Nouveaux rôle et enjeux pour l'État dans la lutte contre la cybercriminalité

Par **Thierry DELVILLE**
PricewaterhouseCoopers (PwC)

La cybersécurité est devenue une préoccupation centrale des dirigeants, qu'il s'agisse des responsables publics ou des dirigeants d'entreprises. Sur les trois dernières années, les chiffres observés à travers des sondages réguliers classent entre la troisième et la cinquième position la cybersécurité au rang des sources d'inquiétude majeures à côté du terrorisme, de l'incertitude géopolitique, de l'augmentation des régulations ou encore des changements climatiques [(1)].

Voilà bientôt quarante-cinq ans qu'un premier virus informatique [(2)] a été identifié sur ce qui n'était pas encore le réseau Internet. Aujourd'hui, l'hyperconnexion, la transformation digitale de l'économie et de la société en général, font du cyberespace le cinquième champ de conflictualité sur lequel sont engagées désormais la plupart des grandes armées.

Les activités criminelles bénéficient également, dans cette nouvelle dimension, d'un contexte très favorable en raison d'une sociologie propre à la cybercriminalité : absence de frontière, population criminelle qui évolue et se diversifie, passant de la recherche du profit facile à des activités mieux préparées et ciblées en y consacrant des moyens plus élaborés. L'espionnage et l'ingérence au profit d'organisations privées voire d'États complices ou donneurs d'ordres perdurent et cristallisent une véritable « cyber guerre froide ». Tout cela est de nature à motiver le passage à l'acte dont le retour sur investissement est bien plus rémunérateur que dans le champ de la délinquance « non cyber ».

Pour lutter contre la cybercriminalité, pour investiguer, pour juger les auteurs interpellés, l'État demeure un acteur central, dans son rôle de protecteur des droits fondamentaux et des libertés individuelles, mais il apparaît de plus en plus évident que mener à bien cette mission appelle d'autres modalités de travail et d'interventions.

Mieux connaître la menace et sa progression

Dans un rapport de 2014 [(3)], une mission interministérielle dirigée par le procureur général Marc Robert avait considéré que la cybercriminalité apparaissait comme une « nébuleuse d'autant plus difficile à cerner qu'elle renvoie à des procédés techniques essentiellement évolutifs maîtrisés par les seuls initiés et que peinent à cerner les dispositifs statistiques traditionnels ». S'inspirant des multiples définitions d'origines nationales et internationales, dont aucune ne répondait à la dimension pédagogique de compréhension partagée du phénomène, il avait suggéré cette définition générique : « La cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication, principalement Internet. »

Connaître la réalité du phénomène constitue en effet un besoin préalable pour évaluer la réalité d'une menace et son évolution. « Si tu ne connais ni ton adversaire ni toi-même, à chaque bataille tu seras vaincu », écrit Sun Tzu dans *L'Art de la guerre*. Connaître la réalité de la cybercriminalité malgré l'absence de définition juridique précise représente à ce titre un défi essentiel. Dans son

(1) https://www.pwc.com/gx/en/ceo-survey/2019/report/pwc-22nd-annual-global-ceo-survey.pdf
(2) Lancé en 1971 sur le réseau Arpanet sous le nom de *Creeper*.
(3) https://www.ladocumentationfrancaise.fr/rapports-publics/144000372/

rapport de 2019, le ministère de l'Intérieur rappelle une nouvelle fois la difficulté d'établir une vision consolidée reposant sur les statistiques dans son rapport sur « l'état de la menace liée au numérique en 2019 [4] ».

La construction d'une vision partagée est à encourager. La connaissance de cette « topographie cybercriminelle » à l'échelle nationale nécessite l'agrégation de données multiples que seule une vision élargie, au-delà de celle des services institutionnels, permettra d'obtenir. S'il est d'usage de qualifier de « chiffre noir » de la délinquance les faits de crimes ou délits non signalés aux autorités, nombre d'experts qualifient de « trou noir » la part de ces mêmes faits commis dans l'espace cyber.

Un cadre réglementaire impose à certaines catégories de victimes d'informer l'ANSSI (Agence nationale de la Sécurité des Systèmes d'Information) dont le rôle de régulateur interministériel s'est renforcé ces dernières années. Ainsi, après la Loi de programmation militaire 2013-2019 et la directive NIS, les OIV et OSE [5] constituent autant d'entreprises stratégiques sur lesquelles reposent des obligations d'équipement et d'information des autorités en cas d'incidents. Les autres entreprises, moins sensibles, ne sont pas soumises à ces obligations.

Ces règles ne créent pas *de facto* d'obligation de déposer plainte ni d'ouvrir une enquête pénale. La poursuite des infractions repose également sur la bonne synergie entre les services de l'État (à vocation technique et à vocation judiciaire) et sur la volonté des victimes qui craignent encore trop souvent pour leur réputation voire d'éventuelles sanctions [6].

Encourager le dépôt de plainte à travers de nouveaux outils [7] et une forte sensibilisation de l'ensemble des acteurs, systématiser les échanges croisés au sein des services de l'État, bâtir les conditions d'un recueil plus large notamment avec le secteur privé permettront d'établir une mesure de suivi pérenne et exhaustive de la cybercriminalité.

Mieux connaître pour mieux prévenir

Si la connaissance des faits et le partage d'informations constituent un point-clé dans la mise en place d'un dispositif de lutte efficace, pour l'État, agir efficacement, c'est avant tout mieux prévenir, sensibiliser, informer.

L'identification des menaces et des réponses techniques est partagée sous l'impulsion de l'ANSSI par le réseau des CERT [8] qui constitue un appui technique essentiel pour les professionnels experts, mais le dispositif n'est pas diffusé au-delà de cette communauté. Combien, sur les trois millions d'entreprises en France, s'appuient sur cette base de connaissance ?

D'autres initiatives majeures ont vu le jour ces dernières années telles que la plateforme cybermalveillance.gouv.fr qui recense les incidents dont ont été victimes les entreprises ou les particuliers avant de mettre ces derniers en contact avec des techniciens référencés sur le site. Ce groupement d'intérêt public (GIP) diffuse aussi *via* les réseaux sociaux de nombreuses informations et messages d'alertes. Également d'autres actions sont à signaler : e-enfance (sur le cyberharcèlement), stop-jihadisme (pour la propagande en ligne), Perceval (pour signaler les escroqueries à la carte bancaire) sans oublier la plateforme Pharos qui recense les signalements de contenus illicites depuis bientôt dix ans.

(4) https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019
(5) Opérateur d'importance vitale et Opérateur de service essentiel.
(6) Le fait de ne pas s'être signalé comme victime d'un vol de données peut valoir très cher au sens de la réglementation RGPD avec des sanctions possibles jusqu'à 2 % du chiffre d'affaires (article 83.4 RGPD).
(7) https://www.interieur.gouv.fr/Archives/Archives-ministres-de-l-Interieur/Archives-Gerard-Collomb-mai-2017-octobre-2018/Communiques-du-ministre/Ouverture-de-la-plateforme-Percev-l-Signalement-des-fraudes-a-la-carte-bancaire
(8) https://www.cert.ssi.gouv.fr/

Les moyens de la prévention s'organisent mais il est essentiel de voir plus loin et d'organiser l'effort collectif de diffusion de la connaissance :

- développer le retour d'expérience des entreprises touchées en le faisant au plan sectoriel pour aller plus loin dans l'actualisation de l'évolution des menaces ;
- encourager le retour d'expérience avec les prestataires certifiés sous l'autorité de l'ANSSI et des autres services de l'État pour informer sur l'apparition de nouvelles menaces et de nouveaux *modus operandi* ;
- développer de nouvelles pratiques et méthodes pour se préparer aux attaques de plus en plus massives et systémiques.

Beaucoup a déjà été fait et il en reste bien davantage à faire !

Quels moyens pour mieux lutter contre la cybercriminalité ?

Faut-il considérer avec Myriam Quemener [(9)] que « le droit s'épuise à poursuivre la preuve numérique dont les frontières s'échappent toujours plus loin » ? Incontestablement le législateur ne cesse de courir après les nouveaux risques numériques. Sur ces trois dernières années, sont ainsi intervenus des textes réprimant (liste non exhaustive) le cyberharcèlement, le *revenge porn,* la provocation au suicide. Tout récemment la loi PACTE [(10)] introduit des règles visant à lutter contre les nouvelles fraudes apparues avec les levées de fonds à partir de monnaies virtuelles (ICO). Cette adaptation permanente aux nouvelles pratiques numériques et la nécessité de créer de nouvelles incriminations ne devrait pas cesser dans les années à venir.

Les moyens et techniques d'enquête se développent également : l'offre *digital forensic* s'est transformée et des avancées importantes ont pu être réalisées en matière d'interception, de géolocalisation et d'exploitation des données de masse que ne manquent pas de récupérer les enquêteurs lors des perquisitions faites sur les lieux d'affaires retentissantes (par exemple dans le cadre des attentats de 2015). Cette évolution profite, pour partie, également aux prestataires privés qui interviennent en cas de crise ou remédiation de crise.

Parmi les attentes en termes d'évolution du droit, il faut souligner les nouveaux enjeux que constituent la conservation des données (après l'arrêt Télé2 de décembre 2016 de la CJUE), les moyens pour les enquêteurs de contourner les techniques d'anonymisation ou encore l'accélération de l'accès transfrontalier aux données. L'essentiel de ces points se situe dans une dimension que le droit national seul ne peut résoudre.

L'essentiel des enjeux de lutte contre la cybercriminalité est adressé à l'échelle internationale. La capacité grandissante d'Europol avec la création en 2013 de l'European Cybercrime Centre (EC3 [(11)]), illustré par exemple par son action dans la gestion des contenus illicites sur Internet avec la création de la plateforme européenne IRU, les nombreux textes de la commission (la directive NIS, RGPD), le Cyberact [(12)], le renforcement du rôle de l'ENISA dans la certification des solutions de confiance à l'échelle européenne, toutes ces avancées traduisent bien l'idée que l'avenir de la lutte contre la cybercriminalité passe par l'Europe et, au-delà, par le développement d'initiatives d'envergure internationale.

La politique pénale doit également gagner en visibilité, par le nombre de magistrats formés et spécialisés en premier lieu, mais aussi se traduire par des sanctions qui reflètent la gravité du

(9) *Le Droit face à la disruption numérique*, Éditions Gualino, avril 2018.
(10) https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France
(11) https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
(12) https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_fr

phénomène et sortent la cybercriminalité d'une perception quelque peu anecdotique. Sans répliquer les sanctions très fortes voire définitives infligées aux États-Unis [13], il importe que l'exemplarité de la sanction infligée par la justice pour les actes de cybercriminalité les plus graves soit posée.

Les acteurs de plus en plus nombreux de la lutte contre le cybercrime

La France a pris assez tôt conscience de l'importance du sujet que ce soit pour légiférer ou pour organiser la première forme de sa riposte. Dès 1994, la Préfecture de Police créait un service d'enquête en charge des fraudes aux technologies de l'information (la BEFTI), peu après, la police et la gendarmerie créaient les structures qui aujourd'hui encore (OCLCTIC, C3N) représentent des pôles d'expertise reconnus à l'échelle internationale, capables d'investiguer sous le contrôle de quelques magistrats spécialisés. D'autres services d'enquête des douanes ou encore Tracfin se sont au fil des années dotés d'équipes dédiées.

Du côté de la justice, la désignation de magistrats référents, la création d'une section spécialisée chargée des faits de cybercriminalité à Paris (Section F1 du parquet de Paris) et la mise en place des JIRS en province sont autant de réponses à cette évolution. La création d'un parquet spécialisé de type PNF ou PNAT représenterait un palier supplémentaire pour une réponse judiciaire mieux adaptée.

D'autres acteurs étatiques interviennent dans le champ de la cybercriminalité. L'ANSSI décrit sur son site Internet la cybercriminalité en ces termes : « La cybercriminalité est un vaste sujet qui concerne en premier lieu les ministères de l'Intérieur et de la Justice, en étroite collaboration avec l'ANSSI. » Le rôle central de cette agence est un fait incontesté et son expertise technique en fait aussi un atout essentiel pour tout ce qui relève de la détection des menaces et de l'analyse des incidents. Les services de renseignement jouent également un rôle essentiel dans cette lutte. La DGSI dispose du pouvoir d'enquête judiciaire pour les attaques mettant en jeu des entreprises ou des cibles relevant de la défense des intérêts vitaux ou stratégiques de la nation.

La « Revue stratégique de cyberdéfense [14] » de 2018 recommande que soit permise la mise en place d'un échange croisé de données techniques entre les experts techniques de la cyberdéfense (l'ANSSI, mais aussi le COMCYBER du ministère de la Défense, et la DGSE) et les enquêteurs en cybercriminalité.

La dimension hybride des attaques cyber où le monde criminel peut côtoyer le renseignement et celui de la défense, donne une perspective particulière au traitement diplomatique de certains faits. Les événements marquants qu'ont été des attaques comme *WannaCry* ou *NotPetya*, d'autres affaires outre-Atlantique ou plus près de nous aux Pays-Bas [15], ont montré une évolution dans les postures diplomatiques et judiciaires avec la désignation d'individus ou d'États criminels supposés [16] (notamment la pratique du *name and shame)* mais également de compagnies insuffisamment protégées et potentielles victimes.

Autres acteurs, et non des moindres, dans cette lutte, les prestataires privés sont particulièrement impliqués dans les phases de prévention mais également celles de remédiation. Ils sont au cœur des crises traversées par la plupart des victimes de cyberattaques et leur identification comme des

(13) https://en.wikipedia.org/wiki/Ross_Ulbricht
(14) http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/
(15) https://www.huffingtonpost.fr/2018/10/04/derriere-laffaire-de-la-cyberattaque-aux-pays-bas-le-puissant-grule-service-de-renseignement-militaire-russe_a_23551536/
(16) https://www.theguardian.com/politics/2018/may/23/uk-threatens-to-name-and-shame-state-backers-of-cyber-attacks

acteurs de confiance repose de plus en plus fréquemment sur des labels ou des certifications. L'État se doit d'avoir vis-à-vis de cette expertise une action en profondeur allant de l'information la plus précise possible (dans les deux sens) pour déjouer les menaces en cours, à l'exercice de son pouvoir de contrôle en cas de dérives ou d'insuffisances avérées. L'animation de cet écosystème d'experts est inévitable, c'est un enjeu de filière mais aussi de souveraineté.

Se préparer aux nouveaux défis du cyber dans une dimension élargie

L'histoire de la cybercriminalité s'écrira encore longtemps et de nombreux textes nationaux interviendront pour répondre aux limites du travail des enquêteurs, accentuer le rôle de vigilance et la responsabilité des opérateurs, incriminer de nouvelles pratiques…

La lutte contre le crime dans les environnements digitaux futurs reposera sur des moyens consacrés à la recherche, à la prospective et à l'innovation. Peu avant le dernier sommet du G7 à Biarritz, la nouvelle responsable d'EUROPOL, Catherine de Bolle, soulignait que l'arrivée de la communication 5G et les nouveaux enjeux liés aux IoT ou à l'IA constituaient autant d'avancées qui remettent en cause les capacités des services d'enquête, qu'il s'agisse d'interception ou de techniques d'investigation.

Au-delà des nouveaux outils et des nouveaux enjeux, c'est bien dans le champ des nouvelles régulations internationales qu'il conviendra d'être présent. Le traité de Budapest, acte fondateur de l'entraide internationale dans cette lutte, date de 2001 et n'est toujours ratifié que par une cinquantaine d'États. L'appel de Paris du président de la République, en novembre 2018, pour la confiance et la sécurité dans le cyberespace ne rencontre pas d'écho de la Chine, des États-Unis ou de la Russie… L'enjeu demeure, comme cela a été rappelé au sommet du G7 de Biarritz en août 2019, de travailler mieux ensemble… Mais de l'intention aux actes, il y a encore du chemin.

Le rôle de l'État sera central dans les années à venir pour lutter contre la cybercriminalité mais il ne se jouera plus, comme par le passé, avec une séparation nette entre le régalien d'un côté et l'expertise de l'autre. La lutte contre le crime dans le numérique se jouera dans un réseau où le partage de l'information deviendra une vertu cardinale. Sensibiliser, prévenir, partager : telles sont et seront plus encore demain les clés à réunir pour lutter à armes, si ce n'est égales à tout le moins comparables, avec des criminels pour qui ces valeurs sont déjà bien intégrées.