Les défis du traitement judiciaire de la cybercriminalité

par Jacques MARTINON

A PROPOS DE L'AUTEUR

Jacques MARTINON

Magistrat judiciaire, Jacques MARTINON a débuté sa carrière en tant que juge d'instruction (2008-2015). Depuis janvier 2016, il a rejoint la direction des affaires criminelles et des grâces (DACG) du ministère de la Justice, afin d'intégrer la mission de prévention et de lutte contre la cybercriminalité, qu'il dirige désormais. Contributeur à la Revue stratégique de cyberdéfense élaborée sous l'égide du SGDSN, il est intervenu comme formateur à la session nationale « *souveraineté numérique et cybersécurité* » organisée par l'INHESJ et l'IHEDN. Il est enfin titulaire du diplôme universitaire de cybercriminalité de l'université de Montpellier (Major 2018). Chargé de cours à Science-Po Paris.

RÉSUMÉ

La cybercriminalité couvre traditionnellement les cyberattaques, visant les systèmes informatiques eux-mêmes, mais également les infractions ayant pour vecteur principal ou étant considérablement facilitées par l'usage d'un réseau de communication. Si toutes les juridictions peuvent connaitre des faits de cyberdélinquance, le tribunal de grande instance de Paris bénéficie toutefois d'une compétence concurrente nationale en matière de cyberattaques. Les contours d'une politique pénale de lutte contre la cyberdélinquance sont en voie de consolidation, toutefois les moyens humains consacrés demeurent trop limités et l'organisation judiciaire toujours en quête de maturité.

Seront présentées dans un premier temps les caractéristiques principales de la cybercriminalité avant d'aborder succinctement l'organisation judiciaire actuelle et les relations des acteurs judiciaires avec ceux de la cybersécurité.

UNE CYBERCRIMINALITÉ POLYMORPHE ET DÉLICATE À APPRÉHENDER PAR LE PRISME JUDICIAIRE TRADITIONNEL.

Le périmètre pénal de la cybercriminalité est un véritable défi intellectuel. L'angle traditionnel des qualifications pénales est en effet peu adapté. Par exemple, les atteintes aux systèmes de traitement automatisé de données (STAD) recouvrent en réalité plus d'une dizaine de « phénomènes cyber » différents, tels le cyberespionnage, le cybersabotage, le rançongiel…

En conséquence, les outils statistiques traditionnels sont quasi inopérants pour apprécier les évolutions des phénomènes au cas par cas. Une approche nouvelle, sous l'angle de la classification des phénomènes cyber constatés, semble nécessaire aujourd'hui.

Une cybercriminalité polymorphe et évolutive

La cybercriminalité, qui d'ailleurs recouvre en réalité une majorité de délits, a pour caractéristiques principales d'être polymorphe et très évolutive.

• Une classification délicate

Les phénomènes cyberdélinquants sont traditionnellement classifiés en deux catégories distinguant l'objet de l'infraction.

La cyberdélinquance au sens strict couvre les phénomènes pénaux dont l'objet est l'atteinte à un système de traitement automatisé de données (STAD) et fait l'objet de la première catégorie. La seconde 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 et la plus fréquente.

Infractions ayant pour objet un système de traitement automatisé de données

Ces infractions visent à porter atteinte aux STAD, comme par exemple le cybersabotage. Ces infractions, notamment réprimées par les articles 323-1 à 323-4 du Code pénal, représentent la cyberdélinquance au sens strict. Dans la pratique, cette catégorie est divisée entre :

✓ les phénomènes de haute intensité qui se caractérisent par une atteinte aux intérêts fondamentaux de la Nation, une dimension internationale, une haute technicité, ou un nombre important de victimes avérées ou supposées ; et

✓ les phénomènes de basse intensité qui se caractérisent par l'absence d'atteinte aux intérêts fondamentaux de la Nation ou un degré de complexité moindre.

Infractions ayant pour vecteur principal ou ayant été grandement facilitées par un système de traitement automatisé de données

Elles couvrent l'utilisation d'un STAD qui a grandement facilité la préparation, l'accomplissement ou la tentative d'une infraction principale n'ayant pas pour objet un STAD. Ces infractions mixtes couvrent également la lutte contre les activités illicites sur l'internet sombre (*darkweb*).

Cette catégorie, la plus vaste, couvre aussi des phénomènes pénaux classiques mais nécessitant des investigations très poussées dans l'espace numérique.

• Phénomène évolutif : les nouveaux métiers de la cybercriminalité

La cybercriminalité ne semble pas connaître la crise, bien au contraire de nouveaux « métiers » fleurissent régulièrement, faisant naître le concept de « *Crime as a Service* », par analogie avec les services informatiques traditionnels tels que le « *Platform as a Service* » ou le « *Software as a Service* ».

Sans prétendre à l'exhaustivité, on peut citer pêle-mêle les locations/ventes d'infrastructures comme des *Botnets* (réseau d'ordinateurs ou d'objets connectés[1] « zombies », sous le contrôle d'un serveur dit *Command & Control*), de maliciels divers (parfois avec une rémunération au pourcentage sur les sommes dérobées comme certains rançongiciels), 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* (facilitant le blanchiment des cryptomonnaies).

Les cryptomonnaies ont d'ailleurs permis de nombreuses opportunités pour les cybercriminels, que ce soit en les dérobant directement au préjudice des plateformes d'échanges ou des particuliers, mais également en détournant la puissance de calcul de terminaux afin de « miner » des cryptomonnaies au bénéfice de l'attaquant (le *Cryptojacking* étant le plus gros phénomène en 2018).

Plus original encore, il existe des compagnes de recrutement via des annonces d'emploi pour des administrateurs de *darknets*, comme ci-dessous pour Liberty Market :

> *« 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. »*
> *Source : www.ladn.eu*

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, comprenant des indications techniques pour rejoindre une discussion Telegram d'un *dealer* : cf. photo infra.

Les malédictions de la cybercriminalité : chiffre noir, brouillard statistique et phénomène du « going dark »

Le traitement judiciaire de la cybercriminalité est rendu plus difficile en raison de plusieurs facteurs, notamment un nombre important d'infractions qui ne sont pas portées à la connaissance de la justice (**A**), d'une mauvaise évaluation des infractions qui sont connues de la justice (**B**) et enfin des techniques d'obfuscation de plus en plus élaborées, utilisées par les cybercriminels pour se soustraire aux autorités judiciaires (**C**).

• 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 particulièrement sensibles[2]. Surtout, la publicité d'une cyber-attaque réussie à l'encontre d'une entreprise peut porter atteinte à sa réputation et sa santé économique. Le règlement européen pour la protection des données personnelles (RGPD) change la donne, dès lors que les violations de données personnelles conduisent à une obligation de notification dans les 72h à la Commission nationale de l'informatique et des libertés (CNIL)[3].

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[4].

• Le brouillard statistique de la cybercriminalité

À l'absence de définition juridique de la cybercriminalité de laquelle découle une difficulté à déterminer un champ infractionnel précis, s'ajoute la dispersion des infractions concernées au sein de plusieurs catégories de natures de l'affaire (NATAFF)[5], ne permettant pas d'obtenir des données fines quant aux poursuites.

En effet, certaines infractions peuvent certes être identifiées par la nature de l'infraction (NATINF), permettant l'exploitation des données du casier judiciaire national, mais elles ne sauraient être isolées au stade des poursuites

Cas ukrainien (15$/jour – SMIC mensuel local 140$)

Source : Trustwave

(1) 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).

(2) La doctrine américaine est différente à cet égard, au vu de l'activisme récent du Department of Justice (DoJ).

(3) Voir le cas d'Airbus en janvier 2019.

(4) https://www.cybermalveillance.gouv.fr/

(5) « Nature de l'affaire » : codification utilisée lors de l'enregistrement au Bureau d'Ordre des tribunaux. L'enregistrement est en général fait par des agents du Bureau d'Ordre, et ne correspond pas à une qualification juridique fixée par un magistrat.

SUITE P.16 ...

dans la mesure où l'exploitation des données du SID[6]-Cassiopée[7] s'effectue principalement par le biais de la NATAFF, nomenclature d'enregistrement des procédures à l'arrivée au parquet[8].

La future plateforme THESEE[9] (projet porté par le Ministère de l'intérieur) est susceptible d'améliorer la connaissance statistique pour certains phénomènes de cybercriminalité. La récente loi de programmation pour la Justice (LPJ) insère d'ailleurs de nouvelles dispositions afin d'encadrer la plainte en ligne[10].

• Le phénomène du « going dark »[11], massif en cybercriminalité

La libéralisation du chiffrement a contribué à améliorer sensiblement le niveau global 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 pour le régime des interceptions judiciaires. De même, la généralisation du chiffrement de type *full disk* sur les terminaux informatiques, dont les ordiphones, a également rendu délicate l'exploitation forensique. Enfin, 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[12].

UNE ORGANISATION JUDICIAIRE EN QUÊTE DE MATURITÉ

Seront ici abordées l'organisation judiciaire actuelle ainsi que les relations des acteurs judiciaires avec les acteurs de la cybersécurité.

Constats sur l'organisation judiciaire actuelle

Sans pouvoir détailler ici les multiples compétences territoriales de l'autorité judiciaire en matière de cybercriminalité, il sera souligné 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 crime de sabotage informatiqu[13].

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 toutefois modestes[14]. 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[15].

Au-delà, les juridictions interrégionales spécialisées (JIRS) connaissent de plus en plus de contentieux de la cybercriminalité, notamment liée à la criminalité organisée[16]. Une réflexion est également en cours concernant la pratique des « cyber-référents » dans les tribunaux.

Relations des acteurs judiciaires avec les acteurs de la cybersécurité

La direction des affaires criminelles et des grâces (DACG), via la mission précitée, participe aux travaux stratégiques du Centre de coordination des crises Cyber (C4), instauré suite à la Revue stratégique de Cyberdéfense de février 2018[17].

La DACG fait également partie du conseil d'administration du groupement d'intérêt public ACYMA[18] (responsable du site internet cybermalveillance.gouv.fr), participe à plusieurs évènements de cybersécurité comme le Forum international de cybersécurité (FIC), et collabore à divers groupes de travail interministériels, en liaison avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

La bataille contre la cybercriminalité ne peut se gagner seule et tous les acteurs impliqués doivent joindre leur effort. Le levier judiciaire doit gagner en maturité mais des progrès récents sont à souligner. La coopération internationale est aussi un facteur clé de ce succès, avec l'aide d'entités telles qu'Europol, Eurojust et Interpol. Sur le plan de l'accès à la preuve numérique, les yeux sont désormais tournés vers Bruxelles où se jouent en ce moment les négociations des futurs textes européens « e-evidence » ■

+ POUR EN SAVOIR PLUS

→ Revue stratégique de Cyberdéfense : http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

→ Etat de la menace cyber (rapport DMISC 2018) : https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Etat-de-la-menace-liee-au-numerique-en-20182https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Etat-de-la-menace-liee-au-numerique-en-20182

→ Dispositif d'assistance aux victimes d'actes de malveillance : https://www.cybermalveillance.gouv.fr/

→ Plateforme PERCEV@L : https://www.service-public.fr/particuliers/vosdroits/R46526

(6) SID : Système d'information douanier

(7) Cassiopée : Chaine Applicative Supportant le Système d'Information Oriente Procédure pénale Et Enfants

(8) Seuls les postes NATAFF B81 *Entrée ou maintien irrégulier dans un système informatique* et B82 *Dégradation, destruction ou vol de données ou de fichiers informatiques*, correspondant aux atteintes aux STAD, sont susceptibles d'être exploités utilement, mais renvoient à une acception extrêmement étroite de la cybercriminalité.

(9) THESEE : Traitement harmonisé des enquêtes et des signalements d'e-escroqueries

(10) Nouvel article 15-3-1 du code de procédure pénale.

(11) 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.

(12) Voir le lancement du réseau Telegram Open Network (TON) et la cryptomonnaie Gram par l'entreprise TELEGRAM, annoncé pour le dernier trimestre 2019, suite à une levée de fonds de 1,7 milliards de dollars.

(13) Nouvel art. 706-72-1 C. proc. pén.

(14) Actuellement deux magistrats, ainsi qu'un assistant spécialisé et un greffier.

(15) Dépêches 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».

(16) Ex : le démantèlement de la Main noire, une plateforme du Darknet.

(17) http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

(18) ACYMA : Action contre la cybermalveillance

ARTICLES ET CONFÉRENCES

Conférences

« *Going dark, going Cyber ? Enjeux et défis de la cybercriminalité et de l'accès aux données* »
16 mars 2018 - Conférence Data Institute de l'université de Grenoble Alpes
→ http://www.msh-alpes.fr/en/going-dark-going-cyber-enjeux-defis-cybercriminalite-acces-aux-donnees

« *Cloud Act, E-Evidence and Cross Border Access to Data* »
Conférence au Forum International de Cybersécurité (FIC 2019).
→ https://www.forum-fic.com/Data/Sites/16/fichiers/ARTOIS-A08-CloudAct.pdf?ts=1549558034

« *L'impact du chiffrement informatique dans les enquêtes pénales* »
Conférence AFDIT Sud-Est 2018, 4ème édition des journées du numériques
→ https://afdit-sud-est.com/videos-2018/

« *Actualités dans la preuve numérique à l'heure du Cloud* »,
Conférence organisée par le Parquet général d'Aix en Provence, 1er juin 2018

Articles parus ou en cours de publication

Article relatif à la conférence précitée du 1er juin 2018 d'Aix-en-Provence, dans la revue Dalloz IP/IT [en cours de publication]

Article relatif aux conséquences du RGPD au sein du ministère de la justice, dans la revue Dalloz IP/IT [en cours de publication]

Actes du séminaire « Cryptoactifs » organisé le 1er février 2019 (voir infra), revue Dalloz IP/IT [en cours de publication]

« *Les implications juridiques et technologiques post Safe Harbour* »Revue de la gendarmerie nationale, décembre 2016 (p14-20)
→ https://en.calameo.com/read/00271929281c96342ba48

Organisation de séminaire

« *Les Cryptoactifs : la justice pénale à l'épreuve des cryptomonnaies* »,
1er février 2019 (public de 150 personnes, organisation fermée et réservée à des acteurs régaliens)

« *Nanotechnologies, biotechnologies, informatiques et sciences cognitives (NBIC) : généalogie des enjeux de sécurité et de justice* »
Co-organisé avec l'Institut National des Hautes Etudes de Sécurité et de Justice (INHESJ) à l'automne 2017
→ voir p5 https://inhesj.fr/sites/default/files/RA_2017_INHESJ_2017ok.pdf