Perspectives de la cybercriminalité des dix à vingt prochaines années

Par Éric FREYSSINET
Officier général de gendarmerie

La cybercriminalité doit être vue comme un phénomène en perpétuel mouvement, qui s'adapte aux technologies et aux usages, et qui s'approprie les défenses que met en place la société, les acteurs de la cybersécurité et bien entendu les autorités judiciaires les pourchassant. L'action des cybercriminels est sous-tendue par des mouvements de fond : motivations essentiellement financières, recettes qui fonctionnent dans la durée, mais il faut se tenir parés aux évolutions des années à venir qui pourraient encore bouleverser les approches de prévention et de lutte. Explorons les perspectives de la cybercriminalité des dix à vingt prochaines années.

En 2008, je m'étais prêté à l'exercice proposé par France 2025 dans le champ de la cybercriminalité en rédigeant un article prospectif[1] sur son évolution, notre réponse et notre niveau de préparation. Mes conclusions étaient alors essentiellement basées sur la perspective d'une omniprésence des outils de communication numérique dans les usages des délinquants de tout poil, des structures cybercriminelles se coordonnant par-delà les frontières et la généralisation de techniques anti-forensiques, c'est-à-dire de méthodes permettant de rendre les traces numériques plus difficiles à découvrir ou exploiter. Par ailleurs, je mettais en avant l'idée que tout développement technologique, tout nouveau service ou produit, serait en permanence la cible des cybercriminels.

Tout cela s'est évidemment concrétisé d'une façon ou d'une autre. Surtout, cela s'est traduit par les comportements que tout le monde connaît, tels le vol de données et l'extorsion par rançongiciels. L'un des éléments clés est maintenant devenu une réalité dans le quotidien de tous les enquêteurs et magistrats : plus une seule enquête judiciaire n'ignore les outils numériques qui sont omniprésents, mais surtout les délinquants les maîtrisent de mieux en mieux. S'agissant de la cybercriminalité en particulier, les tendances de fond persistent et vont se poursuivre dans les années qui viennent.

Nouvelles technologies, nouveaux usages, nouvelles opportunités…

La tendance de fond principale, qui doit guider tous les observateurs des menaces numériques, est bien celle-là : tout nouveau produit, tout nouveau service, toute nouvelle technologie seront l'objet immédiat de l'attention des cybercriminels. Cette recommandation d'attention est évidemment valable pour tous ceux qui lancent un nouveau produit ou

[1] https://eric.freyssi.net/2008/10/30/faire-face-nouveaux-defis-delinquance-numerique/

service numérique : il est indispensable d'intégrer dans sa conception et dans le plan d'accompagnement une véritable attention aux risques que font peser les acteurs externes, et notamment les délinquants numériques.

Trop souvent, ce conseil n'est pas suivi et le marché est envahi d'objets connectés, de plateformes en ligne, de nouveaux moyens de paiement électroniques pour lesquels les risques numériques n'ont pas été pris en compte ou ont été sous-évalués. Cet enjeu semble avoir enfin été pris en compte avec la perspective d'un nouveau règlement européen, dont les travaux sont lancés en cet automne 2022, le "Cyber Resilience Act"[2], qui promeut une vraie politique de sécurité et de suivi des vulnérabilités pour les produits et services numériques, sous la responsabilité de toute la chaîne d'acteurs, depuis l'éditeur jusqu'au distributeur.

Si l'on se projette dans les années qui viennent, les nouveautés restent de bons indicateurs de ce qu'il faut observer comme source de nouvelles menaces. Ainsi, dans les années à venir, les dispositifs numériques liés aux mobilités seront l'objet de toutes les attentions : conduite autonome ou assistée, chargement électrique des véhicules, systèmes de transport intelligents avec leur lot d'interfaces de communication entre les véhicules et les infrastructures routières.

Les scénarios sont multiples et doivent être évalués à l'aune des risques qu'ils font porter sur l'intégrité physique des personnes, et bien entendu sur leur vie privée (tout en prenant en compte la vie « privée » des entreprises au travers de l'activité de leurs employés). La spécificité des moyens de transport est peut-être leur impact sur la vie quotidienne des personnes et des communautés. On notera ici que ce sont des objets et des usages qui nous apportent potentiellement des bénéfices par plus de sécurité sur les routes, plus de fluidité dans les déplacements, un meilleur respect de l'environnement, mais ces mêmes solutions sont aussi porteuses de risques nouveaux.

Un autre exemple de « nouveauté », ou en tous cas d'usage émergent, sera peut-être celui des métavers. Il s'agit de plateformes permettant des interactions dans un espace représenté en deux ou trois dimensions, au travers non seulement de pseudonymes mais aussi d'avatars qui interagissent entre eux et avec les objets de l'environnement. Aussi, même si les plateformes de réseaux sociaux existent sous différentes formes depuis le début des années 2000, leur intérêt croissant pour ces modalités avancées d'interaction apportera peut-être, par une généralisation de leur usage, un cortège de nouveaux risques, et en tous cas une attention plus grande des cybercriminels. La préexistence de plateformes telles que Second Life aura permis d'observer déjà une partie des risques potentiels.

Aucun de ces risques n'apparaît comme réellement nouveau par sa nature : harcèlement ou même agression sexuelle numérique, vol de biens numériques (monnaies virtuelles ou objets numériques). Mais c'est peut-être la nature même de ces plateformes qui rendra plus difficiles le contrôle de ces pratiques ou l'identification des auteurs : les échanges y sont hautement volatils et laissent peu de traces (contrairement aux réseaux sociaux qui nécessitent une certaine permanence des publications pour leur fonctionnement), et les protocoles envisagés prévoient une réelle décentralisation, donc une multiplication des serveurs sur lesquels ces interactions sont susceptibles de se réaliser (contrairement au modèle très centralisé des réseaux sociaux dominants actuels).

Cela veut dire aussi qu'il faudra peut-être adapter les outils, et surtout les méthodes de ceux qui sont chargés de nous protéger, pour s'adapter à ces nouveaux environnements :

[2] https://digital-strategy.ec.europa.eu/fr/library/cyber-resilience-act

former les spécialistes de la sécurité routière à la sécurité numérique et les doter de nouveaux outils pour collecter les traces des infractions, s'associer à des spécialistes de la cybercriminalité ; et demain, patrouiller les espaces virtuels en évolution permanente, et non plus seulement les appréhender comme des espaces de publication.

Vers la fin des rançongiciels… et après ?

Nous l'évoquions plus haut, les rançongiciels chiffrants, modalité la plus aboutie aujourd'hui des extorsions numériques, sont devenus la forme plus visible et peut-être la plus profitable de la délinquance numérique sur Internet. Tout d'abord, cette pratique ne doit pas masquer une réalité beaucoup plus variée (hameçonnage, détournement de comptes numériques, fraude au virement électronique), et surtout la menace universelle du détournement de données confidentielles ou personnelles, détournement qui est même le préalable à l'installation d'un rançongiciel, voire qui vient compléter la stratégie d'extorsion, les délinquants menaçant de publier ces données.

On peut sans hésiter se convaincre qu'un jour ou l'autre, la méthode d'extorsion par rançongiciel chiffrant disparaîtra progressivement, car on peut avoir l'espoir que les stratégies de protection finiront par payer – cloisonnement des réseaux et contrôle renforcé de l'accès aux données, gestion des sauvegardes, meilleure capacité de détection des intrusions dans les réseaux et sur les postes de travail, etc. Mais ce dont on doit rester tout autant convaincus est que les délinquants développeront de nouvelles stratégies tout aussi lucratives, ne serait-ce que pour les raisons évoquées dans la section précédente sur le développement de nouveaux produits, services et usages numériques.

Les nouvelles stratégies qui s'imposeront chez les cybercriminels reposeront sur plusieurs caractéristiques : répartition des tâches (et donc des risques), scalabilité (c'est-à-dire la capacité à exploiter un grand nombre de victimes), efficacité dans la durée (reposant sur des usages suffisamment généralisés, comme l'est le stockage de fichiers sur des ordinateurs et des serveurs partagés, connectés à Internet).

On peut par exemple imaginer que l'extorsion puisse porter par exemple sur l'intégrité des données – donc dans la confiance que l'on peut avoir en leur utilisation. Ou encore, les délinquants pourraient cibler des objets numériques contenant peu de données, mais indispensables à la vie des organisations ou des territoires. Une autre stratégie pourrait consister à exfiltrer de façon la plus discrète possible de très grands volumes de données, et menacer de les révéler au moment d'événements financiers importants. Il est en tous cas certain que quoi que l'on fasse pour se protéger, la tentation restera toujours trop grande pour les délinquants numériques.

Il est possible aussi que les équilibres se déplacent vers d'autres formes de détournements plus immédiatement lucratifs. Ainsi, la généralisation des échanges sous forme de monnaies électroniques de plus en plus interopérables, reposant ou non sur des technologies de type « chaîne de blocs », notamment dans des pays émergents sur tous les continents, pourrait amener un attrait croissant des cybercriminels. Nous reviendrions ainsi à une délinquance qui a marqué les années 1990 et le début des années 2000, avec l'essor du *carding* (copie et revente de données de cartes bancaires), mais profitant des faiblesses de ces nombreux systèmes nouveaux.

Il est vraisemblable que les deux tendances de fond que nous venons d'évoquer vont cohabiter. Mais c'est peut-être dans l'organisation même des cybercriminels que les inquiétudes les plus importantes sont à soulever.

Nouvelles organisations cybercriminelles : vers des pseudo-États ?

En effet, c'est avant tout la capacité des délinquants numériques à se jouer des frontières physiques – en réalité de toutes les frontières techniques et organisationnelles[3] – qui constitue peut-être l'évolution la plus préoccupante, car elle met en lumière les difficultés subsistant en matière de coopération, renforcées par les tensions internationales.

L'offensive russe de mars 2022 en Ukraine en a apporté une illustration importante. De fait, de nombreux groupes criminels agissaient alors depuis ce territoire et la coopération internationale commençait à porter ses fruits avec plusieurs opérations judiciaires sur le territoire ukrainien. Le conflit a porté un frein à ces actions, et – l'avenir nous le dira certainement – les délinquants se sont peut-être dispersés vers d'autres territoires, depuis lesquels ils peuvent toujours agir.

En réalité, une des frontières les plus complexes à envisager est celle qui existe entre les acteurs de la délinquance numérique : les mêmes personnes peuvent participer à plusieurs groupes, ils se rendent ou se vendent des services les uns aux autres, dans des relations croisées dans toutes les directions, et parfois les motivations peuvent être difficiles à déterminer entre ceux qui sont uniquement motivés par l'appât du gain et ceux qui travaillent au profit d'un État étranger.

Mais, comme je l'évoquais en septembre 2020 dans cette même revue[4] : « L'une des tendances de fond qui semble se construire petit à petit est la possibilité, voire l'ambition, pour certains délinquants numériques de créer petit à petit leurs propres territoires autonomes dans l'espace numérique. » Ils ont par exemple souvent besoin d'un support juridique traditionnel pour une partie de leurs activités, comme la création d'une entreprise, le recrutement de personnels et le paiement de salaires. La libéralisation croissante des échanges, l'acceptabilité de plus en plus grande du télétravail rendent de plus en plus fluides ces modèles économiques.

Comme je l'évoquais dans le même article, l'essor des cryptomonnaies a permis des échanges plutôt stables avec des monnaies virtuelles sans aucun contrôle d'une quelconque autorité nationale ou supranationale. Mais ce sont peut-être d'autres évolutions qui apporteront les derniers outils ou de nouvelles opportunités à cette indépendance numérique des groupes cybercriminels : des nouveaux marchés de l'énergie portés par la crise des combustibles fossiles, les flux migratoires liés à la crise climatique ou encore de nouveaux acteurs dans la fabrication des composants électroniques. Autrement dit, les modifications des flux d'informations, des modes d'approvisionnement en biens numériques essentiels et les mouvements des personnes sont autant de possibilités pour les groupes criminels de camoufler différemment ou de façon encore plus forte leurs activités et leurs trafics.

Ce qui sera intéressant à observer, c'est peut-être la façon dont ils vont chercher petit à petit à créer plus de confiance au sein de leur propre écosystème. En effet, de nombreuses opérations judiciaires, les observations et publications des chercheurs en cybersécurité ont mis à mal la confiance que les cybercriminels pouvaient avoir dans leurs moyens de communication chiffrée (démantèlement de plateformes de messagerie instantanée comme Encrochat) ou d'infiltration dans des places de marché cybercriminels.

[3] « Appréhension des cybermenaces en 2017 : de la cybercriminalité à la cyberdéfense », *Revue de la défense nationale*, 2017/10, n°805, pp. 82-86, https://www.cairn.info/revue-defense-nationale-2017-10-page-82.htm

[4] « Les menaces numériques du XXIe siècle : de l'escroc qui se joue des frontières aux futurs territoires autonomes cybercriminels », *Enjeux numériques*, n°11, septembre 2020, pp. 35-39.

Ainsi, on peut imaginer des modèles de confiance où l'information validée serait stockée de façon sécurisée, mais anonymisée dans des *blockchains*, donnant une certaine reconnaissance de la valeur d'un acteur cybercriminel sans identifier précisément les personnes qui l'ont certifié. De même, on pourrait imaginer qu'ils y stockent la propriété de certains avoirs numériques ou matériels. Ce sont ces briques technologiques, au départ pensées pour bénéficier au plus grand nombre, qui pourraient finalement se révéler utilisées de façon encore plus massive chez les cybercriminels, pour échapper à la régulation des États traditionnels. Il faudra une réponse technique, mais aussi juridique, qui préserve l'innovation et les libertés tout en permettant les contrôles.

Conclusion

Plus de trente ans d'évolution de la cybercriminalité nous ont d'abord appris qu'elle ne pouvait pour l'instant que se développer, ne serait-ce que grâce à l'essor des technologies et de leurs usages dans une population sans cesse croissante. Le principal moteur de cette évolution est justement dans les nouveaux produits, les nouveaux usages et les nouveaux services numériques. La tendance de fond reste l'appropriation frauduleuse du bien d'autrui pour s'enrichir, sous une forme ou sous une autre, sans toutefois que l'on puisse nier le risque pour l'intégrité physique des personnes, les outils numériques ayant une importance croissante dans la vie de tous les jours, les transports, la protection des bâtiments ou des territoires, ou encore la santé.

Toutefois, l'évolution la plus importante dans les années qui viennent est la nécessité pour les délinquants numériques de se protéger de plus en plus, et donc de développer des stratégies leur permettant d'être plus discrets ou en tous cas plus difficiles à identifier et surtout à interpeller. C'est peut-être dans ce domaine que l'on verra les plus grandes innovations. Pour lutter contre cette tendance, il faudra à la fois innover, prévenir, mais aussi inventer des nouvelles régulations qui, tout en préservant les droits individuels et collectifs, permettent d'en maîtriser les abus.