Les menaces numériques du XXIe siècle : de l'escroc qui se joue des frontières aux futurs territoires autonomes cybercriminels

Par le Colonel **Éric FREYSSINET**
Chef du Pôle national de lutte contre les cybermenaces
Direction générale de la Gendarmerie nationale

Cybercriminalité et territoires

Les moyens de télécommunications – et encore plus Internet – ont été pensés pour abolir les frontières, rapprocher les individus, les organisations et les peuples. La réalité technique et juridique est toute autre, et il convient de les penser comme des juxtapositions et interconnexions de territoires numériques (Freyssinet, 2017), aux règles locales sur lesquelles viennent se greffer les contraintes des territoires. En termes de sécurité numérique, on cherchera à préserver chaque système d'information, chaque sphère informationnelle personnelle contre les regards indiscrets, les assauts des cybercriminels ou des États-voyous. On cherche donc à reconstruire, dans ce monde par nature ouvert, un territoire à protéger et des frontières à surveiller.

Protéger son territoire numérique

Pour être en mesure de protéger son territoire numérique, il s'agit, évidemment, d'abord de le définir de façon précise et exhaustive. La première difficulté de l'usager numérique, de l'entreprise, de toute organisation possédant un patrimoine informationnel à sécuriser (et nous en possédons tous aujourd'hui) est d'en dresser les contours : quelles sont les données et les systèmes d'information que je dois protéger et où sont-ils situés ?

S'agissant des données, on peut les classer en plusieurs catégories : les données que l'on crée, les données que l'on acquière et les données créées ou acquises par d'autres et qui nous concernent directement.

Le dernier bloc est souvent plus difficile à cerner ou à maîtriser, mais, par exemple, il s'agira pour un individu de l'ensemble des informations que possède une plateforme de réseau social sur nos activités et interactions avec ce service. Pour une entreprise, une collectivité, une administration, ce sont par exemple les plans d'un architecte pour des locaux que l'on souhaite construire, ou les données qu'un fournisseur a collectées au fur et à mesure des échanges ou des transactions.

Ces données peuvent ensuite être classées en fonction de leur sensibilité selon différents critères comme la confidentialité, les exigences de disponibilité ou la préservation de leur intégrité dans le temps.

Cette approche par les données permet d'éviter l'écueil de l'approche matérielle reposant uniquement sur ses propres systèmes d'information. Ainsi, non seulement devons-nous prendre en compte la sécurité des systèmes d'information que l'on possède, mais aussi de tous ceux qui contiennent ou traitent nos données.

Chacun peut ainsi définir son territoire numérique comme l'ensemble des systèmes d'information que l'on possède ou qui contiennent ou traitent des données de son patrimoine informationnel.

Au passage, cela veut dire qu'une partie non négligeable de son territoire numérique peut être partagé avec d'autres personnes, chacun ayant un rôle différent ou complémentaire (comme un propriétaire, un locataire, un syndic dans un immeuble en co-propriété). Cela veut aussi dire que son territoire numérique n'est pas uniquement localisé dans un lieu que l'on possède ou que l'on loue, mais peut aussi recouvrir d'autres lieux, y compris dans plusieurs pays.

Les responsabilités des uns et des autres peuvent être fixées par l'usage, la simple convention, le contrat ou le droit. S'agissant du droit, on peut citer, par exemple, la notion de responsable de traitement en matière de données à caractère personnel – dont on rappelle que le Règlement général sur la protection des données de l'Union européenne prévoit qu'il puisse partager ses responsabilités avec son sous-traitant ; le droit a donc bien pris en compte la complexité de la définition d'un territoire numérique.

Si l'on prend un peu de recul, cela veut dire que pour un État, son territoire numérique – celui dont il est chargé d'assurer d'une façon ou d'une autre la sécurité – s'étend bien au-delà de ses frontières terrestres, partout où se trouvent les territoires numériques de ses citoyens, de ses entreprises. Très concrètement, cela veut dire que la justice française est chargée de protéger les données de ses usagers, qu'elles soient hébergées à Roubaix ou dans la Silicon Valley.

Quelles conséquences pour les personnes et les autorités chargées d'assurer la sécurité des territoires numériques ?

Pour les personnes, les entreprises et leurs responsables de la sécurité des systèmes d'information, on a vu que c'est souvent le contrat qui va leur permettre de s'assurer des moyens de sécuriser leur territoire numérique. Cela n'ira pas forcément sans difficulté dans un monde où le marché permet de faire appel à des prestataires sous différentes juridictions.

Aussi, la conséquence la plus importante est certainement que si l'on veut penser le droit de la sécurité numérique, il est inconcevable de renvoyer sans arrêt les États vers leur territorialité. Il faut au contraire construire les outils juridiques qui permettent à chaque État, chaque justice nationale, chaque acteur de la sécurité numérique, de protéger son territoire numérique, d'assurer sa souveraineté tout en respectant celle des autres.

C'est dans cet esprit que des discussions sont en cours [(1)] dans le cadre de la convention du Conseil de l'Europe sur la cybercriminalité de 2001 pour parvenir à un second protocole additionnel qui prévoira notamment les requêtes directes d'une autorité judiciaire d'un pays auprès d'un opérateur d'un autre pays partie à la convention.

Mais la réalité du quotidien est parfois plus simple, et tous les jours, dans le monde entier, les acteurs en charge de la sécurité numérique – et plus spécifiquement les centres d'alerte et de réaction aux attaques informatiques (CSIRT [(2)]) – s'échangent des données sur les incidents et s'efforcent de les résoudre par une coopération directe. Ces échanges ne correspondent pas forcément au cadre juridique existant, mais ils correspondent à un besoin légitime et sont réalisés dans un cadre d'éthique et de confiance [(3)].

Comment les cybercriminels se jouent des territoires numériques

Les cybercriminels sont en général vus comme se moquant des frontières. En réalité, les frontières entre les pays mais aussi entre les territoires numériques sont à la fois pour eux des alliés qui les protègent et des limites qu'ils vont devoir surmonter.

(1) Groupe de rédaction du T-CY : https://www.coe.int/fr/web/cybercrime/t-cy-drafting-group
(2) En anglais : Computer security incident response team.
(3) Ethics for incident response and security teams : https://www.first.org/global/sigs/ethics/ethics-first

Il est vrai que ces frontières géographiques et politiques sont un avantage pour eux, parce qu'elles ralentissent la coopération entre les acteurs de la sécurité, les services d'enquête et la justice, ou encore parce qu'elles rendent plus complexes la traçabilité de leurs actions et de leurs transactions financières. Mais elles sont autant d'obstacles, comme pour tout un chacun.

Prenons le cas d'en escroc spécialiste du hameçonnage (*phishing*). Son objectif est de collecter un maximum de coordonnées bancaires ou d'identifiants de services en ligne. Dans un scénario typique, il agira depuis un pays parlant la même langue que le nôtre, il aura pris le contrôle d'un site Web dans un pays proche pour y installer son kit de hameçonnage, invisible pour le propriétaire du site Web, et il diffusera l'annonce permettant d'attirer les victimes grâce à des courriers électroniques ou des SMS. Pour ce faire, il fera souvent appel à un sous-traitant, spécialiste du *spam*, gérant, par exemple, un *botnet,* dont les machines victimes sont réparties sur la planète et dont le serveur de commande et de contrôle est situé dans un autre pays avec la capacité de relayer les courriers électroniques.

Une fois les données de ses victimes collectées, il va chercher à les revendre sur un marché cybercriminel, dont il ne connaît pas la localisation, parce qu'il y accède par le protocole de prédilection pour préserver l'anonymat, à savoir Tor [(4)]. Il sera payé en crypto-monnaies – souvent des *bitcoins* qu'il pourra conserver sous cette forme ou transformer en monnaie locale sur une plateforme d'échange.

On le voit, la façon dont s'est construit l'écosystème cybercriminel (Freyssinet, 2013) a pour objectif principal de brouiller les pistes pour ceux qui cherchent à en détecter l'activité ou à en identifier les auteurs.

Cela n'est pas sans un coût pour le cybercriminel qui doit souvent faire confiance à des inconnus, payer des frais aux différents intermédiaires, voire parfois prendre le risque de perdre les données qu'il aura chèrement (mais malhonnêtement) acquises.

Retour sur la crise épidémique de 2020

Si l'on se replace dans les circonstances de la période de confinement de la crise du Coronavirus en mars et avril 2020, la diminution de la mobilité physique a énormément entravé les délinquants classiques : cambriolages, trafics de stupéfiants ont été très lourdement freinés. Les cybercriminels n'ont, quant à eux, pas été en reste.

Le contexte d'abord est celui d'une forte croissance de la cybercriminalité observée depuis le début de l'année 2020. Ainsi, au premier trimestre de l'année 2020, la gendarmerie nationale mesurait une augmentation de + 22 % des faits cybercriminels détectés ou portés à la connaissance de ses enquêteurs, par rapport à la même période de l'année 2019. Les rançongiciels [(5)], par exemple, étaient en forte hausse (+ 134%). Cette tendance s'est donc poursuivie tout au long de la crise, sans être freinée par les événements.

Au moment du confinement, deux tendances ont été observées dans chacun des pays concernés : un déplacement massif des thématiques utilisées par les cybercriminels pour propager leurs arnaques vers la thématique de la crise épidémique, et un acharnement particulier à profiter des

(4) Tor ou *the onion router* est un protocole permettant de router les communications par au moins trois serveurs intermédiaires à chaque fois, ce qui masque les adresses des serveurs et de ceux qui les consultent. Cette fonctionnalité est de plus en plus souvent intégrée à des navigateurs Web, comme Brave. Les sites Web accessibles *via* Tor sont ce que l'on appelle souvent improprement le *darkweb*.

(5) Logiciel malveillant qui bloque l'accès aux données de la victime en procédant à leur chiffrement. Pour obtenir le mot de passe ou la clé de déchiffrement, la victime est invitée à payer une rançon, souvent en crypto-monnaie.

faiblesses des entreprises et des établissements de santé parfois désorganisés par le télétravail d'une partie de leurs employés. Ainsi, on a noté à partir du mois de mars 2020 une forte hausse des attaques sur le protocole RDP (Galov, 2020) qui permet l'accès à distance sur les serveurs ou machines de bureau ; il avait souvent été configuré à la hâte au moment du confinement sans toujours faire attention aux règles de sécurité.

La typologie des attaquants observés était intéressante, avec, par exemple, des scénarios d'escroquerie à la vente de masques sanitaires impliquant des sociétés fictives un peu partout dans le monde. L'un de ces escrocs, identifié par l'Office central de lutte contre les atteintes à l'environnement et à la santé publique (OCLAESP) et la DGCCRF, est un français, réfugié à l'étranger [(6)].

Cet épisode démontre, s'il en était besoin, que la cybercriminalité se joue des contraintes des territoires géographiques.

Vers des territoires cybercriminels autonomes ?

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. Ainsi, de la même façon que beaucoup d'acteurs privés ont tendance à vouloir imposer leurs propres règles en lieu et place de la législation des pays où se trouvent leurs clients et usagers, les délinquants qui gèrent des plateformes de marché en ligne y imposent évidemment leurs propres règles : contrôle d'accès, règles de comportement, paiement de taxes (frais sur les transactions) et possibilité d'être expulsés.

Mais cela pourrait aller beaucoup plus loin. Le moteur principal de cette transformation est l'existence des crypto-actifs (les crypto-monnaies comme le *bitcoin*, créé en 2009, et toutes les variantes). De tels actifs virtuels, échangeables contre des monnaies ayant cours légal, constituent en pratique un outil permettant de jouer le rôle de monnaie. Malgré leur caractère décentralisé, l'administration de ces crypto-actifs est souvent centralisée au sens où un nombre limité de personnes maîtrise leur fonctionnement (les mécanismes de création crypto-monétaire). On peut donc imaginer une prise de contrôle intégrale de l'un de ces crypto-actifs et, de toute façon, la possibilité d'en créer de nouveaux, même s'il faudra les faire reconnaître comme moyen d'échange.

Le second moteur de cette transformation est justement la nature particulière des territoires numériques, telle que nous venons de la décrire : ils se jouent des frontières politiques et géographiques, et tant le droit que la technologie autorisent la création d'un espace numérique sous le contrôle d'une groupe de personnes, hébergé de façon mouvante sur les plateformes physiques d'entreprises légitimes de l'économie numérique ou même sur les infrastructures d'entreprises cybercriminelles ayant pignon sur rue.

Un pouvoir trop important constitué autour de cette indépendance virtuelle présente de forts risques d'influence sur les états légitimes, par la corruption et la consolidation d'économies parallèles fortes. Afin de répondre à ce risque, plusieurs actions sont indispensables : la détection et le démantèlement de telles tentatives d'autonomisation cybercriminelle dans l'espace numérique, et la construction de nouveaux outils juridiques pour y faire face, sans freiner l'innovation et l'investissement légitimes. C'est l'une des raisons pour lesquelles il est indispensable de légiférer pour encadrer les crypto-actifs, notamment en ce qui concerne la transparence des organes de contrôle.

(6) https://www.lemonde.fr/societe/article/2020/04/20/coronavirus-une-arnaque-au-materiel-de-protection-a-plus-d-un-million-d-euros_6037114_3224.html

Références

FREYSSINET É. (2013), « Botnets : illustration de nouvelles formes de criminalité organisée », *Revue du GRASCO*, n°6, juillet, pp. 10-18.

FREYSSINET É. (2017), « Appréhension des cybermenaces en 2017 : de la cybercriminalité à la cyberdéfense », *Revue Défense nationale*, 2017/10, n°805, pp. 82-86.

GALOV D. (2020), *Remote spring: the rise of RDP bruteforce attacks*, Kaspersky Securelist blog, 29 avril.