloo, 2014.
61. O'Neill M., Fyfe N. R., « Plural policing in Europe: relationships and governance in contemporary security systems », *Policing and Society*, v. 27, n. 1, 2017, pp. 1-5.
62. Ocqueteau F., Warfman D. (2011), *La sécurité privée en France*, Paris, Puf, 2011.
63. Oosthoek K., Doerr C. (2021), « Cyber Threat Intelligence: A Product Without a Process? », *International Journal of Intelligence and CounterIntelligence*, vol. 34, n. 2, 2021, pp. 300-315.
64. Paliotta A. P., « Una riflessione preliminare sul processo di Istituzionalizzazione della Cyber Intelligence », *Quaderni di Cyber Intelligence*, vol. 1, 2022, pp. 10-20.
65. Pech Y., « Vers une intelligence cyber ? Penser le renseignement augmenté dans la noosphère », *Prospective et stratégie*, vol. 10, n. 1, 2019, pp. 73-102.
66. Ponemon Institute, *The State of Threat Feed Effectiveness in the United States and United Kingdom*, Ponemon Institute Research Report, 2021.
67. Robert M., *Rapport sur la cybercriminalité*, Groupe de travail interministériel sur la lutte contre la cybercriminalité, 2014.
68. Robert P., Zauberman R., *Mesurer la délinquance*, Presses de Sciences-Po, Paris, 2011.
69. Roubelat F., « Anticipation et renseignement », *Prospective et stratégie*, vol. 10, n. 1, 2019, pp. 7-11.
70. Salamon Y., *Cybersécurité et cyberdéfense : enjeux stratégiques*, Ellipses – Édition Kindle, Paris, 2020.
71. Shearing C. D., Stennin P. C., « Private security: Implications for social control », *Social Problems*, vol. 30, n. 5, 1983, pp.493–506.
72. Taillat S., Cattaruzza A., Danet D., *La cyberdéfense. Politique de l'espace numérique*, Armand Colin, Paris, 2018.
73. Tounsi W., *Cybervigilance et confiance numérique: la cybersécurité à l'ère du Cloud et des objets connectés*, ISTE, Paris, 2019.
74. Vincze E. A., « Challenges in digital forensics », *Police Practice and Research*, vol. 17, n. 2, 2016, pp. 183-194.
75. Wagner D., Mahbub K., Palomar E., Abdallah A. E., « Cyber threat intelligence sharing: Survey and research directions », Computers & Security, vol. 87, 2019, 101589.
76. Wakefield A., Fleming J., *The SAGE Dictionary of Policing*, Sage, London, 2009.
77. Wall D. S (dir.), *Crime and the Internet*, Routledge, New York, 2001.
78. Wall D. S., « Catching Cybercriminals: Policing the Internet », *International Review of Law Compurters & Technology*, vol. 12, n. 2, 1998, pp. 201-218.
79. Wall D. S., « Policing cybercrimes: situating the public police in networks of security

within cyberspace », *Police Practice and Research: An International Journal*, vol. 8, n. 2, 2007, pp. 183-205.
80. Wenger E., *Communities of Practice: Learning, Meaning, and Identity*, Cambridge University Press, Cambridge, 1998.
81. Yar M., Steinmetz K. F., *Cybercrime and Society*, Sage – Kindle Edition, London, 2019.

Sitographie

1. ANSSI, *État de la menace rançongiciel à l'encontre des entreprises et des institution*s, 2021, disponible à l'adresse suivante : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf
2. ANSSI, *Panorama de la menace informatique 2021*, 2022, disponible à l'adresse suivante : https://www.cert.ssi.gouv.fr/uploads/20220309_NP_WHITE_ANSSI_panorama-menace-ANSSI.pdf
3. Baker K., *What is cyber threat intelligence ?*, disponible à l'adresse suivante : https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/
4. Centre Canadien pour la Cybersécurité, *Introduction à l'environnement de cybermenace*, Centre de la sécurité des télécommunications, Ottawa, 2022, disponible à l'adresse suivante : https://cyber.gc.ca/fr/orientation/introduction-lenvironnement-de-cybermenaces
5. IC3, *Federal Bureau of Investigation Internet crime report 2021*, 2022, disponible à l'adresse suivante : https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
6. Lee R. M., *Intelligence Defined and its Impact on Cyber Threat Intelligence*, disponible à l'adresse suivante : https://www.robertmlee.org/intelligence-defined-and-its-impact-on-cyber-threat-intelligence/
7. Polizia Postale e delle Comunicazioni, *Resoconto attività - Polizia Postale e delle Comunicazioni Anno 2020*, 2021, disponible à l'adresse suivante : https://questure.poliziadistato.it/statics/29/5.01.2021--allegato-al-consuntivo-2020--attivita-polizia-postale.pdf?lang=it
8. Polizia Postale e delle Comunicazioni, *Resoconto attività - Polizia Postale e delle Comunicazioni Anno 2021*, 2022, disponible à l'adresse suivante : https://questure.poliziadistato.it/statics/46/resoconto-attivita-polposta-2021-e-calabria.pdf?lang=it