L'IMPACT DU NUMÉRIQUE DANS L'ENQUÊTE

La société est en plein bouleversement de par la prolifération et la massification des technologies de l'information et le développement des services numériques. Cette révolution s'accompagne d'une numérisation croissante de nos modes de vie et de nos interactions. Véritable phénomène culturel et sociétal, créateur de valeurs et de données, elle constitue un enjeu de changement et de transformation pour les métiers et les pratiques de l'investigation judiciaire. Le numérique est générateur d'opportunités inédites, ainsi que de nouvelles menaces. Face à ce nouveau paradigme, l'Institution doit s'inscrire dans une posture d'adaptation constante et d'innovations majeures. Cet article s'intéresse à l'impact du numérique et du phénomène de digitalisation de la société pour l'enquête judiciaire, notamment les adaptations résultant de l'évolution de la criminalité au cyberespace.

L'espace numérique : nouvelles opportunités d'investigation

Le développement des services supportés par le numérique et des écosystèmes connectés a conduit à une profonde évolution des modes de vies. En effet, le numérique se superpose et interagit avec le monde physique en intégrant une multitude d'interfaces, de capteurs et d'actionneurs, tandis que les utilisateurs développent par leurs activités quotidiennes une identité et une empreinte numériques. La limite entre le virtuel et le réel est en passe d'être abolie. Elle s'inscrit dans une logique de continuum cyberespace-espace physique (Hazane, 2018). En conséquence, l'enquête judiciaire ne se limite plus à une approche territoriale de son traitement, car l'enquêteur doit adopter une posture réflexive transverse intégrant pleinement les traces numériques, et donc, potentiellement, des ramifications nationales ou internationales.

FRANÇOIS BOUCHAUD

Capitaine de gendarmerie, dirige le Département coordination opérationnelle cyber (DCOC) du C3N

PASCAL MARTIN

Lieutenant, dirige le Groupe des relations internationales (GRI) du DCOC

La démocratisation de l'emploi des réseaux sociaux constitue l'une des grandes révolutions de l'Internet qui réorganise les rapports sociaux entre groupes ou individus ainsi que l'accès à l'information. L'Homme se digitalise et s'inscrit dans une communauté virtuelle d'usagers, influençant par la même occasion sa manière de vivre et de consommer l'information. La passion et les instincts « premiers » prennent ainsi le pas sur la réflexion et la critique traditionnelle, tandis que les

identités réelles et numériques forment un ensemble progressivement indivisible. En conséquence, les réseaux sociaux modifient les réflexes policiers et ouvrent de nouvelles perspectives opérationnelles : aide à l'enquête, collecte d'informations pratiques, réalisation de rapprochements ou d'environnements des mis en cause, cartographie des interactions, matérialisation d'infractions et infiltration numérique de groupes criminels. Dans le cadre d'une gestion de crise (ex : alerte enlèvement), l'emploi des plateformes sociales comme vecteur de diffusion massive de messages ciblés dans un délai contraint constitue une nouvelle opportunité.

L'espace numérique : nouvelles sources de preuves pour l'enquête

La révolution numérique se déploie également au travers de la diffusion d'objets connectés scrutant et interagissant avec le monde physique. Agrégat de solutions matérielles et logicielles dans une architecture en réseau, cet écosystème génère une grande diversité d'informations : des données d'utilisateurs, de contexte, de système, des logs de fonctionnement, etc. L'accroissement du nombre d'objets amène à un volume total d'informations échangées extrêmement élevé. Les données collectées constituent une nouvelle manne économique pour les acteurs du numérique. Elles sont l'« or noir » du XXIe siècle. Tous les deux ans, la volumétrie des données générées par l'Internet des objets double la taille de l'univers numérique (Cosquer et al., 2016).

L'Internet des objets ouvre de nouvelles perspectives pour les enquêtes judiciaires, en particulier dans le domaine de la question des sources de données. En effet, celles-ci diffèrent par leur nature, leur nombre, leur format et les protocoles utilisés. Classiquement, les matériels étudiés sont des ordinateurs, des appareils mobiles, des passerelles, des équipements de stockage ou des serveurs. L'Internet des objets renvoie aux appareils ménagers, aux systèmes domotiques, aux équipements médicaux pour le vivant – homme ou animal -, aux voitures, aux lecteurs RFID (*Radio Frequency Identification*), etc. Cette hétérogénéité des équipements est renforcée par les phénomènes du « fait maison » (*maker kit*) et du « DIY » (*Do It Yourself*), où un objet physique trouve sa place dans l'écosystème numérique et connecté par l'apposition de dispositifs de communication (ex : le végétal dit connecté). En outre, les données numériques varient également en fonction des interactions avec l'environnement, la structuration de l'écosystème et les services rendus. Le croisement des traces autorise des recoupements d'informations et des investigations aux potentialités inédites. Ces éléments sont susceptibles d'orienter la stratégie d'investigation d'une scène de crime en offrant des informations sur un parcours et une logique criminelle.

L'objet est souvent sélectionné par l'enquêteur au regard de ses propriétés mécaniques et de la proximité directe par rapport à l'événement survenu. Toutefois, un système connecté constitue dans de nombreuses situations un acteur certes passif, mais tout aussi pertinent.

L'enquête criminelle utilise de plus en plus les techniques cyber

C'est le cas pour les thermostats connectés disposant de la fonctionnalité de géorepérage (*geofencing*), matérialisant la proximité directe du téléphone exploitant le service.

Les traces proviennent également d'informations indirectes. Lorsqu'un incident se produit localement au sein d'un dispositif connecté, tous les journaux du flux de trafic constituent de potentielles traces probantes telles que l'enquêteur peut retrouver dans les pare-feu ou les systèmes de détection d'intrusions *Intrusion Detection System* (IDS) (Joshi et al., 2016). Or, cette donnée doit être contextualisée pour être valorisée : par exemple, une serrure intelligente est en mesure d'enregistrer les événements d'ouverture et de fermeture d'une porte. Par association, elle offre l'opportunité d'identifier la manière d'accéder dans un bâtiment sécurisé et donc révèle la présence ou l'absence d'une personne. Aussi elle date un passage. En reconnaissant le moyen de l'accès (badge, téléphone portable, digicode, commande vocale, etc.), l'enquêteur est en mesure de personnaliser l'événement, un mode opératoire et son potentiel acteur. La solution est d'autant plus intéressante à étudier qu'elle peut constituer un maillon d'un écosystème beaucoup plus complexe et étendu, fédéré autour d'une couche de service propre. La serrure intelligente peut appartenir à un environnement domotique doté d'une solution d'assistance vocale commune à plusieurs systèmes concourants et interdépendants.

L'objet connecté est donc la face visible et locale de l'infrastructure de l'Internet des objets, porte d'entrée des investigations judiciaires. La recherche, l'identification et l'analyse de cet élément catalyseur sont primordiales pour comprendre l'architecture globale et obtenir une information pertinente au regard de l'enquête. L'enquêteur doit être en mesure d'associer à un phénomène criminel et sa donnée, un dispositif physique. Il doit ainsi comprendre le parcours de l'information dans l'architecture connectée, de son initialisation à son interception. Cette perception oriente les investigations et les actes techniques dans l'obtention de traces probantes pour le procès pénal. La valeur ajoutée de l'Internet des objets vient du fait que le tout est plus grand que la somme des parties, ce qui explique que les approches unité par unité (centrées sur l'objet décontextualisé) passent à côté de la valeur ajoutée de l'Internet des objets (Bouchaud, 2021).

L'espace numérique : vecteur criminel et enjeu sécuritaire du 21e siècle

Un nouveau paradigme sécuritaire est apparu avec l'essor de l'informatique dans les années 90, présageant une réorganisation des prérogatives régaliennes de l'État et une tendance à la normalisation du concept de guerre numérique (Liang et al., 2006). En France, la doctrine s'est progressivement adaptée à cette nouvelle menace notamment face à l'accroissement du nombre de cyberattaques. Ces agissements menés par des acteurs étatiques, non étatiques, pirates informatiques, activistes ou organisations criminelles ont été définis dès 2008 dans le livre blanc sur la défense et la sécurité nationale (Mallet, 2008).Cette prise de conscience doctrinale résulte notamment de l'attaque DDOS subie par l'Estonie en 2007. Dix ans plus tard, le constat établi par le Secrétariat Général de la Défense et de la Sécurité Nationale vient confirmer cet état de fait : « le cyberespace apparaît aujourd'hui comme un catalyseur de progrès mais aussi un lieu de confrontation, de domination et de trafics en tout genre » (SGDSN, 2018).

Quatre typologies de menaces liées au cyberespace sont ainsi mises en exergue par le corpus doctrinal français : le cyberespionnage, le sabotage, la désinformation et la cybercriminalité. Cette appréhension quadripartite de la menace cyber contribue fortement à la structuration de la cyberdéfense française et au renforcement des moyens opérationnels pour contrer cette menace inédite, aux conséquences économiques et stratégiques croissantes. Les forces de sécurité sont désormais confrontées à un nouveau paradigme sécuritaire où l'imputation de l'attaque est « extrêmement difficile » (Poupard, 2018), basée sur une approche techno-centrée afin de « préciser l'auteur d'une cyberattaque par des preuves ou un faisceau d'indices » (Ministère des Armées, 2019), et dont l'attribution publique relève des plus hautes autorités politiques de l'État en fonction des enjeux géopolitiques.

L'espace numérique : nouveau champ opérationnel de la criminalité organisée

Les services de sécurité doivent s'adapter à un espace en évolution constante, favorisant la confrontation et l'action

offensive, sans limitation géographique quant à la portée des attaques, avec des actions d'une grande précision ou d'ampleur. Considérant ces caractéristiques particulièrement avantageuses pour tout attaquant, la criminalité, organisée ou non, s'est adaptée et a su pleinement tirer profit de ce nouveau vecteur : elle n'a jamais été aussi éloignée géographiquement de ses cibles, tout en ayant la capacité de frapper au cœur de celles-ci, et avec des risques minimes de rétorsions judiciaires en raison de l'anonymat offert par le cyberespace. En effet, en considérant l'activité criminelle selon un prisme économique, la rationalité des acteurs tend à rechercher une moindre exposition pour une rentabilité maximisée. Si l'impact de la cybercriminalité a été sous-estimé, car les effets ont été perçus comme étant moins concrets car virtuels, les conséquences en matière de sécurité nationale et économiques sont importantes, tandis que les atteintes aux biens (sabotage) et aux personnes (proxénétisme, pédopornographie, trafics de stupéfiants, etc.) trouvent un nouveau champ d'expression.

Si les activités illicites en ligne ont pu être l'œuvre de pirates isolés il y a quelques années, la cybercriminalité organisée constitue aujourd'hui une menace majeure qui nécessite un changement de doctrine dans l'action des forces de sécurité intérieure. Les groupes criminels organisés se sont professionnalisés et numérisés. Leur organisation, similaire à celles de structures privées ou étatiques, leur permet de mener des cyberattaques toujours plus sophistiquées techniquement et dont il devient de plus en plus difficile de se prémunir.

Les « cyber-GCO » (Groupes de criminalité organisé) portent de graves atteintes à l'État français, à son tissu économique et industriel, et à ses citoyens, tout en limitant fortement les risques d'être appréhendés, puisque agissant à distance et sous le sceau de l'anonymat.

Ainsi, les cyber-GCO ont connu une forte croissance et une importante montée en compétence technique : que les opérations les plus sophistiquées et complexes relèvent d'*Advanced Persistent Threat* (APT), dont les liens avec des États sont souvent mis en exergue par la presse, ne doit pas oblitérer le fait que certains groupes cybercriminels sont également des APT autonomes.

Ces structures criminelles ciblent un large spectre de victimes, de l'OIV (Opérateur d'Importance Vitale) au particulier, traduisant leur grande adaptabilité. Au sein de cette criminalité organisée, il existe à la fois une nouvelle génération de criminels ayant saisi les opportunités qu'offrent les vulnérabilités de la numérisation de la société, mais également des groupes traditionnels qui déplacent leurs activités vers l'espace numérique, que ce soit par opportunisme ou dépendance aux nouvelles technologies.

In fine, six groupes peuvent être distingués : ceux appartenant à un État étranger et leurs services de renseignement, ceux soutenus ou tolérés par les États, les groupes structurés qui sont assimilables aux groupes criminels organisés traditionnels, les groupes de circonstance qui se constituent et agissent en fonction des objectifs visés, les groupes d'activistes (« *hacktivistes* »), les groupes cyberterroristes ou financés par ces mouvances afin de procéder à des actions. Tous ces groupes ne s'inscrivent pas dans une étanchéité organisationnelle ou opérationnelle lorsque leurs intérêts convergent.

L'ensemble de ces facteurs génère une adaptation constante de la Gendarmerie Nationale d'un point de vue organisationnel (avec la création du Commandement du cyberespace de la Gendarmerie et de ses antennes) et doctrinal (formation, coordination, évolution des process) pour mener des actions de prévention auprès du public et d'assistance auprès des victimes, mais également pour diligenter les investigations confiées dans ce cadre et participer aux futures gestions de crises cyber, dont l'impact sera toujours plus important en raison de la connectivité croissante de nos sociétés.

Le développement de nouveaux protocoles de communication (5G, LoRaWAN, SigFox, et 6G à compter de 2030), va permettre une démocratisation de l'emploi des objets connectés par la population : cette technologie peut absorber jusqu'à un million d'objets connectés par kilomètre carré. Or, la conjonction de ces nouvelles architectures couplées à l'Internet des objets va générer une augmentation exponentielle de la surface d'attaque. Cette dernière constituera un élément central de la capacité des cybercriminels à opérer avec une plus grande granularité, en élargissant constamment le spectre de leurs capacités offensives. En outre, ces objets connectés pourront devenir de nouveaux vecteurs d'attaques et être utilisés massivement à l'instar des botnets.

Enfin, ces nouvelles technologies imposent aux forces de sécurité intérieure, une importante adaptation capacitaire de leurs techniques de surveillance et d'enquête, notamment en matière d'interception des communications. Cette problématique se conjugue aux risques de souveraineté quant à la pleine maîtrise de ces technologies, à l'accès et au stockage des données, et du maintien des services, dont l'indisponibilité provoquerait une paralysie critique de la société.

Bibliographie

HAZANE E. (2018), « Sécurité numérique des objets connectes, l'heure des choix », https://www. frstrategie.org/sites/default/files/documents/publications/notes/2018/201815.pdf

COSQUER C. and LANCKRIET J. (2016), « Les objets connectés et la défense », Revue défense nationale, N° 787, pp. 97-103.

JOSHI RC. and PILLI E. S. (2016), « Fundamentals of Network Forensics », Springer.

BOUCHAUD F. (2021), « Analyse forensique des écosystèmes intelligents communicants de l'Internet des objets », thèse de doctorat, Université de Lille.

LIANG Q. and XIANGSUI W. (2006), « La guerre hors limites », Payot et Rivages, p. 80

MALLET JC. (2008), « Livre blanc sur la défense et la sécurité nationale », p. 53

SGDSN (2018), « Revue stratégique de cyberdéfense », p. 3 et 9

POUPARD (2018), « Commission de la défense nationale et des forces armées, Audition de M. Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information, sur le projet de loi de programmation militaire, session ordinaire 2017-2018, compte-rendu n° 53, jeudi 8 mars 2018, séance de 11 heures 00 »

MINISTÈRE DES ARMÉES (2019), « Politique ministérielle de lutte informatique défensive, Commandement de la cyberdéfense », p. 5

François BOUCHAUD en bref…

Capitaine de gendarmerie, dirige le Département coordination opérationnelle cyber (DCOC) du Centre de lutte contre les criminalités numériques (C3N) au sein du Commandement de la gendarmerie dans le cyberespace (ComCyberGend). Titulaire de plusieurs masters (Systèmes embarqués, Génie industriel et Management de la sécurité), il détient un doctorat en informatique et applications.

Pascal MARTIN en bref…

Lieutenant, dirige le Groupe des relations internationales (GRI) du Département de coordination opérationnelle cyber (DCOC) au sein du Commandement de la gendarmerie dans le cyberespace (ComCyberGend). Titulaire d'un master en droit, il est doctorant en histoire contemporaine à l'Université de Bordeaux sous la direction du professeur Sébastien-Yves Laurent.