À la poursuite des cybercriminels

Par **Jacques MARTINON**
Mission de Lutte contre la Cybercriminalité (MLC)

Introduction

Le cybercriminel est dans la majorité des cas un délinquant ayant le souhait d'optimiser sa rentabilité économique et qui s'adapte en conséquence aux nombreuses opportunités du monde numérique. L'aspect communautaire est également important, des spécialistes émergeant afin d'offrir une galaxie de services (*Cybercrime as a Service*) dans le cadre d'un écosystème désormais bien établi. Toutefois, certains acteurs de la cybercriminalité ont des motivations différentes, soutenus voire armés par des ressources étatiques plus ou moins clandestines, dans le cadre de guerres économiques larvées (cyberespionnage) ou de démonstrations de puissance (cybersabotage), multipliant les pré-positionnements à l'intérieur de systèmes critiques. Comme le relève la « Revue stratégique de Cyberdéfense » (février 2018 [(1)]), la menace est hybride et le cloisonnement entre cyberdéfense et cybercriminalité s'estompe.

Les acteurs judiciaires de lutte contre la cybercriminalité doivent donc adapter rapidement leurs stratégies, méthodes et organisations afin d'améliorer leur efficacité. La France n'a initié véritablement ce mouvement qu'en 2015, dans les suites du rapport de référence sur la cybercriminalité « Protéger les internautes », élaboré sous l'égide du procureur général Marc Robert [(2)]. Des progrès indéniables ont été réalisés, mais la poursuite de ces efforts est essentielle afin de consacrer un véritable levier judiciaire redouté par les cybercriminels et activable dans le champ de la cyberdéfense.

Si toutes les juridictions peuvent connaître des faits de cyberdélinquance [(3)], il convient de relever que le tribunal de grande instance de Paris bénéficie d'une compétence concurrente nationale en matière de cyberattaques [(4)]. Les contours d'une politique pénale de lutte contre la cyberdélinquance sont en voie de consolidation en priorisant les tendances les plus préoccupantes touchant la population française ainsi que son tissu économique.

Seront présentées dans un premier temps les caractéristiques principales de la cybercriminalité (1), avant d'aborder les adaptations stratégiques et organisationnelles des acteurs judiciaires, ainsi que les nouvelles relations de ces acteurs avec ceux de la cybersécurité (2).

Une cybercriminalité polymorphe et occulte

La typologie de la cybercriminalité demeure un défi intellectuel puisque l'angle traditionnel des qualifications pénales est imparfait. Les « cyberattaques » recouvrent en réalité de

(1) http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf
(2) Rapport « Protéger les internautes » du groupe de travail interministériel sur la lutte contre la cybercriminalité, février 2014, consultable à l'adresse suivante http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
(3) Nous utiliserons indifféremment les expressions « cybercriminalité » et « cyberdélinquance », étant entendu que le terme « cybercriminalité » est le plus usité du fait de son pendant anglo-saxon « cybercrime », alors même que la quasi-intégralité des infractions « cyber » sont bien des délits, et non des crimes au sens du droit pénal français.
(4) Article 706-72-1 du Code de procédure pénale (créé par la loi n°2016-731 du 3 juin 2016) : « Pour la poursuite, l'instruction et le jugement des infractions entrant dans le champ d'application de l'article 706-72, le procureur de la République, le pôle de l'instruction, le tribunal correctionnel et la cour d'assises de Paris exercent une compétence concurrente à celle qui résulte de l'application des articles 43, 52 et 382. »

nombreux « phénomènes cyber » distincts dans leur mode opératoire et leur motivation, tels le cyberespionnage, le cybersabotage, le rançongiciel…

Aujourd'hui, la cybercriminalité reste largement occulte, notamment car les outils statistiques traditionnels sont *de facto* inopérants pour apprécier finement les évolutions des phénomènes. À cela s'ajoutent les problématiques classiques du chiffre noir et d'une preuve numérique parfois chimérique.

Une cybercriminalité polymorphe et évolutive

La cybercriminalité a pour caractéristiques principales d'être polymorphe et naturellement très évolutive, bénéficiant du dynamisme de l'écosystème numérique.

Une classification délicate

La cyberdélinquance au sens strict couvre les phénomènes pénaux dont l'objet est l'atteinte à un Système de Traitement automatisé de Données (STAD) réprimée par les articles 323-1 à 323-4 du Code pénal. Dans la pratique, cette catégorie est divisée entre les phénomènes de haute intensité (atteinte aux intérêts fondamentaux de la Nation, dimension internationale, haute technicité, nombre important de victimes avérées ou supposées) et de basse intensité.

La seconde catégorie regroupe les phénomènes qui ont pour vecteur principal un STAD ou ont été facilités par son utilisation, il s'agit de la cyberdélinquance au sens large, incluant de nombreuses escroqueries. Ces infractions mixtes couvrent également la lutte contre les activités illicites sur l'Internet sombre (*darknets* [5]).

Les nouveaux métiers de la cybercriminalité

La cybercriminalité prospère et de nouveaux « métiers » fleurissent régulièrement, faisant naître le concept de « *Cybercrime as a Service* » (analogie avec les services informatiques traditionnels), telles les locations/ventes d'infrastructures de type *botnets* (réseau d'ordinateurs ou d'objets connectés [6] « zombies », sous le contrôle d'un serveur dit *Command & Control*), de maliciels divers (comme certains rançongiciels qui connaissent un regain dévastateur auprès des entreprises et des collectivités territoriales), des services de *Crypter/Packer* (augmentant la furtivité des maliciels), de *Money mules* (personne qui transfère de l'argent acquis illégalement pour le compte de tiers) ou encore de *Mixer/Blender* [7] (facilitant le blanchiment des cryptomonnaies).

Les cryptomonnaies sont sources de nombreuses opportunités, qu'elles soient dérobées aux plateformes d'échanges ou aux particuliers, ou bien que la puissance de calcul de terminaux soit détournée afin de « miner » des cryptomonnaies au bénéfice de l'attaquant (*Cryptojacking*).

Plus original, il existe des campagnes de recrutement *via* des annonces d'emploi pour des administrateurs de *Darknets,* comme ci-dessous pour Liberty Market (figure 1) :

> « **Nous cherchons à recruter un membre**, homme ou femme, qui possède une bonne orthographe. Vous devrez être familier avec la gestion ergonomique des pages web. Il faudra que vous puissiez vous connecter au moins une heure et demie, quatre fois par semaine. Vous serez en charge de la correction des posts du forum et responsable de leur bonne lisibilité. Vous devrez aussi corriger des douzaines de posts à chaque connexion. Vous aurez votre propre tableau de bord afin que vous puissiez travailler en toute autonomie. »

Figure 1. Source : www.ladn.eu

(5) Le plus célèbre étant le protocole TOR (*The Onion Router*).
(6) Un cas célèbre étant le Botnet issu du maliciel Mirai en 2016, ayant servi à des attaques DDos (*Distributed Denial of Service*) touchant notamment OVH et Dyn, cette dernière affectant une partie critique d'Internet au niveau de la gestion des services DNS (*Domaine Name System*). En août 2019, le C3N (Gendarmerie nationale) a démantelé avec succès le Botnet Retadup, composé de plus de 500 000 machines infectées.
(7) Le site Bestmixer.io a toutefois été mis sur la touche par une action conjointe d'EUROPOL et des enquêteurs financiers néerlandais, avec un chiffre d'affaires estimé à 200 millions d'euros.

Dans la même veine, on relèvera un service de type « Tag Telegram », où des personnes sont simplement rémunérées pour réaliser des tags dans des zones urbaines prédéterminées, de façon à fournir des indications techniques pour rejoindre une discussion Telegram d'un dealer. Ce nouveau *job* permet de matérialiser « l'ubérisation » rampante des trafics de stupéfiants, où le consommateur commande directement sa drogue *via* son *smartphone* et une application de messagerie cryptée, et se fait livrer à domicile H24 7j/7.

Figure 2 : cas ukrainien (15$/jour – SMIC mensuel local 140$). Source : Trustwave

Une des conséquences probables pourrait être l'éclatement des logiques des territoires de points de *deals*, avec un déplacement sur la visibilité, furtivité et popularité de leur vecteur numérique de communication. D'autres tendances inquiétantes semblent se dessiner avec des applications d'échange décentralisées, anonymes et basées sur les cryptomonnaies (par exemple : Openbazaar, Haven).

Une cybercriminalité occulte

La lutte contre la cybercriminalité est handicapée par plusieurs facteurs, notamment un nombre important d'infractions qui ne sont pas portées à la connaissance de la justice et une preuve numérique aléatoire.

Le chiffre noir de la cybercriminalité

Certains phénomènes cybercriminels de haute intensité, comme le cyber-espionnage ou le cyber-sabotage, sont peu judiciarisés, du fait de leur nature sensible [(8)]. La publicité d'une cyber-attaque à l'encontre d'une entreprise peut nuire à son image. Le règlement européen pour la protection des données personnelles (RGPD) est un espoir, dès lors que les violations de données personnelles conduisent à une obligation de notification dans les 72 heures à la CNIL [(9)].

Concernant les particuliers, les raisons du chiffre noir sont diverses, du fait d'un caractère parfois imperceptible de l'infraction ou d'un sentiment erroné de l'inutilité de la plainte, souvent couplé à de faibles préjudices matériels.

Une meilleure sensibilisation semble nécessaire, d'où l'importance du dispositif national d'assistance aux victimes d'actes de cybermalveillance [(10)], et des mesures facilitant le dépôt de plainte. La future plateforme THESEE (projet porté par le ministère de l'Intérieur) est susceptible d'améliorer la connaissance statistique pour certains phénomènes de cybercriminalité. La récente

(8) La doctrine américaine est différente à cet égard, au vu de l'activisme récent du *Department of Justice (DoJ)* à l'encontre de ressortissants chinois ou russes.
(9) Voir le cas d'Airbus en janvier 2019.
(10) https://www.cybermalveillance.gouv.fr/

Loi de Programmation pour la Justice (LPJ) insère d'ailleurs de nouvelles dispositions afin d'encadrer la plainte en ligne [11].

Preuve numérique, "going dark [12]" et extraterritorialité

La libéralisation du chiffrement a amélioré sensiblement le niveau de cybersécurité, mais a provoqué de manière collatérale des difficultés propres aux investigations judicaires. La banalisation des applications de messageries instantanées chiffrées avec des protocoles particulièrement robustes, comme ceux dits *End to end,* est un défi actuel. De même, la généralisation du chiffrement de type *full disk* sur les terminaux informatiques, dont les *smartphones*, a rendu délicate l'exploitation forensique. Enfin, comme déjà évoqué, les architectures réseaux de type TOR (*The Onion Router*) participent à l'obfuscation des comportements criminels sur les *Darknets*. Demain, la fusion annoncée entre les applications de messageries et les cryptoactifs ne manque pas d'inquiéter les professionnels [13]. L'annonce du LIBRA par la société Facebook, avec son caractère systémique au vu du nombre de ses utilisateurs potentiels, a suscité une forte réaction politique qui devra se concrétiser en régulation efficiente en termes de mécanismes AML (mesures anti-blanchiment) et KYC (connaissance de clientèle).

Complétant un tableau déjà bien sombre, s'ajoute la difficulté d'une preuve numérique désormais largement stockée en dehors de nos frontières, du fait de l'essor de l'informatique à distance (*Cloud*), mais une éclaircie semble percer les nuages.

En effet, une révolution est en cours avec le futur règlement européen "E-Evidence", doublé d'une directive dite « représentant », cette dernière posant le prérequis juridique de l'applicabilité du droit européen aux entreprises mondiales dirigeant leur activité économique sur le territoire européen [14]. Le sujet est au centre de tensions diplomatiques avec les États-Unis, un indispensable dialogue devant être mené par la Commission européenne avec ces derniers afin de résoudre certains conflits de lois. Des négociations entourant un second protocole additionnel à la Convention de Budapest contre la cybercriminalité (Conseil de l'Europe) sont par ailleurs bien avancées.

Dans l'intervalle, et anticipant ces révolutions dans l'accès transfrontalier à la preuve, la politique interne de certains GAFAM (Google par exemple) s'est modifiée récemment en transférant la gestion de certaines réquisitions judiciaires françaises de leur maison mère basée aux États-Unis à leur filiale de droit irlandais [15].

Une adaptation stratégique et organisationnelle des acteurs judiciaires

Une enquête cyber possède plusieurs spécificités, souvent liées à la preuve numérique. La dissémination des victimes cyber sur le territoire conduit à une certaine rationalisation du traitement judiciaire, tandis que la culture du silo administratif doit laisser la place à des échanges inter-institutionnels du fait de la nature transversale des enjeux numériques.

(11) Nouvel article 15-3-1 du Code de procédure pénale.
(12) Cette expression d'origine militaire fait référence à la perte soudaine des communications de l'adversaire pouvant être analysées au profit de moyens de communications indétectables.
(13) Voir le lancement du réseau TON et la cryptomonnaie GRAM par l'entreprise TELEGRAM, annoncé pour le dernier trimestre 2019, suite à une levée de fonds de 1,7 milliard de dollars.
(14) Le Règlement général de Protection des Données (RGPD) européen avait posé une première pierre à l'édifice, quoique sur des critères de rattachement distincts.
(15) Force est de constater que la quasi-totalité des sociétés californiennes du numérique sont installées en Irlande, potentiellement pour des questions d'optimisation fiscale.

Aperçu de stratégies judiciaires

Seuls quelques exemples seront évoqués dans le présent article, par manque d'espace mais aussi par volonté de ne pas trop en dévoiler (le lecteur nous pardonnera mais les cybercriminels sont à l'affût de toute information en la matière [16]). Comme le disait le Doyen Carbonnier, à propos du procès civil : « Si les coups bas sont interdits, les simples ruses de guerre ne le sont pas. »

La récupération de la preuve numérique nécessitera souvent d'identifier et de localiser les serveurs "Back End", où se situe l'essentiel des éléments pouvant être dissimulés derrière une multitude de serveurs "Proxy", afin de lancer *in fine* des opérations de perquisition chez le prestataire. Il n'est pas rare que les serveurs en question soient à l'étranger, et une fine coopération judiciaire internationale sera primordiale.

Concernant les techniques spéciales d'enquête, le régime de l'enquête sous pseudonyme est particulièrement adapté. La traçabilité de certains cryptoactifs comme le Bitcoin peut également être facilitée par des logiciels commerciaux.

Lors de l'interpellation des suspects, priorité sera donnée au "Live Forensics", c'est-à-dire aux investigations numériques d'urgence sur les supports informatiques découverts, afin de minimiser des difficultés techniques ultérieures comme le chiffrement des données.

Enfin, la recevabilité des preuves obtenues par des services d'enquête étrangers n'est pas un sujet simple, et la jurisprudence nous paraît relativement instable. Ainsi la Cour de cassation a considéré que la création d'un faux site pédophile par les autorités américaines constituait une provocation à l'infraction, et donc annulera la procédure française (Cass. Crim., 7 février 2007, n°06-87.753). Toutefois, en 2014, elle validera un recueil de preuve *via* un forum créé par le FBI sur la fraude à la carte bancaire (Cass. Crim., 30 avril 2014, n°13-88.162). Assurément les débats juridiques se poursuivront avec la multiplication des techniques de pot de miel (*Honey Pot*) par certaines autorités étrangères.

Adaptations organisationnelles et relations des acteurs judiciaires avec ceux de la cybersécurité

Constats sur l'organisation judiciaire en 2019

Sans pouvoir détailler ici les multiples compétences territoriales de l'autorité judiciaire en matière de cybercriminalité, il sera rappelé le rôle primordial du tribunal de grande instance de Paris bénéficiant depuis la loi du 3 juin 2016 d'une compétence concurrente nationale en matière d'atteintes aux STAD et de crimes de sabotage informatique [17].

Cette réforme a permis de consolider la création en 2015 d'une section dite « F1 » du parquet de Paris dédiée au traitement de certaines affaires de cybercriminalité, notamment les plus complexes. Les effectifs de cette section sont en progression [18]. Le constat est plus inquiétant au siège, avec l'absence notamment de juge d'instruction véritablement spécialisé. Des dépêches de centralisation du traitement de certains phénomènes de cybercriminalité sont à relever, produites par la Mission de Lutte contre la Cybercriminalité de la Direction des Affaires criminelles et des Grâces (DACG) du ministère de la Justice [19].

(16) Preuve en sont les échanges en procédure pénale détectés sur certains forums de *Darknets*.
(17) Nouvel article 706-72-1 du Code de procédure pénale.
(18) Trois magistrats, ainsi qu'un assistant spécialisé et un greffier (septembre 2019).
(19) Exemple : dépêches DACG des 10 mai 2017 et 22 juin 2018 concernant d'une part la mise en œuvre opérationnelle de la compétence nationale concurrente du parquet de Paris en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et le traitement judiciaire des « rançongiciels », et d'autre part la centralisation du traitement des « fraudes aux réparations informatiques ».

Au-delà, les juridictions interrégionales spécialisées (JIRS) connaissent de plus en plus de contentieux de la cybercriminalité, notamment liée à la criminalité organisée [20]. Enfin, un réseau de magistrats « cyber-référents » dans les tribunaux, cours d'appel et JIRS est en voie de généralisation, dans les suites de la première réunion nationale des magistrats cyber-référents, co-organisée le 14 juin dernier par le parquet de Paris et la DACG.

Densification des liens entre les acteurs judiciaires et ceux de la cybersécurité

L'administration centrale (DACG), *via* la mission précitée, contribue aux travaux stratégiques du centre de coordination des crises cyber (C4), instauré suite à la « Revue stratégique de Cyberdéfense » précitée, ainsi qu'aux réunions du Groupe de Contact permanent (GCP). Ce GCP, piloté par la délégation ministérielle en charge des industries de sécurité et à la lutte contre les cybermenaces (DMISC), a pour objectif d'améliorer le dialogue avec les acteurs privés comme Apple, Google, Twitter, Microsoft, Facebook, et récemment Dropbox, dans un esprit constructif partagé.

Enfin, la DACG fait partie du conseil d'administration du GIP ACYMA (cybermalveillance.gouv.fr) et participe à la formation commune « Souveraineté numérique et cybersécurité » de l'IHEDN (Institut des hautes Études de la Défense nationale) et de l'INHESJ (Institut national des hautes Études de Sécurité et de Justice) dont le public est constitué de hauts cadres publics et privés, ainsi que de membres de la société civile.

Conclusion

Le levier judiciaire doit encore gagner en maturité mais des progrès sont indéniablement en cours. La coopération internationale est un facteur-clé de ce succès, avec l'aide conjointe d'EUROPOL, d'EUROJUST et d'INTERPOL. Les menaces issues du monde numérique ne doivent pas rester sans réponse, d'autant que la surface d'attaque ne cesse de s'étendre, avec des conséquences potentiellement systémiques pour l'économie et des mises en danger de l'intégrité physique de nos citoyens. Le constat peut sembler alarmiste mais quelle réaction adopter demain en cas de rançongiciel paralysant un hôpital ou entraînant un dysfonctionnement d'une voiture connectée à pleine vitesse sur autoroute ? Jusqu'ici, tout va (presque) bien.

Figure 3 : Gunshow, KC GREEN

(20) Exemple : le démantèlement de la Main noire, une plateforme du *Darknet*, sous la supervision de la JIRS de Lille.