Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE
L'INTÉRIEUR

ÉTAT DE LA MENACE LIÉE AU NUMÉRIQUE EN 2018

LA RÉPONSE DU MINISTÈRE DE L'INTÉRIEUR

Rapport n° 2
Mai 2018

Délégation ministerielle aux industries de sécurité et à la lutte contre les cybermenaces

Sommaire

Le mot du ministre

« Faire de la cybersécurité une culture nationale »

Cyberattaques contre les systèmes d'information d'entreprises ou d'institutions, financement d'organisations terroristes par du crowdfunding, escroqueries en ligne : chaque jour, nos policiers, nos gendarmes, nos services de renseignement sont confrontés à une délinquance qui investit l'espace *cyber*.

Pour faire face à cette menace de plus en plus prégnante et protéiforme, j'ai annoncé, à l'occasion du *Forum international de la cybersécurité* (FIC) de Lille, ma volonté de doter la France d'une stratégie renforcée de lutte contre les cybermenaces pour les années à venir.

Pour savoir où l'on va, il faut d'abord savoir où l'on est. En cela, la publication de ce rapport sur « l'État de la menace liée au numérique en 2018 », qui développe un panorama riche et approfondi des phénomènes cyber et des réponses actuellement apportées par le ministère de l'Intérieur, est particulièrement précieuse. Il sera complété par une cartographie exhaustive des différentes ressources existantes au sein du ministère de l'Intérieur, réalisée par Thierry Delville, délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces.

À partir de cette base, nous pourrons alors élaborer une stratégie à la hauteur des enjeux. Dès l'été 2018, des propositions visant à encore mieux prévenir les cybermenaces, gérer les cybercrises et lutter contre la cybercriminalité me seront remises. Elles viendront nourrir une feuille de route pluriannuelle qui devra se donner pour objectif de faire de la France une des nations les plus en pointe en matière de lutte contre les cybermenaces.

La cybersécurité constitue un enjeu crucial. Pour nos concitoyens qui doivent pouvoir réaliser leurs démarches administratives, utiliser leurs smartphones, leurs tablettes, en toute sérénité. Pour nos entreprises qui doivent pouvoir pratiquer leurs activités sans risquer un espionnage industriel ou un blocage de leurs chaînes de production. Pour l'État qui doit être en capacité de protéger ses données les plus sensibles, de garantir l'intégrité de ses systèmes d'information, tout simplement d'assurer sa souveraineté.

Aussi, notre stratégie de lutte contre les cybermenaces ne saurait être l'affaire de quelques experts. La cybersécurité doit en effet être l'affaire de tous, une *culture nationale,* partagée par tous les acteurs. C'est toujours dans cet esprit, qu'avec l'ensemble des équipes du ministère de l'Intérieur, nous travaillerons.

Gérard COLLOMB
Ministre d'État, ministre de l'Intérieur

Ce document est la deuxième édition d'un état de la menace liée au numérique établi par l'ensemble des services du ministère de l'Intérieur, sous la coordination de la délégation ministérielle aux industries de sécurité et à la lutte contre le cybermenaces (DMISC).

Il dresse un panorama complet des enjeux, des menaces et des réponses apportées par le ministère faisant du thème de la cybersécurité un enjeu essentiel de l'action de l'État et une question primordiale de la protection des citoyens.

D'aucuns trouveront ce document trop détaillé. Mais, en juger par les retours de la première édition, et par les événements survenus tout au long de l'année 2017, le thème de la lutte contre les cybermenaces apparaît de plus en plus central et nécessite plus que jamais un effort d'explication.

Il est essentiel d'exposer les faits, de faciliter la connaissance de phénomènes qui évoluent en permanence, et de partager l'analyse du risque cyber et de ses mutations.

Si certaines informations ne peuvent figurer dans ce document et resteront classifiées, l'essentiel des phénomènes constatés et des actions poursuivies et réprimées sont toutefois détaillés, dans l'objectif de permettre une représentation précise de l'ampleur de la menace.

Les données statistiques ne permettent pas encore d'appréhender finement l'ensemble des faits de cybercriminalité, en raison d'outils de recueil en cours d'évolution. Par ailleurs, de très nombreux faits ne sont pas signalés auprès des services de sécurité intérieure, ce qui nuit à leur recensement et leur compréhension. Les victimes, le plus souvent des entreprises, sont en effet tentées de ne pas déposer plainte, compte tenu d'un risque réputationnel.

Pourtant, seule la connaissance précise de la sinistralité du risque cyber permettra d'accroître l'efficacité de la protection numérique, la sensibilisation de l'ensemble des acteurs, l'amélioration de la couverture assurancielle et plus globalement l'efficacité de la réponse apportée.

Ce document doit contribuer à libérer la parole et nourrir la réflexion et la collaboration de tous les acteurs publics et privés face à un phénomène qui touche aujourd'hui le monde économique et tout à chacun dans la vie quotidienne.

Thierry DELVILLE
Délégué ministériel aux industries
de sécurité et à la lutte contre les cybermenaces

Synthèse

Partie 1 - Enjeux stratégiques liés aux cybermenaces

La société connait aujourd'hui une phase de transformation numérique de grande ampleur et l'ensemble de nos systèmes sont de plus en plus interconnectés. Aussi, les attaques informatiques ne constituent plus un simple risque conjoncturel, mais sont devenues systémiques. L'adaptation des moyens de lutte doit être permanente pour faire face à l'évolution des cybermenaces, l'implication de l'ensemble de la chaîne des acteurs institutionnels et privés doit être recherchée et la société doit renforcer sa résilience.

Enjeux économiques

Les attaquants informatiques peuvent conduire aussi bien des opérations très ciblées que des actions massives et indiscriminées. Désormais, les cybercriminels attaquent aussi les entreprises, plus «rentables» que les individus.

Pour les organisations, les atteintes motivées par l'appât du gain, le sabotage, l'espionnage ou l'ingérence économique ont des incidences financières et réputationnelles. Pour se protéger, elles disposent de deux principaux outils complémentaires : la prévention et le transfert de risque par le biais de l'assurance, dont la couverture du risque cyber commence à se développer, même si les actifs intangibles ne peuvent encore être assurés de façon standardisée.

Aucun secteur économique n'est à l'abri. Les secteurs bancaire et financier constituent des cibles de choix pour les hackers, tant en raison des flux monétaires générés que des données sensibles de leurs clients ; il en est de même du secteur de la santé, très producteur de données.

Enjeux sociétaux

Sur Internet, les trafics illicites sont facilités par trois mécanismes : les forums de discussion, les *darknets* et les cryptomonnaies. Sur les *darknets*, il est constaté l'importance du trafic de stupéfiants et des activités délictueuses connectées à la délinquance économique et financière comme le *carding*. Des atteintes aux personnes, notamment aux mineurs, y sont présentes, tout comme la vente de produits pharmaceutiques illicites ou détournés à d'autres fins.

Sur un autre plan, le vecteur numérique est au cœur de la stratégie de communication djihadiste, tant à des fins de propagande, d'influence, d'intimidation ou de déstabilisation. Pour la France, l'Allemagne et le Royaume-Uni, le retrait, une heure après publication, des contenus terroristes en ligne constitue un enjeu prioritaire pour renforcer notre capacité collective à prévenir et lutter contre le terrorisme.

Enfin, il a été constaté une utilisation de plus en plus accrue des outils de chiffrement et d'anonymisation sur Internet. Ceux-ci soulèvent des questions techniques, juridiques et opérationnelles dans la lutte contre la criminalité et le terrorisme et rendent l'accès à la preuve numérique délicat.

Enjeux juridiques et normatifs

La dimension internationale de la cybercriminalité implique aussi d'harmoniser les législations nationales ou à tout le moins, de faciliter la coopération au niveau européen et international afin de renforcer les moyens de lutte contre ce phénomène.

Pour lutter efficacement, notamment contre les atteintes portées aux systèmes d'information, il apparait nécessaire de développer d'autres approches en matière d'investigations, comme celle de l'extension du champ d'application de la technique d'enquête sous pseudonyme.

La législation européenne aura un impact particulier en 2018, notamment sur les administrations et les entreprises, avec le RGPD qui entrera en application le 25 mai prochain et la transposition de la directive NIS.

Enfin, un arrêt de la Cour de justice de l'Union européenne est venu interroger les législations encadrant la conservation des données de connexion, fin 2016. Or, la conservation et l'accès aux données nécessaires aux enquêtes constitue un enjeu de premier plan. Un an plus tard, les travaux se poursuivent.

Partie 2 - Usages et phénomènes

Évolution des usages

Le taux de pénétration de l'Internet continue de progresser en France (87 %) et dans le Monde (54 %) ; il en est de même pour les réseaux sociaux. Depuis quelques années, le smartphone s'impose comme plateforme multi-usages et est la cible de nombreux logiciels malveillants.

L'évolution de l'usage des cryptomonnaies doit être suivie avec attention, car elles sont largement utilisées par les cybercriminels (anonymisation, minage clandestin, attaques de plateforme d'échanges, levée de fonds ICO…).

Du fait de leur développement, les objets connectés et les espaces intelligents augmentent considérablement la surface d'attaque pour les cybercriminels.

De nouvelles pratiques telles que les *fake news*, *hoax* et *swatting*, se développent sur Internet. Leur détection ne constituant pas en elle-même une réponse suffisante, les forces de l'ordre intègrent ces éléments dans leur processus de gestion de crise.

Phénomènes

Les attaques de mai et juin 2017, *Wannacry* et *NotPetya*, ont eu un aspect inédit par leur dimension massive et internationale, la diversité des victimes touchées, l'ampleur de la propagation et les dommages causés de manière indiscriminée.

Les rançongiciels sont devenus une menace majeure qui touche, outre des particuliers, tous les secteurs d'activités et peut impacter significativement le bon fonctionnement des petites entreprises. Toutefois, ces évènements ne doivent pas masquer d'autres phénomènes, comme les attaques ciblées (y compris le cyber-espionnage) ou les attaques visant les systèmes bancaires et de paiement (*jackpotting*…).

Tout un écosystème facilitant la mise en œuvre d'attaques cyber par des groupes criminels s'est mis en place, induisant la notion de « crime-as-a-service ». En 2017, la mise à disposition de plateformes de location de rançongiciel est une tendance émergente (« *Ransomware as a Service* ») avec l'apparition d'un nouveau modèle économique début 2018.

La mise hors ligne des sites *AlphaBay* et *Hansa Market* à l'été 2017 a porté un coup d'arrêt à deux des plus grands sites de revente de produits illicites sur les darknets.

La France est particulièrement touchée par le vol des données personnelles, qui reste l'objectif principal des intrusions dans les systèmes de traitement automatisé de données.

Si de nombreuses attaques par déni de service (DDoS) sont réalisées à partir de botnets d'objets connectés, il est constaté une diminution du phénomène à l'instar des défigurations.

Les phénomènes criminels en lien avec le piratage des standards et lignes téléphoniques se développent selon deux procédés, le *phreaking* et le *spoofing* de ligne téléphonique.

Les contenus de provocation et d'apologie au terrorisme signalés à la plate-forme PHAROS ont connu une baisse significative pour la deuxième année consécutive.

En matière d'escroquerie, l'année 2017 a vu un net recul des faux ordres de virement internationaux (FOVI) et la recrudescence d'autres types d'escroquerie, comme celles par exemple, de sites frauduleux proposant des placements indexés sur le cours du diamant ou celles dites au faux support technique dont une nouvelle campagne a été détectée en novembre 2017.

Les fraudes à la carte bancaire poursuivent leur évolution avec des outils de *skimming* de plus en plus sophistiqués, déployés souvent par des groupes criminels plus ou moins structurés d'Europe centrale ou balkanique.

Les techniques d'ingénierie sociale demeurent une tactique essentielle pour la commission de nombreux crimes, souvent complexes, liés au cyber et facilités par lui.

Le phénomène de l'exploitation sexuelle des mineurs en ligne est toujours inquiétant. Il est noté la diversification de l'origine des images et vidéos à caractère pédopornographique qui mettent en scène des victimes de plus en plus jeunes et la pérennisation des faits d'abus sexuels d'enfants commis à distance («*live streaming*»).

Perception de la menace et coût de la cybercriminalité

Sans avoir un caractère exhaustif, l'étude menée sur l'ensemble des faits portés à la connaissance de la gendarmerie montre une tendance globale en hausse de 30 % par rapport à 2016 ; plus de 60 % du total de ces infractions sont des escroqueries liées à Internet.

La majorité des entreprises sont touchées par des cyber-attaques ; près de 80% en ont constatées au moins une en 2017.

L'évaluation du coût de la cybercriminalité reste encore un exercice complexe , bon nombre de victimes ne déposant pas plainte. Les attaques, dans près d'un cas sur deux, ont des impacts concrets sur le business des entreprises touchées. Le coût estimé d'une violation de sécurité est en moyenne de plusieurs centaines de milliers euros pour une entreprise de taille moyenne (ETI) et le préjudice moyen d'un détournement de données pour chaque entreprise victime porte sur plusieurs millions d'euros.

Partie 3 - Les actions du ministère de l'Intérieur

Le ministère de l'Intérieur s'est depuis longtemps mis en ordre de bataille pour faire face aux cybermenaces et s'adapte continuellement. Le délégué ministériel aux industries de sécurité et à la lutte contre les cyber menaces (DMISC) joue un rôle de pilotage stratégique en matière de lutte contre les cybermenaces. Une feuille de route a été demandée par le ministre de l'Intérieur, visant un plan de renforcement des actions de lutte dans ce domaine.

Prévenir

Par sa présence dans les territoires, le ministère est un acteur majeur de la sensibilisation des particuliers, des acteurs économiques et des collectivités territoriales. Ses services ont participé tout au long de l'année à des évènements destinés au grand public ou à un public plus ciblé. L'opération « Permis Internet », a permis de sensibiliser plus de 950 000 élèves.

La direction générale de la sécurité intérieure (DGSI) effectue des actions ciblées vers le monde économique et le service central de renseignement territorial (SCRT) a un rôle de soutien et de capteur au profit des services spécialisés en charge de l'intelligence économique.

Enquêter

Au niveau de l'accueil dans les services locaux, la prise en compte des victimes passe avant tout par la capacité du dispositif à accueillir, écouter, analyser et orienter vers le service idoine.

Les services spécialisés dans la lutte contre la cybercriminalité poursuivent leur développement tant en matière d'investigation que d'analyse numérique (forensic). Le schéma général tend, dans ces deux domaines, vers la mise en place d'un réseau territorial animé ou piloté par les services centraux.

Le partenariat avec les opérateurs de l'Internet continue de progresser. Dans une démarche coordonnée par la DMISC et co-pilotée avec le Secrétariat d'État au Numérique, le ministère soutient très activement les travaux menés avec Europol et dans le cadre de l'EU Internet Forum.

Innover

Le ministère s'engage également dans une démarche de recherche et de développement. Les échanges avec le monde académique ou dans le cadre du Comité de Filière des industries de sécurité (CoFIS) se développent.

Le ministère innove en matière de transformation numérique et dématérialise ses processus pour mieux signaler et communiquer autour du cyber, grâce à la plateforme d'assistance aux victimes de cybermalveillance, aux équipements Néo et à la brigade numérique de la Gendarmerie, ainsi qu'aux projets Thésée et Perceval qui permettront de mieux appréhender certains phénomènes de masse relevant de la cybercriminalité.

Enfin l'élaboration de solutions d'identité numérique a été confiée conjointement au Ministre d'État, ministre de l'Intérieur et au Secrétaire d'État chargé du numérique, en vue de mettre en œuvre un parcours d'identification numérique sécurisée pour des personnes physiques ou morales.

La lutte contre les cybermenaces recouvre l'ensemble des actions menées en matière de lutte contre la cybercriminalité, de cyberdéfense et de sécurité des système d'information

Partie I

Enjeux stratégiques liés aux cybermenaces

Comme l'ont démontré les attaques *WannaCry* et *NotPetya* en 2017, l'adaptation des moyens de lutte doit être permanente pour faire face à l'évolution des cybermenaces.

Le renforcement de la lutte contre les cybermenaces doit garantir à la fois le respect des droits fondamentaux et des libertés publiques et la protection de l'ordre public numérique qui incombe au ministère de l'Intérieur.

La lutte contre les cybermenaces passe par le développement d'équipements adaptés et de techniques spéciales d'enquête. L'augmentation exponentielle des données numériques à collecter et exploiter doit aussi être prise en considération dans le cadre des investigations. Bien évidemment, les procédures mises en œuvre doivent à la fois assurer la recevabilité des preuves numériques collectées devant les juridictions et garantir la protection des libertés fondamentales.

Ces réflexions appellent une connaissance précise de l'évolution des comportements ainsi que de l'évolution des technologies de l'information et des communications, lesquelles peuvent impliquer une adaptation des normes définies au niveau national, européen et international.

1.1. Enjeux sociétaux des cybermenaces

La société connait aujourd'hui une phase de transformation numérique de grande ampleur. L'ensemble de nos institutions et de nos systèmes administratifs, mais aussi industriels[1] a recours à des dispositifs numériques, de plus en plus interconnectés. Aussi, les attaques informatiques ne constituent plus un simple risque conjoncturel mais sont devenues systémiques.

Il revient à l'État, et en premier lieu au ministère de l'Intérieur, garant de l'ordre public, de rendre l'espace numérique plus sûr. Cette réponse doit être à la hauteur de ces enjeux, en prenant en compte l'interdépendance et la porosité entre les domaines physique et cyber.

Afin de mieux anticiper et réagir face aux crises à venir, l'implication de l'ensemble de la chaîne des acteurs institutionnels et privés doit être recherchée.

En effet, comme l'indique la récente revue stratégique de cyberdéfense[2], face *« à des cyberattaques croissantes en nombre, en intensité et en sophistication, il convient d'opposer un dispositif national de protection et de défense informatique robuste, en vue de protéger les populations et les intérêts économiques et sociaux de la Nation »*. Cela requiert *« la mobilisation de capacités et de compétences diverses, au sein de l'État mais aussi au cœur de la société »,* en particulier de mieux intégrer nos moyens de défense cybernétique et de renforcer notre résilience.

Les attentats terroristes des trois dernières années ont mis en exergue le recours de plus en plus prégnant aux technologies de l'information et de la communication dans la diffusion de propos provoquant ou faisant l'apologie du terrorisme et la préparation des actes terroristes.

(1) En particulier avec les systèmes d'acquisition et de contrôle de données (SCADA en anglais) qui sont des systèmes de télégestion et de contrôle d'installations techniques et industrielles.

(2) http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf

1.1.1. L'emploi d'Internet à des fins terroristes

Le vecteur numérique au cœur de la stratégie de communication djihadiste.

Les groupes islamistes radicaux se sont appuyés sur le vecteur Internet dès son émergence, au début des années 1990. L'Islamic Media Center, premier site djihadiste, a été créé en 1991[3]. Au tournant du siècle, la stratégie de communication s'étend aux forums et introduit une notion d'interactivité inédite. La professionnalisation de la cyber communication franchit une nouvelle étape avec la publication d'Inspire, premier magazine en ligne de propagande djihadiste en langue anglaise diffusant des éléments de langage justifiant l'action armée, l'utilisation de moyens de communication cryptés et la mise en œuvre de modes opératoires pour la commission d'attentat (fabrication de bombes artisanales, production de poison). À partir de la fin des années 2000, les mouvement djihadistes développent leur propagande en ligne via l'utilisation des réseaux sociaux, puis des forums de jeux vidéo en ligne.

L'activisme terroriste *se caractérise, dans le domaine cyber[4], par un cyber-djihadisme particulièrement actif et visible, qui détourne les technologies de l'information et de la communication à* des fins :

- de propagande et d'influence : apologie et provocation aux actes terroristes, désignation de cibles dans le monde physique, recrutement, accompagnement dans la radicalisation, collecte de fonds[5], etc.;
- d'intimidation : diffusion de messages hostiles, divulgation de données personnelles des « ennemis du Jihad », etc.;
- de déstabilisation : attaques en saturation de trafic (DDOS) contre des sites officiels en période de crise terroriste, altération de sites Internet par défigurations (« défaçages »), fausses alertes mobilisant les services de secours, etc.

Les récentes évolutions

Les organisations Al Qaïda (AQ) et surtout l'État Islamique (EI), ainsi que les groupes qui leur sont affiliés, sont les principaux pourvoyeurs de propagande jihadiste sur Internet. Al Qaïda et l'État Islamique parviennent ainsi à compenser les difficultés rencontrées sur le terrain en occupant l'espace médiatique offert par Internet. Toutefois, il faut noter une baisse de la production de la propagande sur Internet depuis 2016.

La chute de Raqqa (Syrie) en octobre 2017 a largement contribué à la modification et au ralentissement des modes de communication de l'État islamique. Les productions jadis quotidiennes (reportages photographiques, bulletins audio Al Bayan…) sont aujourd'hui moins nombreuses. L'arrêt de la publication et de la diffusion du magazine officiel « Rumiyah » (dernière parution au mois de septembre 2017) démontre un affaiblissement des ressources médiatiques. Néanmoins, le mode opératoire de diffusion des matériels reste le même : le contenu est déposé sur des services dits « drive », puis sa publicité est faite sur les médias sociaux[6] en diffusant le lien de ces services de stockage.

---

(3) HECKER Marc – directeur des publications à l' Institut Français des Relations Internationales - Paris

(4) L'activisme qui s'illustre dans le domaine cyber est également désigné sous le terme d'hacktivisme.

(5) Collecte de fonds via les Mosquées, le crownfunding ou en recourant à des campagnes de phishing comme par exemple celle en provenance d'Irak en juin 2017.

(6) On regroupera dans ce terme les réseaux sociaux « classiques » comme Facebook et Twitter, ou encore plus récemment Baaz, mais également les messageries chiffrées comme Telegram ou Periscope..

À la fois hébergeur et réseau social sécurisé offrant une messagerie chiffrée, Telegram demeure le pilier de la communication de DAECH, point de lancement de tous les contenus qui se propagent par la suite. D'autres entités terroristes s'appuient également sur ce réseau social pour diffuser leur propagande, où la modération des contenus reste très limitée.

Les capacités de lutte informatique active des organisations terroristes demeurent limitées, même si la prolifération des armes numériques est susceptible de leur permettre des attaques plus complexes. Les attaques numériques par des personnes se revendiquant des organisations précitées continuent d'être circonscrites à des opérations de faible intensité, non coordonnées et n'affectant pas des entités ciblées. En effet, elles se caractérisent principalement par des défigurations et des attaques en déni de service.

Même si ces faits ne sont pas sans conséquences économiques et pourraient, pour certaines d'entre elles, s'approcher d'un acte de sabotage (en particulier les attaques en déni de service), aucune d'entre elles ne peuvent être, à ce stade, considérée comme une attaque informatiques constitutive de « cyberterrorisme *» et attribuable* à une organisation terroriste.

1.1.2. L'évolution des usages des technologies de l'information et des communications

Une utilisation de plus en plus accrue des outils d'anonymisation

Depuis les révélations d'Edward Snowden en juin 2013, il a été constaté une utilisation exponentielle des outils d'anonymisation sur Internet. Un pic d'utilisation de Tor a été mesuré à partir du mois de septembre 2013, ainsi qu'en décembre 2017 (voir figure 1 ci-dessus). Par ailleurs, le nombre moyen d'utilisateurs directs quotidiens de Tor en France est passé de 50 000 à près de 100 000 aujourd'hui.

Les services d'enquête ont également noté une augmentation de l'utilisation d'autres types de services d'anonymisation, tels que la location de serveurs relais[7] positionnés dans différents pays, notamment européens.

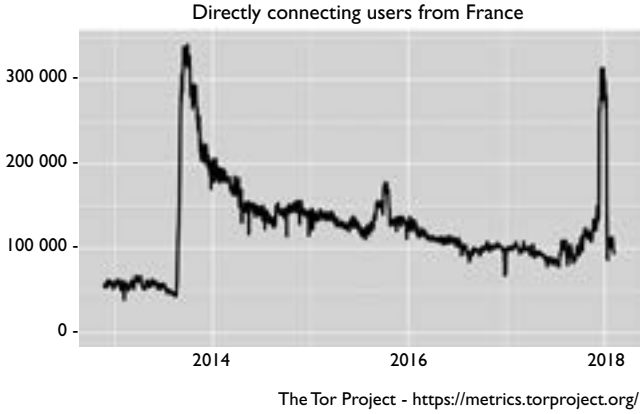


Figure 1 : *Nombre d'utilisateurs directs de Tor en France*

(7) Egalement désignés sous la terminologie VPN pour Virtual private network.

Une généralisation du chiffrement

Parallèlement à l'utilisation de plus en plus accrue des outils d'anonymisation, on assiste à une quasi-généralisation du chiffrement, tant par les entreprises qui en font un argument de protection des données de leurs clients que par le recours systématique des assaillants pour se dissimuler.

Ces outils posent des difficultés pratiques et juridiques aux enquêteurs et à l'autorité judiciaire dans leur lutte contre le crime en général et le terrorisme en particulier. En effet, certaines données leur sont inaccessibles parce que stockées sur un appareil verrouillé (ordinateur, tablette, smartphone), d'autres sont accessibles mais inintelligibles parce que chiffrées.

Le chiffrement des données stockées dans un espace distant ou sur un appareil saisi rend beaucoup plus difficile le recueil d'une éventuelle preuve exploitable démontrant la participation de l'utilisateur à une infraction.

Le chiffrement des communications électroniques rend par ailleurs inefficaces les interceptions de données échangées entre suspects sur les réseaux de télécommunications.

Dès lors, les services enquêteurs sont obligés de recourir de plus en plus souvent à des experts pour tenter de mettre au clair le contenu des communications chiffrées. Or, ces opérations d'expertise prennent du temps et se révèlent coûteuses.

La localisation des données

Aux problèmes techniques posés par le chiffrement en matière d'enquête, s'ajoute la complexité des demandes de renseignement lorsque les prestataires ne sont pas établis dans l'Union européenne et le nécessaire recours à une demande d'entraide pénale internationale. La mise en œuvre de ces procédures peut être rendue encore plus complexe en cas de localisation des données de ce prestataire au sein de multiples pays[8] notamment en matière de juridiction compétente ou d'entraide pénale. Cela peut alors susciter d'autres questions tenant à la localisation des données et à la détermination des juridictions territorialement compétentes pour y accéder.

(8) Affaire Microsoft Ireland. Dans un dossier de trafic de stupéfiants, un juge de l'État de New York avait émis en décembre 2013, un mandat de perquisition à l'encontre de Microsoft, afin d'obtenir la communication des données de contenu d'un compte email, stockées sur un serveur en Irlande. Le 14 juillet 2016, une Cour d'appel des État-Unis (Second Circuit) a considéré que le gouvernement américain ne pouvait pas contraindre une entreprise à transmettre des données électroniques de ses clients, stockées à l'étranger (pas d'application extraterritoriale de la loi SCA). Le gouvernement américain a contesté cette décision devant la Cour Suprême américaine qui a accepté, en octobre 2017, de se saisir. La situation a évolué avec le Cloud Act, promulgué le 23 mars 2018, qui permet aux autorités fédérales de contraindre les opérateurs américains, à fournir les données stockées sur des serveurs, qu'ils soient situés aux États-Unis ou non. De ce fait, le gouvernement américain, soutenu par Microsoft, a déposé une requête de désistement..

1.1.3 Un contexte favorable aux trafics illicites sur les darknets

D'après le constat de l'OCRTIS[9], les transactions et trafics illicites sont facilités par trois mécanismes :

- Les forums : leur rôle est central, car ce mode de discussion permet aux internautes d'échanger des nouvelles adresses de cryptomarchés, ainsi que des avis sur des vendeurs ou produits. En revanche, les transactions illégales n'y sont pas ouvertement pratiquées.
- La cryptomonnaie, qui est une monnaie virtuelle dont l'émission et les transactions sont validées par des calculs cryptographiques effectués au sein d'un réseau informatique décentralisé ; la plus connue étant le Bitcoin.
- Le darkweb[10] et les cryptomarchés qui sont des sites marchands, où les transactions se font exclusivement en cryptomonnaie.

Accessible par le biais de réseaux d'anonymisation spécifiques dont le plus connu est Tor, le darkweb se subdivise en communautés. Régulièrement présenté comme un lieu où s'épanouissent les criminels, il ouvre un vaste espace d'échange sécurisé et légal où coexistent dissidents politiques et activistes, groupuscules extrémistes et criminels. Ces profils très variés cherchent à effacer leurs traces sur Internet, à dissimuler leurs identités réelles et leurs transactions, ce que permettent Tor et le recours à des techniques de chiffrement, de messagerie sécurisée ou au paiement en cryptomonnaies. Le darkweb est composé d'une multitude d'acteurs aux rôles bien définis. Sur les places de marché (*marketplace*) se rencontrent vendeurs et acheteurs sur le modèle de plateformes à succès du clearweb (comme Ebay, le Bon Coin). Gérées par des administrateurs, elles hébergent des forums où se négocient les modalités de transactions et de livraison. Des tiers de confiance, touchant jusqu'à 7 % de commission sur la transaction, s'assurent de la conformité de l'opération. Certains vendeurs optent pour un modèle plus individualiste et conduisent leurs affaires depuis un autoshop, une boutique autonome où le contact avec le vendeur s'effectue sans intermédiation. Depuis les premières opérations d'envergure sur le darkweb (Silkroad en 2013, Onymous en 2014), il est constaté une réelle montée en puissance des capacités d'anonymisation qui rend toujours plus difficile la tâche des « cyberpatrouilles » des forces de sécurité.

Importance du trafic de stupéfiants

Polymorphe et extrêmement diversifiée, la criminalité sur le darkweb peut néanmoins s'appréhender par le prisme de grands ensembles regroupant divers crimes et délits. Le premier agrégat regroupe les trafics de stupéfiants et d'armes. Les stupéfiants, qui représentent plus de 20 % (contre moins de 5 % pour les armes) des affaires liées au réseau Tor entre 2014 et 2017, dominent largement ce premier agrégat. Par ailleurs, près de 70 %[11] des annonces retrouvées sur Alphabay, l'une des principales places de marché anglophone avant qu'elle ne soit fermée en juillet 2017 par le FBI, concernaient la vente de stupéfiants ou de documentation connexe. Pour lutter contre ces trafics massifs, les services d'enquête maintiennent une veille opérationnelle active.

(9) Office central pour la répression du trafic illicite des stupéfiants

(10) Le darkweb met à disposition différents contenus non indexés présents sur les darknets. Le réseau Tor est le plus connu et le plus utilisé d'entre eux, mais on trouve aussi des réseaux tels que Freenet, I2P, GNUnet ou Zeronet…

(11) Les chiffres concernant les annonces sur Alphabay ont été établis à partir d'une consultation en date du 22 mars 2017.

La délinquance économique et financière, et l'industrialisation des techniques de piratage

Le second agrégat regroupe un ensemble d'activités délictueuses connectées à la délinquance économique et financière et représente le tiers des plaintes enregistrées et près de 25 % des annonces sur Alphabay. On distingue notamment le vol et recel de données de carte bancaires dit carding, le trafic de fausse monnaie et de faux documents. Moins spectaculaires que les trafics évoqués supra, ces infractions touchent néanmoins un nombre plus important de victimes. Les infractions économiques et financières sont facilitées par la mise à disposition de logiciels malveillants, de guides méthodologiques ou encore de kits de piratages. Ces outils sont régulièrement consacrés au piratage de sociétés ou au vol de données privées. Les annonces pour ce type de produits représentent moins de 2 % des offres sur Alphabay. Ce chiffre est toutefois trompeur car l'impact de la vente de ces dispositifs est conséquent. Les atteintes aux systèmes de traitement automatisé des données ont représenté 18 % des plaintes en lien avec le darkweb. Cet écart s'explique notamment par le caractère multi-cibles des attaques, un logiciel malveillant pouvant servir à pénétrer un nombre important de systèmes.

Les atteintes aux personnes

Exclue des places hébergées par d'autres sites criminels, la communauté pédophile se retrouve sur des forums spécifiques. Toujours présents sur le web de surface via les réseaux peer to peer, les pédophiles déplacent progressivement leur activité sur le darkweb, dont le caractère technologique ne constitue plus un obstacle. En outre, l'accès de plus en plus précoce à des appareils électroniques connectés risque d'augmenter significativement le nombre de victimes potentielles. Par ailleurs, des « kits de suicide » ou des « kits du violeur », ces derniers comprenant notamment la vente de GHB, sont accessibles sur le darkweb, bien que leur impact soit difficile à évaluer.

Produits pharmaceutiques illicites ou détournés à d'autres fins

L'OCLAESP[12] réalise des veilles ciblées, d'initiative, sur le clearweb et le darkweb ou dans le cadre d'alertes d'autorités étrangères ou de signalements en provenance de la plateforme Pharos. Ces veilles permettent de se tenir informé des pratiques de détournement des produits pharmaceutiques. En 2017, cet office s'est intéressé au Fentanyl (analgésique opioïde), suite au signalement par le Canada de l'existence de nombreux décès liés à son usage détourné à des fins stupéfiantes. Suite aux signalements par Pharos et du pôle santé du parquet de Paris, il a également réalisé une veille sur les kits « suicide » contenant du Nembutal. Barbiturique utilisé comme anesthésiant/euthanasiant vétérinaire en France, il est utilisé dans d'autres pays dans le cadre de l'assistance à la fin de vie (Belgique et Suisse en Europe).

(12) Office central de lutte contre les atteintes à l'environnement et à la santé publique

Opération « PANGEA »

L'OCLAESP participe à cette opération internationale, menée sur Internet et destinée à la lutte contre les ventes illicites de produits alimentaires contrefaisants et/ou ne répondant pas aux normes du marché, coordonnée notamment par Interpol et l'Organisation Mondiale des Douanes (OMD). « PANGEA X » s'est déroulée du 12 au 19 septembre 2017 dans près de 100 pays et a impliqué de nombreux services français[13]. Elle a donné lieu à un grand nombre d'arrestations et de constatations dans le monde entier, ainsi qu'à la saisie de milliers de médicaments potentiellement dangereux.

Le bilan de l'opération en France s'établit comme suit :
– 433.023 produits de santé illicites ainsi que 1 404 kg de produits de santé en vrac, saisis par les douanes ;
– l'identification de 11 sites Internet illégaux de vente de médicaments qui ont fait l'objet de procédures judiciaires par l'OCLAESP et le SCRC/C3N.

1.2 Enjeux économiques des cybermenaces

Le cyberespace est devenu un lieu de confrontation. Les attaques à l'encontre des systèmes informatiques de l'État, des infrastructures critiques, des entreprises ou des citoyens sont quotidiennes, sans que l'on puisse toujours en saisir l'origine et en comprendre les motivations, ni même distinguer avec certitude qui, acteurs étatiques ou non étatiques, en sont les commanditaires et les exécutants.

Les attaquants informatiques peuvent conduire aussi bien des opérations très ciblées que des actions massives et indiscriminées ; ils poursuivent quatre types d'objectifs, non exclusifs entre eux : l'espionnage, les trafics illicites et le profit, le sabotage, la déstabilisation et les attaques informationnelles.

Les attaques « WannaCry » et « NotPetya » en mai et juin ou encore le piratage des courriels d'un important cabinet d'audit et de conseil en septembre ont rappelé la réalité des cybermenaces qui pèsent sur l'économie et la société.

Pour les organisations, les atteintes motivées par l'appât du gain, l'espionnage pour obtenir un avantage concurrentiel ou le sabotage ont des incidences financières et réputationnelles. Aussi, elles doivent absolument prendre la mesure de la gravité de ces cybermenaces, car si leur responsabilité peut être engagée (il est rappelé à cet égard les obligations imposées tant par la loi relative à l'informatique, aux fichiers et aux libertés de 1978 que par le nouveau règlement européen sur la protection des données, RGPD/GDPR, qui entrera en application le 25 mai 2018), elles risquent également de disparaitre.

Pour se protéger, elles disposent de deux outils principaux complémentaires, la prévention et le transfert de risque par le biais de l'assurance, dont la couverture du risque cyber commence à se développer. Nécessaire, la prévention se traduit aujourd'hui prioritairement par la sensibilisation et la formation des personnels, qui restent le maillon faible de la cybersécurité.

(13) OCLAESP, services douaniers (DNRED, SNDJ), Agence nationale de sécurité du médicament, OCLCTIC, C3N…

1.2.1 Le développement du marché de la cybersécurité

La valeur économique d'une entreprise se mesure aujourd'hui également à son degré d'exposition aux cyber-risques ; l'offre de cybersécurité s'est accrue sensiblement et les entreprises du secteur sont désormais en mesure de proposer des solutions adaptées à chacune.

Selon l'étude du pôle interministériel de prospective et d'anticipation des mutations économiques (PIPAME)[14] de novembre 2015 et les données présentées à l'occasion du salon MILIPOL 2017, la cybersécurité représenterait en France près de 12,3 % du chiffre d'affaires marchand de la filière nationale de la sécurité.

Le rapport 2017 de l'observatoire de la filière de la confiance numérique[15], qui couvre le marché de la cybersécurité proprement dite et des produits et solutions de sécurité numérique, estime que ce secteur représente plus de 850 entreprises. 80 % de ces sociétés réalisent moins d'un million d'euros de chiffre d'affaires. Au total, la cybersécurité représente un chiffre d'affaires de 4,3 M€ et la sécurité numérique[16] 4,5 M€. La croissance annuelle moyenne du secteur est forte (12,4 %). Le nombre de personnes employées dans le secteur est estimé à 60 000.

Selon ces études, ce secteur bénéficie d'opportunités réelles de développement avec la prise de conscience des enjeux de sécurité, des réglementations nouvelles, l'émergence de thèmes nouveaux (objets connectés, villes intelligentes, automobiles connectées, transformation numérique, « privacy by design », Big Data, intelligence artificielle, etc...).

Concomitamment, le développement du marché de l'assurance cyber permet aux entreprises de réduire l'impact financier lié à une cyber-attaque, voire de bénéficier le cas échéant de l'assistance d'experts mobilisés par l'assureur. Contribuant également à la prise de conscience, à l'encouragement des investissements et à l'amélioration de la réponse aux incidents cyber, ce marché de l'assurance s'étoffe progressivement, mais est encore embryonnaire sur le segment des PME. Estimé à 3,5 milliards de dollars, ce marché mondial est très inégalement réparti entre le continent américain (85 % du marché) et l'Europe (5 %).

La perception par les chefs d'entreprise reste difficile en raison de la singularisation du risque cyber et de ses caractéristiques diamétralement opposées au risque industriel, par nature plus stable et circonscrit[17].

La propriété intellectuelle, la réputation, la perte d'opportunité sont des actifs intangibles particulièrement exposés au risque cyber. Leur poids dans la valorisation des entreprises a considérablement augmenté et ils représentent désormais une part significative des pertes potentielles. Sur ce point, le marché n'est pas encore en mesure d'assurer ce type d'actifs de façon standardisée[18].

---

(14) Étude PIPAME « Analyse du marché et des acteurs de la filière industrielle française de sécurité », https://www.entreprises.gouv.fr/etudes-et-statistiques/analyse-du-marche-et-des-acteurs-la-filiere-industrielle-francaise-securite

(15) Étude commanditée par l'Alliance pour la Confiance Numérique (ACN) dans le cadre de son observatoire 2017 – 82 entreprises y ont contribués.

(16) La sécurité numérique englobe l'ensemble des solutions, matériels et installations dédiés à instaurer la confiance par la mise en œuvre de systèmes numériques (biométrie, gestion des accès, détection par exemple).

(17) Étude Bessé & PWC : «Les dirigeants d'ETI face à la menace cyber» mars 2018.

(18) Rapport du Club des juristes « Assurer le risque cyber », janvier 2018.

1.2.2 Contre-ingérence économique

Au-delà des enjeux liés à l'espionnage, au sabotage ou au terrorisme, les cyberattaques peuvent également constituer un vecteur d'ingérence économique efficace.

Elles peuvent ainsi permettre de capter une technologie ou un savoir-faire, d'acquérir une information stratégique, d'effectuer un chantage ou d'exiger une rançon, etc. Elles peuvent également avoir pour but de déstabiliser un acteur économique, une autorité de régulation ou encore un groupe de consommateurs, souvent à des moments « choisis stratégiquement » (contexte de fusion-acquisition, congés, publication d'un bilan, fin d'exercice budgétaire, etc.), en altérant le fonctionnement, la productivité ou encore en neutralisant tout ou partie des capacités de la cible, pendant un temps donné.

Ces aspects, liés au maintien des avantages concurrentiels des entreprises nationales, constituent un enjeu majeur pour les économies de marché occidentales, au sein desquelles les récentes crises ont affaibli nombre d'acteurs (baisse des commandes, besoins accrus en trésorerie, mouvements sociaux, etc.). Les ingérences sont susceptibles d'intervenir tout au long de la vie d'un organisme, à l'occasion de la participation à un séminaire, à un salon ou à un concours, lors d'une campagne de prospection commerciale, de tentative de pénétration d'un marché étranger ou lors de la négociation d'une augmentation de capital. Les atteintes au potentiel (scientifique, technique, économique, industriel, etc.) de la Nation résultant d'une cybermenace peuvent donc provoquer des dégâts considérables sur l'économie du pays, agir comme vecteur de déstabilisation et nuire, in fine, à la capacité de l'État à exercer sa pleine souveraineté et à agir indépendamment des interférences extérieures.

L'ingérence économique peut également servir de mécanisme de collecte d'informations de nature cyber. C'est le cas d'une démarche de mise en conformité soutenue par des cabinets de conseil et des sociétés d'investigation numérique étrangers, qui peut permettre d'accéder à des données techniques suffisantes pour engager une cyberattaque contre un acteur national.

1.3. Enjeux juridiques et normatifs des cybermenaces

Le ministère de l'Intérieur veille à l'adaptation constante des textes législatifs et réglementaires aux évolutions technologiques et comportementales en matière cyber, de façon à renforcer l'efficacité des moyens d'investigation et des dispositifs de prévention tout en veillant à trouver le juste équilibre entre d'une part, la sauvegarde de l'ordre public, la prévention et la répression des infractions et d'autre part, le respect de libertés individuelles.

La dimension internationale de la cybercriminalité implique également d'harmoniser les législations nationales ou à tout le moins, de faciliter la coopération au niveau européen et international afin de renforcer les moyens de lutte contre ce phénomène.

1.3.1 Évolution du cadre français

Droit interne

En 2017, deux textes législatifs sont à signaler particulièrement.

- Loi n° 2017-242 du 27 février 2017 portant **réforme de la prescription en matière pénale** a allongé les délais de prescription de l'action publique pour les crimes et délits.

Si cette modification n'est pas propre aux infractions considérées comme relevant de la cybercriminalité, elle impactera nécessairement les procédures en cette matière en permettant d'engager des poursuites et donc de procéder à des enquêtes pendant un délai plus long.

Désormais, le délai de prescription de l'action publique est de 6 ans pour les délits, contre 3 ans auparavant. Pour les infractions terroristes, à l'exception de la provocation et de l'apologie, ce délai est porté à 20 ans. Quant aux crimes, le délai de prescription de l'action publique passe de 10 à 20 ans. Il est de 30 ans pour les crimes terroristes.

En principe, ces délais courent du jour où l'infraction est commise. La loi du 27 février 2017 a toutefois maintenu le principe du report du point de départ pour les délits prévus à l'article 706-47 du code de procédure pénale lorsqu'ils sont commis sur des mineurs à la date de leur majorité. Elle a en outre consacré tout en l'encadrant le principe jurisprudentiel de report du point de départ du délai de prescription pour les infractions occultes ou dissimulées. Le délai ne commence à courir qu'à partir du moment où elles ont été découvertes sans toutefois que le délai de prescription ne puisse excéder 12 ans pour les délits et 30 ans pour les crimes à compter du jour de la commission de l'infraction.

Lors des débats parlementaires, la question de prévoir un délai de prescription propre aux infractions en matière de droit de la presse commises par l'intermédiaire d'un service de communication au public en ligne, passant de trois mois à un an, a de nouveau été soulevée. Elle a toutefois été écartée par l'Assemblée nationale considérant qu'elle ajoutait un nouveau régime dérogatoire injustifié au regard de l'impératif de protection de la liberté d'expression, qui vaut tout autant sur internet que pour la presse imprimée.

Si l'exercice de l'action publique en matière de provocation ou d'apologie d'actes de terrorisme est soumis au délai de prescription de droit commun, le délai de la prescription de la peine pour ces mêmes délits est à présent le même que pour l'ensemble des délits en matière de terrorisme, soit vingt années à compter de la date à laquelle la décision de condamnation est devenue définitive (au lieu de cinq années avant la loi du 27 février 2017).

- Loi n° 2017-1510 du 30 octobre 2017 renforçant **la sécurité intérieure et la lutte contre le terrorisme :**

Face à la persistance de la menace terroriste, cette loi dote l'État de nouveaux instruments permanents de prévention et de lutte contre le terrorisme permettant ainsi d'accompagner la fin de l'état d'urgence (1er novembre 2017). Elle instaure plusieurs mesures de police administrative, applicables jusqu'au 31 décembre 2020, dans le but de prévenir les actes de terrorisme.

Comme les précédents textes, la loi n° 2017-1510 du 30 octobre 2017 prend en compte l'utilisation qui peut être faite des moyens informatiques et numériques dans les dispositifs de lutte contre le terrorisme afin de renforcer leur efficacité.

Les saisies et visites domiciliaires administratives

Le nouvel article L. 229-5 du Code de la sécurité intérieure prévoit que, lorsque la visite révèle l'existence de données relatifs à la menace d'une particulière gravité pour la sécurité et l'ordre publics que constitue le comportement de la personne concernée, il est possible de procéder à la saisie des données contenues dans tout système informatique ou tout équipement terminal présent sur les lieux de la visite, soit en procédant à une copie, soit par saisie de leur support lorsque la copie ne peut être réalisée pendant le temps de la visite. Cet article précise les conditions de leur exploitation et les modalités d'effacement des données et de restitution des supports.

L'extension des techniques spéciales d'enquêtes en matière d'atteintes aux intérêts fondamentaux de la Nation

Les techniques spéciales d'enquêtes, notamment celles qui comportent en elles-mêmes une dimension numérique[19] ou qui peuvent être mises en œuvre au moyen de communications électroniques (comme l'infiltration), antérieurement à cette loi, s'appliquaient à dix-neuf séries de crimes ou délits (articles 706-73 et 706-73-1 du code de procédure pénale). L'article 9 étend le recours à ces techniques pour certaines infractions relevant des atteintes aux intérêts fondamentaux de la Nation en modifiant les articles 706-73 et 706-73-1 du code de procédure pénale. Il s'agit des infractions de nature criminelle du titre I du livre 4 du Code pénal, comme par exemple l'intelligence avec une puissance ou une organisation étrangère en vue de susciter des actes d'agression contre la France ou le sabotage.

La captation des données informatiques échangées par protocole sans fil

Les techniques de renseignement concernant la captation de données informatiques ne prévoyaient que l'interception des données échangées avec des périphériques audiovisuels. La nouvelle loi modifie l'article L.853-2 du Code de la sécurité intérieure pour permettre la captation de données informatiques émises ou reçues quel que soit la nature du périphérique notamment des données informatiques transmises par le biais de réseaux sans fil (comme le « Wi-Fi »).

Accès en temps réel aux données de connexion de l'entourage d'une personne présentant une menace terroriste

La loi n° 2016-987 du 21 juillet 2016 avait élargi le recours administratif à ce type de technique de renseignement à l'environnement de la personne visée. Cependant, aucune limite ne venant circonscrire cette notion d'entourage, le Conseil constitutionnel l'avait censuré, avec un effet différé au 1er novembre 2017.

Cette nouvelle loi a pour objectif de trouver un juste équilibre entre des mesures numériques nécessaires à la lutte contre le terrorisme et la protection des libertés individuelles.

Perspectives

Pour lutter efficacement contre les menaces actuelles ou émergentes, notamment contre les atteintes aux systèmes de traitement automatisé de données (systèmes d'information), il apparait nécessaire de développer d'autres approches en matière d'investigations.

En particulier, l'extension du champ d'application de la technique d'enquête sous pseudonyme[20] est souhaitable. En effet, son développement opérationnel constitue un enjeu majeur de l'efficacité de l'action des forces de l'ordre face aux évolutions des modes opératoires criminels sur les darknets. Parallèlement à l'extension de son champ d'application, il pourrait être procédé à l'harmonisation et la modernisation des régimes procéduraux de l'enquête sous pseudonyme.

(19) L'enquête sous pseudonyme, la captation de données informatiques et le recours à l'Imsi catcher.

(20) Pour certaines infractions limitativement énumérées par la loi, l'enquête sous pseudonyme consiste pour des agents spécialement habilités à interagir, en utilisant un pseudonyme, avec les suspects par échanges électroniques afin de recueillir des éléments de preuve d'une infraction, et ce sans aucune provocation à la commettre.

1.3.2 L'impact des directives et règlements européens et de la jurisprudence de la CJUE sur la lutte contre les cybermenaces

Plusieurs textes concernent directement la lutte contre les cybermenaces en Europe. Présentant divers champs d'application, ils nécessitent, le cas échéant, une transposition en droit national. A ce titre, on peut citer :

- La directive 2013/40/UE[21] du Parlement européen et du Conseil du 12 août 2013 relative aux **attaques contre les systèmes d'information** et remplaçant la décision-cadre 2005/222/JAI du Conseil. La France est en conformité avec cette directive et a procédé à des compléments de transposition :
  - avec le décret n° 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale,
  - les arrêtés de juin et août 2016 fixant les règles de sécurité et les modalités de déclaration des systèmes d'information d'importance vitale et des incidents de sécurité relatives à chaque secteur ou sous-secteur d'activités d'importance vitale
  - et la loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.

La Commission a publié le 13 septembre 2017 un rapport sur l'évaluation de la transposition de cette directive.

- **Le règlement (UE) 2016/679**[22] du 27 avril 2016 relatif à « la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE » (règlement général sur la protection des données ou RGPD) et **la directive (UE) 2016/680**[23] relative à « la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil ». Cette directive (UE) 2016/680 devra être transposée pour le 6 mai 2018. Le gouvernement a déposé le 13 décembre 2017 un projet de loi relatif à la protection des données personnelles pour adapter en ce sens la loi n° 78-17 du 6 janvier 1978 relative à l'informatique et aux libertés.
- La directive (UE) 2016/1148[24] du 6 juillet 2016 concernant des mesures destinées à assurer **un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union** (directive NIS). Cette directive a été transposée par la loi n° 2018-133 du 26 février 2018. Cette transposition aura des conséquences sur les relations entre acteurs de cybersécurité au niveau national. Des décrets et arrêtés sont encore attendus pour préciser les services essentiels retenus par la France et les mesures de sécurité applicables.
- La directive (UE) 2017/541[25] du 15 mars 2017 relative à la **lutte contre le terrorisme** remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil qui définit les infractions de nature terroriste et prévoit des peines minimales correspondantes. Elle oblige les États membres à incriminer la provocation publique à commettre une infraction terroriste. Elle comprend également une obligation pour les États

(21) http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32013L0040
(22) http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679
(23) http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680
(24) http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148
(25) http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32017L0541

membres de prévoir des mesures de suppression des contenus constituant une provocation publique à commettre une infraction terroriste s'ils sont hébergés sur leur territoire. Les États membres doivent faire leur possible pour obtenir le retrait de ces contenus s'ils sont hébergés en dehors de leur territoire. Si une suppression à la source n'est pas possible, les États membres peuvent aussi mettre en place des mécanismes pour bloquer l'accès à ces contenus depuis leur territoire.

- La révision de la directive **service de médias audiovisuels** (SMA) 2010/13/UE[26] qui vise notamment à assurer la libre prestation de ces services au sein de l'Union. Actuellement, elle dispose notamment que les services de médias audiovisuels ne peuvent contenir aucune incitation à la haine fondée sur la race, le sexe, la religion ou la nationalité. La Commission a déposé une proposition de révision de cette directive visant notamment à **inclure les services de plateforme de partage de vidéos dans le champ d'application** tout en faisant bénéficier ces opérateurs d'un régime différencié avec des obligations moindres. Si les négociations entre le Conseil et le Parlement européen ne sont pas achevées, on peut constater que les deux institutions souhaitent étendre l'interdiction des contenus haineux ou violents aux contenus comportant une incitation à commettre des actes terroristes.

- La décision-cadre 2008/913/JAI[27] relative à la **lutte contre le racisme et la xénophobie** incrimine l'incitation publique à la violence ou à la haine visant un groupe de personnes ou un membre d'un tel groupe, défini par référence à la race, la couleur, la religion, l'ascendance, l'origine nationale ou ethnique. En mai 2016, la Commission a conclu avec les principales plateformes (Facebook, Twitter, YouTube et Microsoft) un **code de conduite** sur la lutte contre les discours de haine en ligne. Les opérateurs s'engagent notamment à examiner rapidement (24 heures) les demandes de retrait de contenus haineux. Dans le cadre de la mise en œuvre de ce code de conduite, la Commission a procédé depuis à trois opérations de test de signalement de contenus haineux pour vérifier la réactivité des opérateurs. Les résultats sont en constante progression (28 % de retraits lors de la 1re phase, 59 % lors de la 2e 70 % lors de la 3e en novembre-décembre 2017). Il convient également de noter qu'un plan national de lutte contre le racisme et l'antisémitisme a été présenté le lundi 19 mars 2018 par le Premier ministre dont la visée première est la lutte contre la haine en ligne. A ce titre, plusieurs objectifs sont retenus notamment la construction à l'échelle européenne d'un cadre juridique de la responsabilité des plateformes numériques pour les contenus haineux, racistes et antisémites et l'évolution de la législation nationale pour lutter de façon plus efficace contre la haine sur internet.

- Depuis le second semestre 2015, il est discuté des difficultés liées à **l'obtention de preuves électroniques dans le cadre des procédures pénales.** Ces discussions ont abouti à l'adoption en juin 2016 de conclusions par le Conseil sur l'amélioration de la justice pénale dans le cyberespace[28]. La Commission, chargée de suivre la mise en œuvre de ces conclusions, a organisé en 2017 des réunions avec un groupe d'experts informel comprenant des représentants des autorités des États membres et des personnes issues de la société civile, et lancé une consultation publique sur la question. Après avoir finalisé l'analyse de ces différentes contributions, elle déposera en avril 2018 une proposition de directive concernant l'accès transfrontière aux preuves électroniques en matière pénale *(e-evidence)*.

(26) http://eur-lex.europa.eu/legal-content/FR/AUTO/?uri=CELEX:02010L0013-20100505&qid=15156753676 32
(27) http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32008F0913
(28) http://www.consilium.europa.eu/fr/press/press-releases/2016/06/09/criminal-activities-cyberspace/

Jurisprudence

Par un arrêt du 21 décembre 2016[29] la Cour de justice de l'Union européenne s'est prononcée dans deux affaires, en Suède et au Royaume-Uni, portant sur l'obligation imposée aux fournisseurs de services de communications électroniques, de conserver de façon généralisée et indifférenciée, les données relatives à ces communications. La CJUE a indiqué que le droit de l'Union, à savoir la directive vie privée et communications électroniques 2002/58/CE, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, s'opposait à une réglementation nationale prévoyant une conservation généralisée et indifférenciée des données de trafic et supposait que l'accès aux données conservées s'effectue après un contrôle préalable par une juridiction ou une autorité administrative indépendante.

Au sein du Conseil, un groupe de travail (« DAPIX ») a été mandaté début 2017 afin d'identifier, avec la Commission et les agences Europol et Eurojust, des solutions aux difficultés opérationnelles et juridiques soulevées par cet arrêt.

Par ailleurs, deux questions préjudicielles relatives à la conservation des données de trafic et de localisation ont été posées à la CJUE et sont pendantes.

Dans l'affaire C-207/16 *(Ministerio Fiscal)*, la CJUE est interrogée sur la notion de « gravité suffisante de l'infraction » permettant de justifier la conservation des données.

Dans l'affaire C-623/17 *(Privacy International),* il est demandé à la CJUE d'indiquer si la conservation des données pour des finalités liées à la sécurité nationale et au renseignement relève ou non du champ d'application du droit de l'Union et de la directive vie privée et communications électroniques.

Travaux au niveau de l'Union européenne

En décembre 2016, le Conseil de l'UE a mandaté la Commission pour entamer une démarche exploratoire sur les solutions à offrir aux services d'investigations judiciaires en matière de chiffrement. La Commission a examiné le rôle du chiffrement dans le cadre des enquêtes pénales lors d'une série de consultations techniques et juridiques auprès de 50 experts des agences européennes, de la société civile, du secteur privé, des agences non gouvernementales et des autorités des États Membres. En octobre 2017, la Commission a présenté ses conclusions au conseil JAI, indiquant qu'il conviendrait de mettre en œuvre un ensemble de mesures juridiques visant à faciliter l'accès à des éléments de preuve chiffrés, ainsi que des mesures techniques visant à renforcer les capacités de déchiffrement. En particulier, il est recommandé de continuer à développer les capacités de déchiffrement d'Europol et de mettre en place un réseau de points d'expertise. La mise en œuvre de ces mesures est attendue en 2018.

En raison de la prochaine entrée en vigueur de la législation européenne relative à la protection des données (RGPD), l'accès à la base de données des noms de domaines dénommée WHOIS est amené à évoluer. Sous la supervision du comité permanent de sécurité intérieure (COSI) du Conseil, Europol a débuté fin 2017 des travaux sur la question de la réforme du WHOIS. Des discussions vont être initiées entre l'Union Européenne et l'organisme en charge de la gestion de cette base de données dénommé « Internet Corporation for Assigned Names and Numbers » (ICANN). Consciente de son importance cruciale pour les forces de sécurité dans

(29) Tele2 Sverige : http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0 &doclang=FR&mode=req&dir=&occ=first&part=1&cid=557470

le cadre de leurs enquêtes, l'UE reconnait l'importance de conserver un accès rapide et complet à cette base de données de manière à permettre aux forces de sécurité d'assurer leurs missions régaliennes tout en se conformant aux règles énoncées dans le RGPD visant à la protection des données personnelles.

1.3.3 Conseil de l'Europe, Assemblée générale des Nations Unies (AGNU) et G7

La convention du Conseil de l'Europe sur la cybercriminalité[30] signée le 23 novembre 2001 à Budapest reste à ce jour le seul instrument international contraignant en matière de lutte contre la cybercriminalité.

Un deuxième protocole additionnel à cette convention est en cours de rédaction depuis septembre 2017, les travaux sont suivis par le ministère de l'Intérieur avec grande attention. Ce protocole envisage des mesures visant à simplifier la coopération judiciaire entre les 56 pays adhérents à la convention et à faciliter la coopération directe avec les fournisseurs de services sur Internet des autres pays membres. Sont notamment étudiés de meilleures possibilités d'accès transfrontalier aux données par les services d'enquête, un cadre simplifié pour les demandes d'entraide judiciaire concernant les données d'abonnés et une formalisation des procédures d'urgence. Les travaux dans ce cadre prévoient d'ores et déjà d'assurer une cohérence avec les travaux en cours dans le cadre de l'Union Européenne. La conclusion de ce projet est attendue pour 2019.

Dans le cadre de l'Assemblée générale des Nations Unies, la Commission pour la prévention du Crime et la Justice pénale a été chargée de constituer en 2011 un groupe intergouvernemental d'experts (IEG), dédié à la rédaction d'une étude approfondie sur le phénomène de la cybercriminalité.

Ce groupe a rendu son rapport en 2013 ; il a été mis en évidence une division de la communauté internationale sur l'opportunité de compléter ou non le cadre juridique existant.

L'IEG a pu se réunir à nouveau en avril 2017 et le ministère de l'Intérieur y était représenté. Les débats ont à nouveau été marqués par des divergences importantes sur les instruments juridiques internationaux à utiliser dans la lutte contre la cybercriminalité. Une majorité d'États, dont la France, se sont montrés réticents à un nouveau texte juridique international, se prononçant en faveur de l'utilisation de la Convention de Budapest comme base juridique pour la lutte contre la cybercriminalité. Les promoteurs d'un nouveau texte international (BRICS[31], Iran, Soudan) restent opposés à cette approche arguant du manque d'universalité de la Convention de Budapest et de ses supposées lacunes juridiques, techniques et procédurales. Le groupe d'expert a été prorogé avec pour mandat de discuter notamment de l'assistance technique, à l'exclusion de tout point relatif à la création d'un nouvel instrument international.

Lors de la réunion des ministres de l'Intérieur du G7 à Ischia, les 19 et 20 octobre 2017, la France, l'Allemagne et le Royaume-Uni ont rappelé que le retrait rapide des contenus terroristes en ligne (sous 1 à 2 heures après publication) est un enjeu prioritaire pour renforcer notre capacité collective à prévenir et lutter contre le terrorisme[32].

(30) http://conventions.coe.int/Treaty/FR/Treaties/Html/185.htm
(31) Brésil, Russie, Inde, Chine et Afrique du Sud
(32) Texte adopté : http://www.g7italy.it/sites/default/files/documents/Joint%20Communiqu%C3%A9.pdf

1.3.4 Coopération internationale

Face aux enjeux de sécurité liés aux technologies de l'information et de la communication, l'action des services du ministère de l'Intérieur au plan international, animée par la Direction de la Coopération Internationale (DCI), est multiple et en constante augmentation.

Les actions de coopération cyber ont été multipliées par quatre depuis 2014, avec une augmentation de 130 % en 2017 par rapport à 2016, principalement dans le domaine de la formation de personnels (notamment d'Afrique francophone) en vue d'optimiser la coopération dans un souci de retour en sécurité intérieure.

Une coopération plus structurelle s'est également mise en place dans ce domaine avec la création d'un poste d'expert technique international (ETI) spécialisé dans la thématique cyber implanté depuis mars 2017 à Dakar, chargé de mettre en place une plateforme cyber dédiée à la lutte contre le terrorisme, la radicalisation et la cybercriminalité, en plus du poste d'ETI mis en place à Pretoria (Afrique du Sud) en 2016. Enfin un poste d'officier de liaison sur la thématique cyber, rattaché au service de sécurité intérieure de Washington, a également été créé en septembre 2017.

De même, un projet innovant de création d'une École Nationale à Vocation Régionale (ENVR) à Dakar dans le domaine cyber a été validé en 2017. L'objectif de cette école sera de dispenser des formations initiales et continues sur des thématiques très diverses : cyberdéfense (armée), cybersécurité (secteur public et privé), cybercriminalité, cyberactivisme, cyberpropagande, cyberdjihadisme, etc… aux différents acteurs publics et privés des pays francophone d'Afrique de l'ouest. Deux ETI seront ainsi recrutés au premier semestre 2018 (un chef de projet et un formateur) et affectés au sein de cette école qui devrait ouvrir ses portes en novembre prochain.

Enfin, la DCI a particulièrement mobilisé le réseau des 74 services de sécurité intérieure implantés à l'étranger afin de développer la remontée d'information depuis l'étranger dans le but d'identifier de nouvelles menaces, de rapporter des bonnes pratiques, d'observer les réformes juridiques, au service des directions opérationnelles du ministère de l'intérieur.

L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) est régulièrement engagé dans les dispositifs organisés par la DCI, ou le Conseil de l'Europe, par exemple les programmes GLACY+ et CyberSouth qui se sont traduits en 2017 par deux missions d'évaluation en Tunisie et en Algérie.

Le chef de l'OCLCTIC assure depuis mars 2017 la présidence de l'European Cybercrime Task Force (EUCTF) qui est une enceinte, intégrée au sein d'Europol (EC3), qui réunit les chefs des unités nationales de lutte contre la cybercriminalité de l'Union Européenne, des représentants d'Europol, d'EuroJust, d'Interpol et de la Commission Européenne. Ses missions consistent à développer et promouvoir une approche harmonisée des stratégies de lutte contre la cybercriminalité au sein de l'Union Européenne. A la fois un organe de consultation et de coopération internationale, elle participe activement aux actions opérationnelles d'Europol (Action Plan) et a la capacité de porter des projets stratégiques devant les instances de l'Union.

Partie II

Usages et phénomènes

Les principaux enjeux stratégiques ayant été identifiés, il convient de préciser **les usages** des citoyens, des collectivités, des administrations et des entreprises, ainsi que **les phénomènes** observés. Cette approche permet éventuellement de confirmer les priorités identifiées ou d'envisager des sujets émergents auxquels il faut se préparer.

Tout nouveau produit ou service numérique reste une cible potentielle des cybermalveillances. Toute vulnérabilité dans les systèmes et les plateformes numériques sera systématiquement exploitée.

2.1 Usages

2.1.1 Internet, médias sociaux et smartphones

En décembre 2017, le taux de pénétration de l'Internet[33] est de 54,4 % au niveau mondial, 85,2 % en Europe, 86,8 % en France. La croissance de l'Internet mobile[34] est la plus forte dans les régions en voie de développement ; fin 2017, le taux de pénétration de ces équipements y atteint 49 %.

Les sites Internet les plus visités en France[35] sont en septembre 2017 : Google, Facebook, Youtube, Microsoft, Orange, Windows Live, Amazon, Wikipédia, Leboncoin, puis MSN, Bing, Free, Impots.gouv.fr, Pages Jaunes et Yahoo.

L'usage des réseaux sociaux[36] est toujours en hausse, avec environ 2,9 milliards d'utilisateurs au niveau mondial selon les estimations, ainsi qu'un nombre d'utilisateurs réguliers en janvier 2018 de 2,16 milliards pour Facebook, 1,5 milliards pour Whatsapp, ou encore 330 millions pour Twitter et 300 millions pour Skype. Le classement est évidemment variable dans les différents pays, avec un taux d'usage important des réseaux sociaux chinois (comme QQ avec 843 millions d'utilisateurs dans le monde) ou russes (comme Vkontakte avec 97 millions d'utilisateurs) dans leurs pays d'origine. Le taux de pénétration des grands réseaux sociaux en France est de 56 % (nombre de comptes par rapport à la population[37]) et la durée moyenne d'utilisation quotidienne de 1,3 heures. En France[38], les réseaux sociaux les plus importants sont Facebook (31 millions de visiteurs uniques par mois), YouTube (26), Twitter (13,6), Instagram (11,9), Snapchat (10,1), LinkedIn (9) et WhatsApp (9).

Les achats en ligne[39] se développent avec 76 % des habitants ayant réalisé un achat au cours du mois de janvier 2017 au Royaume-Uni, 72 % en Allemagne, 67 % aux USA ou encore 62 % en France. La banque en ligne, quant à elle, est utilisée par 34 % des Français, chiffre en forte hausse.

Depuis quelques années, on constate l'émergence du smartphone comme plateforme multi-usages. Globalement en Europe, le trafic Web est plus élevé sur smartphone que sur poste informatique ; ce n'est pas encore le cas en France, mais la hausse annuelle de l'usage du smartphone y est conséquente. En 2017, on utilise en France autant le smartphone qu'un ordinateur pour aller sur les réseaux sociaux ou écouter de la musique, un peu moins le smartphone que l'ordinateur pour effectuer une recherche ou consulter ses mails. D'autres usages du smartphone sont en augmentation : bien évidemment la prise de photos (chute importante des ventes d'appareils photos) et de plus en plus pour consulter ses comptes bancaires…

(33) http://www.internetworldstats.com/
(34) https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf
(35) http://www.statista.com/statistics/473883/sites-internet-les-plus-visites-france/
(36) http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
(37) We Are Social Singapour: http://fr.slideshare.net/wearesocialsg/
(38) https://www.blogdumoderateur.com/50-chiffres-medias-sociaux-2017/
(39) We Are Social Singapour: http://fr.slideshare.net/wearesocialsg/

2.1.2 Le développement des crypto-monnaies

L'irruption des monnaies virtuelles dans le cyberespace à la fin des années 2000 a constitué une véritable révolution technologique en matière financière. Unités de compte n'ayant pas de statut légal, elles ne sont régulées par aucune banque centrale. Leur création repose sur un processus technologique popularisé sous le nom de Blockchain, entièrement déconnecté des établissements financiers traditionnels. Il existe plusieurs centaines de cryptomonnaies, les plus connues étant *Bitcoin, Ethereum* et *Monero*…

Le phénomène a trouvé un écho bien au-delà du public visé à sa création, notamment par le biais du succès rencontré par le Bitcoin, monnaie virtuelle bidirectionnelle, à savoir convertible en devises légales et bénéficiant d'un cours de change permettant d'effectuer le chemin inverse, d'une devise vers le Bitcoin. A l'origine simple « jouet » de mathématiciens, d'informaticiens et d'amateurs de jeux vidéo, le Bitcoin, créé en 2009, a progressivement suscité l'avènement d'un véritable écosystème international d'entreprises : d'une part les « mineurs » qui mettent à disposition leurs calculateurs pour valider cryptographiquement les transactions (opération appelée minage) et qui obtiennent en échange le droit de générer/miner de nouveaux Bitcoins, d'autre part les opérateurs privés de change avec des monnaies ayant cours légal et les intermédiaires de paiement en bitcoin sur l' « Internet légal ».

Le Bitcoin peut être utilisé pour ordonner des virements internationaux de façon rapide, simple et à moindre coût comme pour régler des achats en ligne tout à fait légaux. Témoins de l'installation de plus en plus marquée du Bitcoin dans l'économie réelle, des sites se sont spécialisés dans la présentation de répertoires de commerçants acceptant les paiements en bitcoins (bitcoin.paris). Matériel informatique, bars, restaurants, voyages, consultations médicales, vêtements, l'éventail des possibilités est large et a tendance à se développer. Le Bitcoin serait ainsi accepté[40] par plus de 100 000 commerces dans le monde, y compris des grandes sociétés comme Microsoft, Dell ou Paypal.

Ce volet légal a malheureusement un pendant illégal. Sur Internet en général et sur le darkweb en particulier, le Bitcoin est le moyen de paiement le plus répandu pour les transactions illicites, comme en témoignent de nombreuses affaires traitées par les services judiciaires depuis 2015 (trafic de stupéfiants, d'armes, de faux documents, vente de services de piratage informatique, paiement de rançons liées à des « sextorsions » ou à des « rançongiciels », etc).

La question de l'encadrement réglementaire des monnaies virtuelles s'est rapidement imposée dans les débats nationaux[41], car un contrôle normatif est susceptible de répondre à une série de risques liés à l'utilisation de ces supports en matière de financement du terrorisme et de blanchiment d'argent[42]. Plus largement, le recours massif au Bitcoin sur les places de marché illégales hébergées sur le darkweb et proposant à la vente des stupéfiants, des armes à feu ou encore des médicaments met l'accent sur les connexions entre monnaie virtuelle et criminalité.

Pour blanchir les revenus de leurs escroqueries, les cryptomonnaies sont un moyen privilégié pour les cybercriminels. Les nouvelles cartes prépayées, dites « Bitcards », adossées au Bitcoin ou d'autres cryptomonnaies, constituent pour eux une opportunité dont l'usage devrait se développer.

Depuis la fin de l'année 2017, le minage de cryptomonnaie clandestin (cryptojacking) se développe et devient peu à peu l'un des nouveaux outils préférés des cybercriminels qui prennent le contrôle de réseaux d'ordinateurs à l'insu de leur titulaire. Ainsi, le service Coinhive propose de miner des cryptomonnaies, principalement Monero, en tâche de fond, directement dans le navigateur de

(40) *http://www.ibtimes.co.uk/bitcoin-now-accepted-by-100000-merchants-worldwide-1486613*
(41) *La Chine est un des rares pays à avoir interdit l'usage du bitcoin*
(42) *Rapport de juin 2014 piloté par TRACFIN sur l'encadrement des monnaies virtuelles et remis au ministre de l'économie et des finances*

l'utilisateur, grâce à un code JavaScript que l'administrateur de la page peut facilement intégrer à son site. L'idée s'est depuis répandue et les modules permettant de miner de la cryptomonnaie dans le navigateur de l'utilisateur, sans avoir recueilli son consentement, se sont multipliés.

2.1.3 L'Internet des objets (IoT)

On entend par « objets connectés » l'ensemble des objets physiques interagissant entre eux et/ou avec des individus via des réseaux de communication (par exemple un pacemaker), et qui collectent des données relatives à leur état et à celui de leur environnement. Il est l'une des sources à l'origine du « Big Data ». IBM estime que le volume total de données échangées par les objets connectés en 2016 se compte en zettaoctets[43].

En 2017, d'après une étude[44], 52 % des Français interrogés possèdent au moins un objet connecté hormis leur smartphone et en 2020, chaque individu aura en moyenne trois objets connectés sur lui. D'ici là, deux milliards d'objets de ce type seront vendus en France. Le marché français de l'Internet des objets est estimé à près de 10 milliards d'euros et ce chiffre devrait doubler d'ici 2019.

Les objets connectés recueillent des données personnelles auprès des utilisateurs ou de leur environnement ; à ce titre, ils sont soumis au respect de la vie privée et à la protection des données. A la fois cibles et vecteurs des cyberattaques, ils constituent aussi une opportunité pour les services du ministère de l'Intérieur.

Objets connectés et protection des données

La loi « informatique et libertés » (LIL) du 6 janvier 1978 pose un cadre qui est toujours d'actualité en ce qui concerne la collecte et l'utilisation de données à caractère personnel. Pour la protection des individus, l'article 7 de la LIL pose le principe de consentement préalable à tout traitement des données. Le consentement comme base légitime de traitement de données personnelles, a connu des évolutions importantes, dans un objectif de protection accrue des personnes. Le RGPD reprend et renforce les principes imposés par la LIL (proportionnalité, pertinence, durée et finalité), pour tout traitement de données à caractère personnel en promouvant la responsabilisation des gestionnaires de ces traitements. Si la plupart des formalités préalables à la mise en œuvre d'un traitement devant la CNIL sont supprimées, subsisteront les obligations particulières, pour les traitements les plus sensibles (analyse d'impact, demande d'autorisation), tandis que les pouvoirs de contrôle et de sanction de la CNIL seront renforcés.

En outre, les opérateurs économiques vont se voir imposer une obligation de protéger la vie privée dès la conception (concept de « Privacy by Design »).

Les objets connectés face aux cyberattaques

Du fait de leur développement, **les objets connectés augmentent considérablement la surface d'attaque** pour les cybercriminels. **Ils sont largement vulnérables** et peuvent être les vecteurs de cyberattaques notamment en déni de service. En effet, la préoccupation de la « sécurité informatique » n'est toujours pas très répandue parmi les fabricants de ces objets, notamment en raison des coûts induits. Ceci aboutit parfois à des solutions techniques mal sécurisées : absence de mots de passe, service web présentant des failles de sécurité qui laissent accéder à toute sa base de données, absence de certification… Les risques sont bien réels.

(43) Un zettaoctet (1021 octets) soit 1.000 milliards de milliards d'octets
(44) Deuxième baromètre des objets connectés OpinionWay à l'occasion du salon Distree#Connect 2017

Selon la CNIL, le risque le plus important est la réutilisation malveillante des informations personnelles volées pour accéder à d'autres comptes en ligne de ces personnes, à des moyens de paiement ou à des demandes de crédits. L'autre risque majeur est celui d'actions ciblées de la part de personnes malveillantes (hameçonnage, harcèlement) touchant potentiellement des enfants et leur famille à travers des messages très personnalisés.

Objets connectés et opportunités pour les services de sécurité

Les objets connectés présentent de nombreuses opportunités pour les activités des forces de sécurité, que ce soit pour la sécurité publique, la police judiciaire ou le renseignement.

En effet, l'exploitation des objets connectés utilisés par des victimes ou par des criminels (montres GPS, pacemakers, bracelets connectés Fitbit…) est aussi susceptible d'orienter utilement les investigations judiciaires, en fournissant des données utiles à l'enquêteur. Voici quelques exemples.

Suite à un meurtre dans l'Arkansas, la justice a demandé en décembre 2016 à Amazon de livrer les enregistrements stockés sur leur serveur, car un objet connecté, un assistant virtuel « Echo », se trouvait sur les lieux du crime. Cette enceinte est dotée d'un micro qui détecte les voix, et peut exécuter un ordre.

Fin 2016 aux États-Unis, un homme qui menait une double vie, finissait par tuer sa femme. Il maquillait son meurtre, en faisant croire à un cambriolage qui aurait mal tourné alors qu'ils se trouvaient tous les deux au domicile conjugal. À l'arrivée des policiers que l'homme avait lui-même appelé, ce dernier était ligoté et le cadavre de sa femme se trouvait juste devant lui. L'exploitation du bracelet connecté Fitbit de la victime permettait de prouver que les propos tenus par son mari étaient mensongers.

Par ailleurs, l'usage de ces objets connectés par les forces de sécurité représente un risque avéré au regard de la possible récupération des données de géolocalisation par leurs adversaires, à l'instar des militaires en opération.

2.2. Phénomènes

Motivation, profil des auteurs

Les cyber-attaques peuvent être réalisées :

- à des fins crapuleuses, pour récupérer, exploiter ou revendre des données (fichiers clients, données bancaires, images intimes...) ;
- à des fins d'espionnage industriel pour des informations confidentielles des entreprises (vol de propriété intellectuelle) ;
- à des fins de déstabilisation (vol d'informations puis leur publication). Ces attaques ont pour objet et pour effet de porter atteinte à l'image de l'entreprise touchée. Elles révèlent ses vulnérabilités en matière de sécurisation des données et entament la confiance de ses clients ou de ses partenaires ;
- à des fins de sabotage en ayant pour effet d'interrompre, voire de stopper définitivement l'activité de l'entité ciblée.

Au risque financier, auquel sont classiquement confrontées les entreprises, s'ajoute une importante menace d'atteinte à leur image et à leur réputation, plus difficilement évaluable. La médiatisation de certaines cyber-attaques planifiées et organisées depuis l'extérieur de l'entreprise ne doit pas conduire à négliger les dangers venant de l'intérieur (salariés/sous-traitants…).

L'expérience opérationnelle montre l'accélération de la transformation numérique du paysage de la criminalité organisée.

Trafiquants de stupéfiants, cyber-escrocs, réseaux de pornographie enfantine, contrefacteurs... : Internet offre de multiples possibilités, pour ces groupes criminels organisés, d'atteindre un grand nombre de victimes potentielles, à court terme, à très faible coût et avec de nombreux avantages : éloignement par rapport aux victimes, échanges facilités entre complices, anonymisation, caractère transfrontalier de la fraude, possibilités multiples de blanchiment d'argent provenant de leurs activités illicites.

Ces groupes relevant de la criminalité organisée traditionnelle se sont très vite appropriés le Net, non seulement pour commettre leurs méfaits, mais aussi pour la vente des marchandises mal acquises. Produits stupéfiants, armes, faux billets, images pédopornographiques, données bancaires ou personnelles volées...sont vendus et achetés en monnaies virtuelles, sur des marchés parallèles, notamment sur les darknets.

Peu de criminels ont les connaissances et/ou les capacités nécessaires à la création de logiciels malveillants. Ils vont donc s'offrir les services de programmeurs ou codeurs de haut niveau qui fabriquent derechef ou sur demande des virus, chevaux de Troie, vers ou autres maliciels. Ces concepteurs de logiciels malveillants les utilisent eux-mêmes ou les vendent sur Internet, généralement sur des forums spécialisés et confidentiels, y compris sur les darknets, proposant même parfois un service d'aide en ligne. Ils doivent aussi louer des serveurs pour lancer leur attaque, recruter des individus prêts à servir de mules pour acheter des marchandises avec des données bancaires volées ou les réceptionner, s'acheter les services d'experts en montage financier pour blanchir leurs profits et brouiller les pistes de la fraude ainsi que d'autres personnels spécialisés dans le domaine des télécommunications pour agir en toute discrétion (notamment avec l'utilisation de techniques d'anonymisation et de chiffrement).

Il reste aussi possible pour les criminels de faire appel aux botmasters, ces délinquants qui contrôlent les Botnets (contraction de « Robots of the Network »), qui permettent notamment la diffusion ou l'installation de virus de récupération de données personnelles (y compris bancaires) ou l'envoi de spam et de phishing. Les Botnets sont des réseaux de machines (ordinateurs, téléphones mobiles, tablettes…) qui ont été infectés par un logiciel malveillant permettant leur contrôle à distance (on parle alors de machines Zombies). Ils sont composés de plusieurs milliers, voire plusieurs centaines de milliers d'ordinateurs.

Contrairement à ce que l'on peut penser de prime abord, il ne suffit pas de fabriquer ou d'acquérir un logiciel malveillant pour réussir une cyberattaque : l'aboutissement de celle-ci repose également sur un écosystème criminel, plus ou moins structuré.

Enfin, sur le plan de l'analyse des cybermenaces, la frontière entre la criminalité et les attaques informatiques d'origine étatique ou terroriste est de plus en plus poreuse :
– la prolifération : des groupes criminels diffusent et vendent à grande échelle du matériel illicite, des malwares, des vulnérabilités (cf. infra). Ils développent en outre des capacités participant à l'anonymisation de chaînes d'attaque ;
– la démultiplication des victimes : la cybercriminalité est pour partie une délinquance de masse ;
– l'externalisation : le recours par des entités étatiques à des criminels (sous-traitance à des individus ou groupes « mercenaires ») pour conduire des actions à leur profit ;
– l'obfuscation : l'utilisation par des entités étatiques des modes opératoires attribués à des mouvements criminels afin de démarquer leur action.

2.2.1 Vecteurs de diffusion des attaques et outils

Les virus se propagent traditionnellement par plusieurs modes :
- En **pièce jointe ou transfert de fichier** par courrier électronique ou sur un réseau social ;
- Par partage d'un fichier sur **un support amovible ou un partage réseau** ;
- Par **installation directe par l'utilisateur** (cas du téléchargement d'une application malveillante, installée volontairement, notamment sur les téléphones mobiles) ;

- Par **exploitation d'une vulnérabilité sur le système via une plateforme d'exploits** (ou exploit kit), vers lequel l'utilisateur est attiré ou redirigé dans sa navigation Internet (notamment en recevant un lien par courrier électronique ou sur un réseau social, mais aussi depuis des bannières publicitaires malveillantes ou la modification d'un site Web souvent visité – technique dite du trou d'eau) ;
- Par une personne malveillante au sein même de la structure ;

Enfin, c'est souvent un premier virus qui va être utilisé pour en installer d'autres.

Tous ces modes de diffusion doivent être pris en compte tant dans les messages de prévention, les méthodes de détection dans les réseaux des entreprises, que dans les stratégies d'enquête qui vont idéalement chercher à identifier la source des attaques.

2.2.1.1 Vulnérabilités

L'évolution du nombre des vulnérabilités, dans les systèmes d'exploitation ou les logiciels, est une donnée difficile à interpréter. En effet, elle révèle à la fois l'activité de ceux qui exploitent ces vulnérabilités (lorsqu'elles sont découvertes par l'action d'un groupe criminel), l'activité des chercheurs en sécurité ou encore la motivation des éditeurs (notamment lorsqu'ils mettent en place des programmes de publication des vulnérabilités qui touchent leurs produits ou de récompense pour les chercheurs qui les découvrent).

Toutefois, les exploitations de vulnérabilités dites « 0-day » ou « Zero-day » (zero-day exploit) découvertes au cours d'une année donnent une mesure intéressante de la menace observée. Ainsi, le nombre d'exploits basés sur des vulnérabilités 0-day aurait évolué[45] entre 2013 et 2015 pour passer de 23 découvertes à 54. Dans le même temps, le nombre total de « Zero-day », c'est-à-dire les vulnérabilités non découvertes par les fournisseurs de logiciels, sont en baisse entre 2014 et 2016[46], ce qui suggère que les programmes de bug bounties et la plus grande attention à la cybersécurité dans le développement des produits rendent plus difficiles leur découverte pour les attaquants. Allant dans le même sens, le nombre de vulnérabilités découvertes sur les systèmes de contrôle industriels est en baisse en 2016, comparé à 2015.

Vulnérabilités « 0-day »

Une vulnérabilité 0-day est une faiblesse dans un logiciel ou un système d'exploitation pour lequel aucun correctif de sécurité n'a été développé et qui n'était pas connue de la communauté avant sa publication. Elles sont particulièrement précieuses pour les attaquants ou les cybercriminels, puisqu'elles permettent d'atteindre un système d'information donné à tous les coups. Certaines peuvent être révélées, mais la plupart du temps, elles sont gardées confidentielles.

Elles peuvent être vendues par un chercheur en sécurité à l'entreprise qui commercialise le produit concerné (y compris via des programmes de bug bounties), à des intermédiaires faisant parfois monter les enchères (brokers) ou à un développeur cybercriminel de plates-formes d'exploit. Les prix varient de quelques milliers à plus d'un million d'euros.

(45) *https ://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf*
(46) *https ://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf*

2.2.1.2 Ingénierie sociale

Dans le contexte de la sécurité de l'information, l'ingénierie sociale fait référence à des pratiques de manipulation psychologique à des fins d'escroquerie. Ces pratiques exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles pour permettre, par une mise en confiance, d'obtenir quelque chose de la personne ciblée (un bien, un service, un virement bancaire, un accès physique ou à un système informatique, la divulgation d'informations…). C'est une des techniques déployées par les auteurs d'escroquerie aux faux ordres de virement internationaux (cf. 2.2.3.2).

Typosquatting

Le *typosquatting* est une technique consistant à acheter des noms de domaine qui ressemblent étrangement à des noms de site connus, mais avec des fautes volontaires, comme des erreurs orthographiques. Quatre principaux types de typosquattage d'une URL sont identifiés : utilisation d'un même terme mais écrit différemment, d'une faute orthographique ou une homonymie, d'un autre domaine de premier niveau (*top-level domain ou TLD*) comme .org au lieu de .com ou encore en utilisant les fautes de frappe de l'internaute.

Ces achats peuvent être considérés comme des actes préparatoires à des attaques de type spear-phishing (campagne de faux emails ciblés), le *typosquatting* permettant de mettre en confiance les destinataires et ainsi de les tromper.

Ainsi début 2018, une campagne de phishing particulièrement évoluée, promettant des billets de vol gratuits, a pu sévir en employant une technique de l'homoglyphie de nom de domaine, difficile à déceler car la lettre « a » est remplacée par le caractère « a » avec rond souscrit. L'URL utilisée renvoie, comme toujours, sur un site de phishing contrôlé par les pirates, demandant aux victimes de rentrer leurs coordonnées bancaires pour valider cette opération. Ce type d'attaque est possible, car il est, en effet, possible d'enregistrer des noms de domaines avec des caractères d'alphabets non latins.

Figure 2 : *Typosquatting se concrétisant sous la forme d'un point relativement discret immédiatement en dessous de la lettre a de france*

Risque d'atteinte à la sûreté informatique de l'État par typosquatting.

Sur signalement conjoint de l'ANSSI et d'un ministère, la gendarmerie (C3N) a ouvert le 13 octobre 2016 des enquêtes judiciaires relatives à trois noms de domaines Internet de nature à prêter confusion avec des noms de domaine Internet institutionnels français. Ces noms de domaines, qui n'avaient été réservés par aucune entité gouvernementale à titre préventif, ont pu être achetés librement par des tiers auprès de registraires (sociétés spécialisées dans la vente de noms de domaines). Ils auraient ainsi pu être utilisés pour envoyer des faux emails à des autorités ou agents de l'État. Toutes les mesures de sûreté ont été prises par l'ANSSI et le ministère concerné pour prévenir la réalisation de telles attaques.

2.2.1.3 Les logiciels malveillants

Quatre catégories de logiciels malveillants (ou virus informatiques) nécessitent une attention particulière :

- Les **RAT** (remote administration trojan) ou Troyen d'administration à distance ;
- Les **rançongiciels** (le virus bloque l'accès au système ou aux données et réclame le paiement d'une rançon) ;
- Les **botnets de distribution de menaces** (diffusion ou installation d'autres virus) ;
- Les **botnets ciblant les systèmes bancaires et de paiement** (ils visent l'utilisation de la banque en ligne, mais aussi les terminaux de point de vente ou encore les distributeurs de billets de banque).

RAT (remote administration trojan) ou Troyen d'administration à distance

Le RAT est une forme de logiciel malveillant contenant un ensemble de modules permettant de parcourir les données sur le système de la victime ou encore d'y intercepter des frappes au clavier ou ce qui s'affiche à l'écran. C'est l'outil de prédilection des opérations d'attaque en profondeur. Ils sont aussi utilisés pour collecter les données personnelles des particuliers.

Ils sont le support d'évolutions techniques pour permettre l'exfiltration des données depuis les réseaux sécurisés des entreprises, par exemple via le protocole DNS de résolution des noms de domaine.

Rançongiciels

Wannacry, Locky, TeslaCrypt…. L'Europe, et en particulier la France, est frappée de plein fouet par cette vague de rançongiciels (ransomware). Ce phénomène délictuel touche, outre des particuliers, tous les secteurs d'activités (industrie, monde bancaire, milieu hospitalier, professions libérales, universités, etc.) et peut impacter significativement le bon fonctionnement des entreprises. A l'origine produits conçus exclusivement par des groupes criminels organisés, générant des millions d'euros de bénéfices illicites,

les rançongiciels deviennent une technologie plus facilement accessible à la petite délinquance. Ils pourraient même, à l'avenir, être utilisés à des fins de revendications militantes ou politiques.

Un rançongiciel est un programme malveillant (virus) qui provoque soit le blocage de la machine, soit le chiffrement de tous les fichiers d'un ordinateur (cryptlocker) voire des fichiers distants, rendant ces derniers illisibles. Le déblocage (ou l'obtention de la clé de déchiffrement) ne peut survenir qu'après paiement d'une rançon. L'infection est généralement provoquée par la réception d'un courrier électronique provenant d'une source anodine apparemment légitime, la propagation pouvant également être opérée via les partages réseau sur les intranets d'entreprise.

A défaut de disposer de sauvegardes récentes, les victimes n'ont d'autre choix que de se résigner à la perte définitive de leurs données (et aux pertes d'exploitation consécutives), ou à accepter le paiement de la rançon en monnaie électronique Bitcoin (BTC). Les rançons exigées pour récupérer les données chiffrées ne sont généralement pas d'un montant excessif (entre 500 et 5.000 euros, en équivalent BTC), sous peine de fragiliser le modèle économique du délit : le coût de la rançon ne doit pas être supérieur à celui de l'arrêt d'activité de l'entreprise. L'efficacité du modèle est fondée sur le volume des victimes, dont une part significative arbitre en faveur du paiement de la rançon. Depuis 2016, le ransomware Locky a ainsi généré plus de 15 millions d'euros de chiffre d'affaires.

Le paiement de la rançon encourage la poursuite de cette activité délictuelle et ne garantit en rien le déchiffrement des données. Il peut, en outre, compromettre le système si le téléchargement de la clef s'accompagne de l'installation d'un RAT (logiciel de prise de contrôle à distance d'un ordinateur).

Des escrocs se font parfois passer pour des entreprises spécialisées dans la sécurité informatique. Ceux-ci proposent, moyennant finances, de déchiffrer les données « sans payer la rançon ». En réalité, ils la payent discrètement, en prenant une marge, et acquièrent ainsi la confiance de la victime, en vue de procéder à d'autres méfaits ultérieurs.

- ***Évolution du phénomène***

À l'origine apanage exclusif de groupes criminels organisés, s'appuyant sur de fortes compétences en informatique, les rançongiciels commencent à devenir accessibles à la petite délinquance. On trouve ainsi désormais en vente, pour quelques centaines d'euros, sur des forums spécialisés de piratage et sur le Darkweb, des rançongiciels « clé en main prêts à l'emploi ».

Au-delà de leur usage actuel crapuleux, on pourrait imaginer, à terme, que les rançongiciels soient utilisés à des fins de revendication politique ou militante, sans contrepartie financière.

Quels que soient les auteurs et motivations, les statistiques de plaintes enregistrées par les force de sécurité montrent une explosion du phénomène. Bien que le phénomène prenne de l'ampleur avec une multiplication du nombre et des variantes de rançongiciels, il a été observé, sur les dernières crises virales, une diminution du nombre de plaintes, les entreprises touchées ayant axé leur réaction sur la remise en état rapide de leurs infrastructures, au détriment de la plainte auprès des forces de l'ordre.

- ***Deux crises virales***

Le 12 mai 2017, une crise virale d'ampleur mondiale a impacté des milliers d'entreprises. Le **rançongiciel Wannacry** infecte plusieurs centaines de milliers de machines de façon quasi-simultanée dans le monde entier. Les ordinateurs touchés subissent un chiffrement de l'intégralité de leurs fichiers. Le virus se propage notamment par le biais des partages-réseau sur les intranets des entreprises ; il utilise des vulnérabilités qui ont été révélées par les divulgations du groupe de hackers « Shadow Brokers ». À défaut de disposer de sauvegardes intègres récentes, les victimes n'ont d'autre choix que de se résoudre à la perte définitive de leurs fichiers, ou à payer la rançon exigée en monnaie électronique Bitcoin (environ 300 euros).

En France, il induit la fermeture de sites de production de la société Renault. Plusieurs hôpitaux britanniques sont sévèrement impactés, ce qui incite les autorités d'outre-Manche à affirmer dans un premier temps qu'il s'agit d'une attaque étatique ciblée. En réalité, l'attaque est indiscriminée.

Les services de police et de gendarmerie ont été saisis de plusieurs centaines de plaintes, toutefois relativement peu nombreuses au regard de l'ampleur des victimes putatives. La division de l'anticipation et de l'analyse (D2A) de la SDLC a procédé aux analyses de la souche découverte sur les serveurs victimes. Ces analyses ont permis de recouper et valider certaines informations, notamment de supprimer un portefeuille Bitcoin indûment diffusé sans vérification. Des actions de prévention ont aussi été menées à l'endroit de partenaires privés et du grand public.

Les investigations sont conduites dans le cadre de la coopération internationale et en coordination avec l'OCLCTIC. Europol a ainsi déjà ouvert un réseau d'échanges dédié à ce dossier et recensé 700 entreprises françaises potentiellement infectées.

Le 27 juin, la crise **NotPetya** a touché en premier lieu l'Ukraine, où le logiciel de déclaration fiscale MeDoc a été infecté pour distribuer la charge active. Celle-ci chiffrait les fichiers des machines infectées et surtout les rendait inopérantes par la suppression des systèmes de lancement du PC. Au redémarrage, l'ordinateur était inutilisable ; **il ne s'agissait donc pas véritablement d'un rançongiciel.** NotPetya se distinguait de Wannacry par une plus forte capacité à se propager au sein des systèmes eux-mêmes, ce qui accroissait la dangerosité de ce logiciel. La société Saint-Gobain a été la cible la plus médiatisée et l'une de celles, avec l'affréteur maritime Maersk et la société pharmaceutique Merck, ayant subi le préjudice le plus important [80 millions d'euros de perte en exploitation[47]]. Les analyses techniques ont bien confirmé qu'une mise à jour malveillante d'un logiciel de comptabilité ukrainien, *MeDoc*, aurait été utilisée comme vecteur d'infection lors de la vague d'attaques.

À cette occasion aussi, la coopération internationale a joué à plein et les canaux Europol et Interpol ont été des outils de communication et des facteurs d'efficacité majeurs. Tout comme dans la précédente crise Wannacry, la division de l'anticipation et de l'analyse (D2A) de la SDLC s'est concentrée sur l'analyse de souches et la veille, permettant de fournir des analyses au plus juste et d'alerter les partenaires ainsi que le grand public dans les meilleurs délais.

(47S) Saint-Gobain : Communication du 23 février 2018 « Résultats 2017 et Perspectives »

Figure 3 : Pourcentage de machines infectées par NotPetya par pays – Source Kaspersky

Les rançongiciels ont renforcé leur caractère de menace majeure du fait de leur processus d'attaques, en chaîne exploitant les failles de sécurité dès qu'elles sont connues. Si le niveau de menace s'inscrit dans la continuité de l'année 2016, les deux attaques en mai et juin 2017 ont ainsi pris un aspect inédit par leur dimension massive et internationale, la diversité des victimes touchées (publiques et privées), l'ampleur de la propagation et les dommages causés de manière indiscriminée. Des entreprises majeures comme Renault (Wannacry) ou Saint-Gobain (Notpetya) ont ainsi été durement affectées.

Concernant le territoire français, ce sont plus de 420 procédures, toutes attaques confondues, qui ont été recensées, sans compter les nombreux faits analogues qui sont interprétés comme de simples escroqueries par les services de plaintes. Finalement, vis-à-vis de l'ampleur du phénomène, très peu de plaintes sont déposées auprès des services de police. En 2017, la gendarmerie a recueilli 218 plaintes pour des attaques présentant 28 rançongiciels différents. Au niveau de la Préfecture de Police de Paris, la BEFTI a ouvert 154 enquêtes (+54 % par rapport à 2016) et a identifié 26 rançongiciels chiffrants distincts. Les familles de rançongiciels se sont très largement diversifiées depuis 2015, avec une augmentation constatée de 752 %[48]. Dans les procédures françaises, les rançongiciels les plus présents sont Locky, Wannacry, Dharma, NotPetya ou encore BTCWare.

(48) Trend Micro, 2017, TrendLabs 2016 Security Roundup, p4

Botnets

Un botnet est le système constitué par l'ensemble des machines (ordinateurs, téléphones mobiles et autres appareils) infectées par un même logiciel malveillant ou une même famille de logiciels malveillants et qui se connecte à un **système de commande et de contrôle** donné.

Tous les logiciels malveillants utilisent aujourd'hui cette architecture en botnet qui permet de rapatrier de l'information vers les attaquants (récupérer les données confidentielles détournées) et transmettre des ordres vers les machines infectées (exécuter une action sur la machine, télécharger une mise à jour du logiciel malveillant, etc.).

Le déploiement rapide des objets connectés a attiré l'attention des cybercriminels. Le premier cas de botnet visant l'Internet des objets a été Mirai. En octobre 2016, en exploitant des failles d'équipements de vidéosurveillance, il avait neutralisé, par une attaque DDOS de 1 200 Gigabytes/seconde, le service DNS Dyn, bloquant ainsi l'accès à des sites tels que Youtube ou Twitter, ou encore l'hébergeur OVH. Mirai comportait environ 50 000 machines infectées au moment de l'attaque. Fin 2017, une nouvelle version beaucoup plus étendue pouvant concerner plusieurs centaines de milliers de machines a vu le jour. Dénommé Satori, ce botnet est toujours en activité, mais a été en partie contenu par d'importantes campagnes de remédiation.

Les attaques ciblant les systèmes bancaires et de paiement

Les virus ciblant les systèmes de paiement des points de vente se sont massivement développés au cours de l'année 2014, ciblant les pays où les pistes magnétiques sont encore utilisées, notamment les États-Unis. La France a toutefois été touchée par ce phénomène ces dernières années.

Les malwares bancaires

Ciblant les comptes en ligne, le malware bancaire Dridex, apparu pour la première fois en 2014, permet de voler les identifiants de connexion et d'injecter du contenu directement sur les sites web des banques ouverts sur des machines infectées. Depuis son démantèlement fin 2015, il était tombé en désuétude ; il avait continué de sévir sur le premier semestre 2016, avant de presque disparaître des radars. Depuis le 30 mars 2017, il est noté un regain d'activité avec une diffusion du malware selon plusieurs méthodes, représentant des millions de messages envoyés, via le spam qui arrive dans les messageries électroniques. Plusieurs grosses campagnes ont été enregistrées de mars à mai. En Australie notamment, le malware bancaire Dridex s'est propagé par une campagne de spams exploitant une faille zéro-day non corrigée de Microsoft Office. La France a été épargnée.

Le jackpotting : une nouvelle forme d'attaque des distributeurs de billets (DAB)

Le « Jackpotting » (ou « BlackBox » : utilisation d'une « boite noire ») consiste à utiliser un ordinateur portable connecté à une prise USB, soit pour accéder aux données du calculateur d'un DAB fonctionnant sous Windows, soit pour injecter un « malware », dans le but de vider totalement ou partiellement ce dernier.

Apparu en 2012 aux États-Unis, le phénomène s'est étendu. Pour l'Europe, 58 attaques ont été recensées en 2016 contre 15 en 2015. En France, les premiers faits ont été constatés en décembre 2016. Depuis, une vingtaine de compromissions de DAB ont été relevées, en région parisienne, dans l'Est, ainsi qu'en région lyonnaise pour un préjudice total de 420 000 euros [cf. §2.2.3.4].

Pour accéder au système de traitement du DAB, deux méthodes sont utilisées par les malfaiteurs, quand l'agence est fermée :

- soit l'accès au système informatique du DAB, en ouvrant la face avant ou en y perçant des trous (recours à une scie-cloche …) pour y connecter un ordinateur muni d'un logiciel adapté et déclencher le retrait de numéraires. Ce mode opératoire semble, en ce moment, être privilégié sur le territoire français par des malfaiteurs chevronnés en provenance d'Europe de l'Est, essentiellement de Roumanie, mais aussi de Moldavie et de Russie ;
- soit la prise de contrôle à distance d'une machine, voire d'un ensemble de machines connectées entre elles, permettant la distribution d'espèces ou même le transfert d'argent sur des comptes pirates. Une attaque a eu lieu récemment en Russie, où les distributeurs ont été infectés via le réseau interne d'un établissement bancaire. Cette méthode reste délicate, car elle nécessite une importante coordination des équipes afin que les « mules » soient présentes devant le bon DAB au bon moment.

La fraude Carte Bancaire « anti-POC » est toujours d›actualité.

Début 2016, sur la base d'un renseignement opérationnel, l'OCLCTIC décelait l'utilisation par une équipe de malfaiteurs, en région parisienne, d'une nouvelle technologie permettant la modification des terminaux de paiement électroniques (TPE) pour capturer les données bancaires des clients. Le travail d'enquête aboutissait à identifier le point de compromission (P) au niveau d'un conducteur de taxi complice, dont le terminal modifié en version « anti-POC »[49] ne communiquait en fait aucune transaction au réseau interbancaire, prévenant dès lors tout risque d'identification par le dispositif de détection du GIE cartes bancaires. Les investigations diligentées sur commission rogatoire permettaient de découvrir un véritable réseau structuré, qui diffusait des TPE modifiés dans des commerces complices. Les données dérobées servaient ensuite à la confection de cartes utilisées dans les Caraïbes. Le GIE évaluait le préjudice de retrait à plus 338.000 euros et à plus d'un million d'euros en tentatives infructueuses. En octobre 2017, 4 individus étaient interpellés en possession de TPE modifiés, de matériel servant à la duplication de cartes bancaires et d'un lot de cartes bancaires prêtes à l'encodage. Ils étaient tous écroués.

(49) Anti points de compromission : le dispositif n'interroge pas la base centrale du GIE carte bancaire permettant de déterminer les dispositifs de paiement compromis.

Cybercrime as a service

Au-delà des groupes de hackers confirmés en mesure de générer des attaques de grande ampleur, les attaques cyber restent accessibles à un large panel d'utilisateurs peu expérimentés, qui peuvent notamment accéder, sur le darknet ou sur l'Internet ouvert, à des « ransomwares » prêts à l'emploi ou à « construire soi-même » et autres exploits. A côté de ces malfaiteurs peu qualifiés qui louent ou achètent des services, nivelant par le bas le niveau de technicité requise, la professionnalisation du cybercrime induit tout un écosystème facilitant la mise en œuvre d'attaques cyber par des groupes criminels ; c'est ce qu'Europol a appelé « **crime-as-a-service** » dans son rapport sur l'état de la menace iOCTA 2014.

Ce principe du « crime-as-a-service » complexifie les investigations des services judiciaires. Plusieurs affaires ont toutefois abouti à l'identification et à l'interpellation d'individus impliqués dans la confection et le trafic en ligne de logiciels de piratage (RAT, crypteurs de malware, exploits kits,...), grâce, notamment, à une coopération internationale efficace.

Les forums d'échanges utilisés par les cybercriminels demeurent des objectifs préférentiels et sont sources de précieuses informations pour les services d'investigation. A ce titre, 2017 a vu, au niveau international, la fermeture spectaculaire de plusieurs sites emblématiques du darknet alimentant des trafics de toute nature (Hansa market, Alphabay, ou encore Dreammarket, dont l'un des administrateurs était un Français qui a été arrêté aux États-Unis). L'OCLCTIC cible tout particulièrement les forums et sites de trafic d'outils de hacking (dossiers Xhash, Gara, Armlet et Vavillon).

En 2017, une tendance émergente a été observée dans le paysage cybercriminel : la mise à disposition de plateformes de location de rançongiciel. Connue sous le nom de « *Ransomware as a Service* » ou « *RaaS* », cette pratique s'est développée rapidement. Depuis le début de l'année 2018, cette tendance est toutefois bousculée par un nouveau phénomène : la gratuité et la collaboration autour de ces outils. Le modèle économique proposé n'est plus de louer le rançongiciel, mais de le paramétrer et de le télécharger gratuitement. L'infection se fait toujours par l'utilisateur, mais cette fois, les bénéfices engrangés sous forme de rançons sont versés sur les portefeuilles des créateurs du maliciels. Le partage des gains est généralement annoncé comme étant 70 % pour l'utilisateur délinquant et 30 % pour les développeurs.

2.2.2 Les attaques visant les systèmes d'information

2.2.2.1 Attaques ciblées et attaques en profondeur (APT) / autres attaques

Les attaques persistantes avancées (advanced persistant threat ou APT) constituent une menace tout aussi importante que les attaques massives comme les rançongiciels.

Elles s'en distinguent cependant, dans la mesure où elles sont furtives pour pouvoir demeurer dans le système d'information de la victime le plus longtemps possible. Elles font l'objet de modes opératoires nécessitant des compétences diverses, et constitués de plusieurs phases distinctes (reconnaissance, compromission initiale, latéralisation et renforcement des accès, exfiltration des données, dissimulation, etc.), qui traduisent leur mise en œuvre par un groupe d'attaquants organisé et doté, parfois, d'outils d'attaque qu'il a lui-même développés.

L'objectif premier est, très régulièrement, d'exfiltrer les données, en vue, in fine, de les exploiter en propre, les revendre ou déstabiliser leur propriétaire initial.

Ces dix dernières années ont été régulièrement marquées par des exfiltrations de données massives. L'année 2017 l'a été, non par l'ampleur des données exfiltrées, mais par la nature d'une de ses victimes emblématiques. En effet, en septembre 2017 le plus important cabinet d'audit et de conseil Deloitte Touche Tohmatsu Limited, a déclaré avoir subi une cyberattaque visant sa plateforme externalisée de courriers électroniques. Les attaquants se seraient maintenus dans les systèmes du cabinet pendant plusieurs mois avant d'exfiltrer les données.

On notera également que la mise à disposition par le groupe d'attaquants Shadowbrokers d'outils numériques abaisse le niveau de compétence requis pour la réalisation de certaines APT et, par conséquent, facilite sensiblement la réalisation d'APT par de nouveaux publics.

Une spécificité de l'année 2017 est liée à l'actualité électorale et aux attaques contre les sites de partis politiques (notamment de type DDOS), qui ont généré plusieurs ouvertures d'enquêtes au sein des services spécialisés.

En 2017, la BEFTI recevait la plainte d'une école d'ingénieur, laquelle découvrait que son serveur avait été piraté et que des notes avaient été modifiées. Il apparaissait en effet que des connexions au serveur de l'école avaient été effectuées à distance, en utilisant les identifiants et codes d'accès d'une employée de l'établissement, durant l'absence de cette dernière. Quatre fichiers de notes stockés sur le serveur avaient été modifiés.

L'enquête permettait la découverte, parmi les logs de connexion au serveur, d'une adresse IP correspondant à un serveur OVH loué par un des élèves. Finalement, les investigations conduisaient à l'interpellation de six individus,. Ils ont tous été condamnés par le tribunal de Paris.

Bien que réputées en croissance, les attaques contre les serveurs DNS[50] font l'objet de très peu de plaintes auprès des services judiciaires. Une saisine en 2016 d'une affaire est toujours en cours après l'interpellation de l'auteur par la BEFTI.

(50) Le DNS (Domain Name System) est un service permettant d'établir une correspondance entre un nom de domaine et une adresse IP.

2.2.2.2 Détournement / « vol » de données

La France est particulièrement touchée par le vol des données personnelles. Dans son rapport publié en 2017, la société Symantec met en avant que la France est le deuxième pays le plus touché par ce fléau au monde puisque, selon son analyse, entre octobre 2015 et octobre 2016, pas moins de 85,3 millions d'éléments d'identité (des simples noms et prénoms à l'adresse en passant par les mots de passe) ont été volés en France. La France se situerait juste derrière les USA et devant la Russie. La négligence des internautes en matière de cybersécurité explique la majorité des piratages. Un internaute sur deux continuerait de répondre aux mails de phishing.

Le « vol » de données personnelles (notamment dans les fichiers clients) reste l'objectif des intrusions dans les systèmes de traitement automatisé de données. Les données obtenues sont réutilisées pour des opérations de phishing visant les clients identifiés, pour l'exercice d'un chantage aux dépens de l'entreprise, ou bien revendues, en particulier sur les forums spécialisés ou les darknets.

Fuite de sujet du baccalauréat 2017

Sur signalement du ministère de l'Éducation nationale le 06 juin 2017, le C3N a ouvert une enquête judiciaire pour fraudes aux examens relative à des fuites de sujets du baccalauréat 2017.

Un individu, agissant sous pseudonyme, affirmait détenir des sujets d'ECE (évaluation des compétences expérimentales), les vendait 20 euros via le système PaySafeCard et en diffusait un échantillon via une plate-forme de partage de fichiers en ligne. Les premiers éléments d'enquête recueillis démontraient que le suspect a pris d'importantes précautions techniques d'anonymat (utilisation de serveurs d'anonymisation sur internet, suppression de son compte Facebook, etc). Une requête Europol SIENA[51] a été adressée aux autorités néerlandaises. Les investigations se poursuivent.

Collecte frauduleuse d'identifiants mots de passe via un réseau Wifi hotspot

Un commerce de bouche alertait en 2017 la BEFTI de la présence d'un réseau Wifi étranger, présentant les mêmes caractéristiques que l'accès légitime qu'il proposait aux clients.

Un dispositif de surveillance permettait de localiser l'émetteur « pirate » et d'interpeller l'auteur. L'individu était trouvé en possession d'un « nano-ordinateur » équipé d'une puissante antenne Wifi et d'une batterie. Il collectait depuis plusieurs années, les identifiants et mots de passe des clients de l'établissement, afin de les réutiliser pour se connecter à leurs services en ligne et leur subtiliser des informations ou documents à caractère personnel. L'enquête se poursuit pour identifier les milliers de victimes.

(51) Secure Information Exchange Network Application : réseau d'échange d'informations sécurisées d'Europol.

2.2.2.3 Les dénis de services

L'Internet des objets (IoT)

De nombreuses attaques par déni de service distribué (DDoS) sont réalisées à partir de botnets d'objets connectés.

Mirai

En septembre 2016, un hébergeur français était victime d'une attaque en déni de service d'une ampleur inégalée à ce jour (supérieure à un térabit/seconde) ; l'enquête a été confiée à la DGSI.

Consécutivement à ces attaques, un internaute a publié le code source d'un malware « Mirai » qui exploite les vulnérabilités d'objets connectés, en a revendiqué la conception et indiqué être à l'origine des attaques contre cet hébergeur et contre Brian KREBS, journaliste américain spécialisé dans le numérique.

La collaboration entre la DGSI et le FBI a permis d'identifier et d'interpeller, aux États-Unis, les deux concepteurs/utilisateurs de « Mirai ».

Si les auteurs n'ont directement retiré aucun bénéfice personnel de cette attaque en déni de service, ils ont largement tiré profit, par la suite, de la commercialisation de l'outil MIRAI.

Dossier Anonymous

Fin janvier et en février 2016, le groupe de pirates informatiques « Anonymous » a contesté le vote de la loi sur la prolongation de l'état d'urgence, la nomination de M. Jean-Jacques URVOAS au ministère de la Justice et, plus globalement, « la politique sécuritaire » du gouvernement.

Des membres de cette mouvance ont procédé à des attaques informatiques, initiées sous la forme d'une succession de dénis de service distribué, qu'ils ont concomitamment revendiqués sur les comptes Twitter @AnonymousArmyFr, puis @DownSecFrance. Trois vagues d'attaques ont ainsi pris pour cible les sites officiels de nombreuses institutions, parmi lesquels le Parti socialiste, Pôle emploi, l'Assemblée nationale, le Sénat, les ministères de la Justice et de la Défense, l'Agence nationale de gestion des déchets radioactifs, l'Agence nationale de la sécurité des systèmes d'information et le ministère de l'Écologie et du Développement Durable (MTES aujourd'hui).

La procédure judiciaire a été confiée par le parquet de Paris à la DGSI.

Les investigations ont conduit à se rapprocher de la police fédérale belge, qui menait parallèlement une enquête pour des faits similaires. Les échanges d'informations avec les autorités belges ont permis d'identifier un Français résidant en Belgique, qui a été interpellé en avril 2016. Il a été entendu en Belgique par la DGSI en mai 2017. La poursuite des investigations, en particulier sur les supports techniques remis à la DGSI par la police fédérale belge, a permis l'identification d'autres internautes qui ont été interpellés et auditionnés.

Déni de service téléphonique

Moins répandues, les attaques en déni de service TDos (Telephonic Denial of Service)[52] saturent les plate-formes téléphoniques et paralysent l'activité de la victime pendant la durée de l'attaque. Si le procédé est techniquement connu depuis plusieurs années dans les milieux académiques et de la sécurité informatique, son utilisation dans les milieux criminels semble assez marginale à ce stade.

2.2.2.4 Les défigurations

Après avoir connu un pic en janvier 2015 après les attentats avec 140 procédures engagées, il est noté que très peu de plaintes sont déposées aujourd'hui auprès des services de police en matière de défiguration. En 2017, six procédures ont été enregistrées auprès de la BEFTI à Paris et deux auprès des services de gendarmerie. Elles ne rendent pas compte de la totalité du phénomène.

En effet, en 2017, 603 cas de défigurations ont été recensés par l'ANSSI à partir de 459 tickets d'incidents enregistrés dans une base de son centre opérationnel SSI. Ces tickets proviennent soit de signalements directs, soit de leur veille internet (zone-H.org …) nécessitant des vérifications. La catégorisation de ces tickets est la suivante :

- Administration centrale : 122 (lycées, universités, agences administratives, préfectures, hôpitaux, ministères, académies, services d'urgence) ;
- Collectivités locales : 292 (mairies, communautés de communes, associations dépendantes d'une mairie, bibliothèques, ports de plaisance, chambres de commerce, d'industrie ou d'agriculture, missions locales, réseaux de transports locaux, régions, départements, musées locaux, conseils départementaux, offices de tourisme)
- Défense : 2
- Opérateurs d'importance vitale (OIV) : 2
- Entreprises : 4
- Autres / Non catégorisés : 37 (associations d'Intérêt Public, pompiers, écoles non publiques, unions professionnelles)

Leur répartition dans le temps est la suivante (par trimestre) :

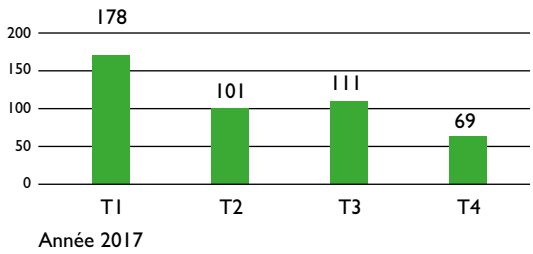


Figure 4 : Défigurations recensées en 2017 par l'ANSSI. NB : Le pic de défigurations du premier trimestre est dû à une vulnérabilité WordPress / Joomla (au moins une centaine sur cette période).

Globalement, la tendance est à la baisse.

(52) Équivalent des attaques en déni de service distribué sur les serveurs informatiques (DDoS)

2.2.2.5 Les attaques téléphoniques

En matière de fraude à la téléphonie, les malfaiteurs adoptent désormais une stratégie d'internationalisation accrue de leurs activités afin d'échapper aux poursuites et utilisent les réseaux sociaux pour amener les victimes à contacter les numéros surtaxés. Ce type de cybercriminalité pourrait encore connaître un accroissement rapide. Selon une récente étude d'Europol, le préjudice de cette fraude dans l'U.E serait passé de moins de 2 milliards d'euros en 2013 à 11 milliards en 2017.

Les phénomènes criminels en lien avec le piratage des standards et lignes téléphoniques

Détourner une ligne dans le but de monétiser des appels, bloquer un système, mettre sur écoute une cible, détruire des données, réaliser des « canulars » … les possibilités offertes par le piratage de lignes téléphoniques à distance sont multiples.

En 2017, les faits signalés à la gendarmerie ont très largement concerné deux procédés : le **phreaking**[53] et le **spoofing de ligne téléphonique.** Le premier concerne majoritairement des escroqueries aux numéros surtaxés (premium rate fraud), consistant à prendre le contrôle d'un autocommutateur[54] pour effectuer des appels vers des numéros payants gérés par l'auteur. Il peut également s'agir de l'exploitation d'une activité de taxiphone consistant à faire payer au client des communications gratuites pour l'auteur, puisqu'elles transitent en réalité par un appareil piraté. Les grands comptes, entreprises ou institutions publiques, sont généralement visés afin de noyer dans la masse les appels frauduleux passés par l'auteur et ainsi retarder la détection de l'escroquerie.

Sur Paris, la BEFTI a été saisie en 2017 de 14 plaintes visant des fraudes aux autocommutateurs téléphoniques. Le préjudice total reste important, environ 570 000 euros, mais inférieur à celui constaté en 2016 (800 000 euros). La BEFTI reste toujours fortement investie sur cette thématique et a ainsi participé ou initié des réunions avec le Médiateur des Communications Électroniques, avec le Commissariat aux Communications Électroniques de Défense (CCED) et avec l'opérateur ORANGE. La sensibilisation efficace des responsables de traitement des standards téléphoniques qui constituent des systèmes d'information à paramétrer et à sécuriser, contribue à diminuer cette menace qui perdure et génère des profits criminels élevés.

Dans le second procédé (spoofing), les victimes pensent s'adresser à leur banque, leur fournisseur d'énergie ou encore leur assurance, mais se retrouvent en réalité en conversation avec l'escroc qui a usurpé la ligne téléphonique du professionnel. Ce dernier obtient ainsi des informations confidentielles ou demande que lui soit effectués des virements pour alimenter un compte ouvert à son nom. Un opérateur de change parisien a récemment été la cible de ce type d'attaque. L'auteur incitait les clients de cet établissement à effectuer des virements vers des comptes ouverts pour les besoins de l'escroquerie en leur faisant miroiter des rendements très attractifs[55] sur des placements imaginaires.

Autre modalité, le **SIM Swapping** est un mode opératoire visant notamment à contourner les procédures d'authentification forte mises en place pour lutter contre les escroqueries aux cartes bancaires sur Internet et le piratage de comptes bancaires. Après avoir récupéré les données personnelles de la victime, parmi lesquelles les identifiants

(53) Le Phreaking est un phénomène né dans les années 1960 aux États-Unis. À l'origine destiné à passer des communications aux frais de la victime, le phreaking est désormais également utilisé pour générer des revenus délictuels.

(54) Private automatic Branch Exchange (PABX) ou Internet private Branch Exchange (IPBX).

(55) https ://lamaisondubitcoin.fr/2017/12/11/attention-escroqueries/

bancaires et le numéro de téléphone, l'auteur usurpe l'identité de la victime auprès de son opérateur mobile pour se procurer une nouvelle carte SIM. De cette manière, les appels et SMS parvenant à la victime sont réceptionnés par le cybercriminel, qui peut ensuite valider des transactions bancaires à partir du compte de la victime avec le code 3D Secure reçu sur son téléphone.

Swatting et appels malveillants

Tirant son nom des unités d'intervention d'élite de la police américaine -Special Weapons and Tactics (SWAT)-, le **swatting** est un appel visant à provoquer indûment une intervention des forces de l'ordre ou des secours. Ce type de « canular » est généralement perpétré par des adolescents ou de jeunes adultes.

L'auteur passe un appel en usurpant le numéro de la victime chez qui il souhaite provoquer indûment l'intervention des forces de l'ordre pour lui nuire. L'alerte relate une situation d'urgence inventée, mais crédible, et contient des informations personnelles précises au sujet de la victime, parmi lesquelles son adresse, sa situation familiale et une description des lieux.

Figure 5 : Infographie Swatting (G.N.)

Le 17 août 2017, une jeune femme de 26 ans, demeurant en Seine-et-Marne, a été interpellée suite à des appels « Police Secours », au cours desquels elle menaçait, avec une voix plutôt masculine, de commettre un attentat dans le RER B. L'enquête menée par la Préfecture de Police de Paris permettait d'établir qu'entre le 17 juin et le 16 août 2017, elle avait contacté 1 200 fois le « 17 Police Secours » en utilisant des cartes prépayées et une vingtaine de numéros de téléphone différents. Identifiée, elle est interpellée gare du Nord. Il s'avérait qu'elle avait déjà été condamnée en 2012 à de la prison avec sursis à la suite de nombreux appels malveillants effectués dans des commissariats de police de Seine-et- Marne entre 2011 et 2012 (plus de 6 400 appels). Pour cette nouvelle affaire, elle était condamnée à quinze mois d'emprisonnement dont dix avec sursis et trois ans de mise à l'épreuve avec mandat de dépôt à l'audience.

Techniques de dissimulation du numéro de téléphone

Masquer son numéro au destinataire d'une communication peut être légitime et n'est en rien illégal. L'utilisation d'un numéro masqué à des fins illicites est toutefois répandue.

Pour ce faire, l'attaquant accède à un **autocommutateur** en le piratant, en exploitant un défaut de sécurisation ou de paramétrage ou encore en utilisant les identifiants de connexion acquis grâce à une complicité au sein de la structure visée. Par ce biais, l'attaquant peut masquer son numéro, mais également configurer un numéro d'appel fantaisiste ou rediriger les appels vers un autre numéro dont il aura le contrôle. L'auteur peut avoir recours à une plateforme Internet dédiée à l'anonymisation ou à la falsification des numéros appelants. Dans ce scénario, les possibilités sont limitées aux services proposés par la plateforme.

Pour falsifier ou masquer son numéro d'appel, l'appelant peut également utiliser une **application mobile** depuis son smartphone et se créer autant de comptes qu'il le souhaite, et donc autant de lignes. En se connectant à Internet au travers de TOR, d'un virtual private network (VPN) ou d'un proxy, l'utilisation de ces applications devient anonyme.

Enfin, les services du type *trunk SIP* proposés par certains opérateurs Internet de télécommunications offrent la possibilité d'afficher ou non le numéro de ligne. Par l'intermédiaire de ces services, le client peut aussi faire afficher sur l'appareil de l'appelé un autre numéro de téléphone, qu'il soit existant ou totalement imaginaire.

Perspectives criminelles et opportunités judiciaires

L'accessibilité des techniques d'usurpation dont la plupart ne demandent pas de connaissances techniques élevées devrait contribuer à la dissémination de ces modes opératoires. Le passage d'un nombre de plus en plus important de plateformes téléphoniques par Internet (IPBX, Centrex) ouvre des perspectives pour les cybercriminels, qui pourront désormais se dissimuler derrière des outils classiques d'anonymisation (VPN, TOR, Proxy).

À l'instar de ce que l'on observe en matière d'attaques en déni de service distribué (DDoS), le piratage des lignes téléphoniques est proposé sous forme de *crime as a service* sur les *Darknets*, témoignant d'une forme de structuration de cette criminalité.

La loi prévoit de lourdes peines pour les auteurs de piratage téléphonique puisqu'il est considéré comme une intrusion et un maintien dans un système de traitement automatisé des données[56]. Outre la peine encourue pour escroquerie, les pirates encourent une peine de deux ans d'emprisonnement et 60 000 euros d'amende, trois ans de prison et 100 000 euros d'amende en cas d'altération du fonctionnement de ce système et jusqu'à cinq ans et 150 000 euros d'amende lorsque le système de traitement automatisé des données est mis en œuvre par l'État. Dans le cas d'un délit de fausse alerte qui s'applique au swatting, les auteurs peuvent écoper jusqu'à 2 ans de prison et 30 000 euros d'amende[57]. Cependant, les poursuites judiciaires peuvent se heurter ou être ralenties par le caractère international de cette criminalité. Néanmoins, l'ensemble des techniques de piratage ouvre des perspectives d'investigations judiciaires y compris par le biais de la décision d'enquête européenne entrée en vigueur le 22 mai 2017. La coopération entre les forces de l'ordre et le secteur privé demeure la pierre angulaire de l'élucidation de ce type d'affaire.

(56) Article 323-1 du code pénal. L'article 323-4-1 prévoit l'extension de ces peines à 10 ans d'emprisonnement et 300.000 euros d'amende lorsque les infractions ont été commises en bande organisée et à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État.

(57) Article 322-14 du code pénal.

2.2.3 L'utilisation d'Internet à des fins criminelles

2.2.3.1 L'utilisation d'Internet à des fins terroristes

Les services et en particulier la DGSI assurent une veille permanente et une analyse régulière des contenus liés à la propagande djihadiste, essentiellement EI et Al Qaida, sur tous les média (sites internet, réseaux sociaux, chaine vidéo …) et dans plusieurs langues. En particulier, ils recherchent les informations de type incitation, les préconisations sur les modes opératoires suggérés ou les évolutions de discours.

Les investigations sont aussi menées par les services sur des sites et contenus, que ce soit à des fins de renseignement ou dans le cadre d'enquêtes judiciaires ; cela concerne des menaces de nouveaux attentats, des revendications d'attentats, ou des cas d'apologie du terrorisme.

Les contenus terroristes et apologiques

Les contenus de provocation et d'apologie au terrorisme signalés à la plate-forme PHAROS, ont connu une baisse significative pour la deuxième année consécutive : 6 300 des 153 600 signalements (4 % du total), contre 11 400 signalements en 2016 et 31 300 en 2015, représentant respectivement 7 % et 16 % du total des signalements.

A l'inverse, le nombre de demandes de retraits de contenus faisant l'apologie du terrorisme a augmenté de 1 000 %, passant de 2 774 en 2016 à 30 634 en 2017. Cette augmentation est le résultat d'un renforcement des ressources humaines de l'OCLCTIC, qui a permis une recherche plus proactive de contenus anciens sur les serveurs d'hébergement qui n'avaient jamais fait l'objet de signalements antérieurs de la part des internautes. Inversement, le nombre d'items faisant l'objet d'un déréférencement par les moteurs de recherche et d'un blocage par les fournisseurs d'accès a baissé, confirmant le ralentissement de la production de matériaux de propagande puisqu'il s'agit de contenus récents.

La cellule de PHAROS dédiée à la lutte contre les discriminations a poursuivi quant à elle son action partenariale et judiciaire (21 procédures sur des faits d'apologie ou de menace ont été adressées aux services judiciaires pour traitement).

En appui aux investigations de la sous-direction antiterroriste de la DCPJ, le point de contact 24/7 de l'OCLCTIC a adressé en 2017, aux partenaires étrangers, 31 demandes de gel de données sur le fondement de la convention de Budapest.

En coopération avec l'ECTC (*European Counter Terrorism Center*) d'Europol, l'OCLCTIC rejoint le dispositif IRMa (*Internet Referral Management Application* ou application de gestion des signalements internet) de l'IRU (*Internet Referral Unit*) d'Europol. IRMa est un outil d'automatisation du traitement des contenus à caractère terroriste. Il permet de récupérer les contenus, de gérer les demandes de retrait vers plus de 150 plateformes référencées et de mesurer les temps de réponse des opérateurs du net. Destinée à devenir une base de données européenne de contenus terroristes, IRMa recensait, au 1er novembre 2017, 40 000 contenus et affichait un taux de retrait de 85 % avec de fortes disparités entre les opérateurs.

Le 9 août 2016, à la suite de l'exploitation d'une liste de comptes sur un réseau social directement signalés par un tiers, le C3N ouvre plusieurs enquêtes judiciaires en flagrance pour apologie du terrorisme. L'étude approfondie de l'un de ces comptes permet de détecter son profil. Son auteur, bien qu'utilisant de multiples cartes SIM

prépayées et permutant fréquemment ses boîtiers téléphoniques, est identifié en la personne d'un détenu de la prison de Val-de-Reuil (27-ZPN), très défavorablement connu. Le 27 septembre 2016, cet individu et un complice présumé sont placés en garde à vue. Présenté en comparution immédiate, le principal protagoniste âgé de 42 ans est condamné à 15 mois de prison ferme pour apologie du terrorisme et provocation directe à un acte de terrorisme.

Le 26 janvier, PHAROS prenait en compte le signalement d'un internaute qui avait repéré un profil sur un réseau social postant des photos semblant correspondre à une ceinture explosive avec le message suivant « Et voilà le résultat et dans quelques heures : feux d'artifice ! ! ! ». Une procédure d'urgence était enclenchée dans le but d'identifier le titulaire de ce compte. Le réseau social communiquait rapidement aux enquêteurs les informations demandées (IP mobiles et fixes, adresses mails enregistrées…). Les investigations permettaient alors de cibler un suspect sur la région de Metz. L'identité trouvée corroborant les éléments du signalement sur le réseau social, la procédure était transmise à l'antenne PJ de Metz qui procédait à l'interpellation de l'auteur dès le lendemain. Celui-ci reconnaissait les faits et était écroué.

Le 17 août 2017, PHAROS détectait un signalement concernant une menace d'attentat repérée sur un profil d'un réseau social postant le message suivant : « Demain attention attentat à Lille avec une ds4 grise ». Un autre message était posté sur ce réseau social par le même profil, dans le cadre d'un dialogue entre internautes au sujet des attentats perpétrés à Barcelone. Les enquêteurs de PHAROS ouvraient une procédure en flagrance pour association de malfaiteurs en vue de commettre un attentat et envoyaient les premières réquisitions qui leur permettaient d'identifier une adresse IP et un numéro de téléphone. La procédure était alors transmise à la DIPJ Lille qui procédait le 18 août 2017 à l'interpellation de 3 individus au domicile identifié. La perquisition amenait la découverte de 4 smartphones, et d'une clé d'un véhicule DS4, signalé volé depuis le 16 août 2017 sur la commune de Lille (59).

Jeux vidéos et apologie du terrorisme

Les forums de jeux vidéos en ligne subissent le déversement de propos apologiques véhiculés par une population majoritairement jeune (12-25 ans), provocatrice et dont l'isolement social favorise l'adhésion à des thèses extrémistes.

Les vecteurs de l'apologie

La présence de profils apologiques sur les plateformes de jeux en ligne se manifeste par une forte activité sur les forums ainsi que par la diffusion de propos apologiques au cours de parties où plusieurs joueurs conversent en direct. Les auteurs formaient une équipe virtuelle sur le jeu en ligne « *Call of duty black ops II* ». En 2016, on recensait en zone gendarmerie une dizaine d'actes d'apologie du terrorisme au moyen d'un jeu en ligne.

Si les faits sont souvent directement signalés à l'éditeur du jeu, ils ne font que rarement l'objet de signalement auprès des services de police.

Consultation habituelle de sites provoquant au terrorisme ou en faisant l'apologie

Suite à la déclaration d'inconstitutionnalité de l'article 421-2-5-2 du code pénal tel que créé par la loi n° 2016-731 du 3 juin 2016, le législateur français, par la loi n° 2017-258 du 28 février 2017 relative à la sécurité publique, a réintroduit, en l'adaptant, l'infraction de consultation habituelle de sites provoquant directement à la commission d'actes de terrorisme ou en faisant l'apologie

Dans sa **décision du 10 février 2017** (n° 2016-611, QPC), le **conseil constitutionnel** avait en effet considéré que le nouvel article 421-2-5-2 du code pénal était inconstitutionnel au motif qu'il portait une atteinte à l'exercice de la liberté de communication de l'article 11 de la déclaration des droits de l'homme et du citoyen qui n'est pas nécessaire, adaptée et proportionnée. Il considérait notamment que les dispositions contestées n'imposaient pas que *« l'auteur de la consultation habituelle des services de communication au public en ligne concernés ait la volonté de commettre des actes terroristes ni même la preuve que cette consultation s'accompagne d'une manifestation de l'adhésion à l'idéologie exprimée sur ces services »* et que l'exclusion du champ de l'infraction de la consultation de bonne foi de ces services faisait peser, par son imprécision, une incertitude sur la licéité de la consultation de certains services de communication au public en ligne dans le cadre de recherches d'informations.

Aussi, l'article 421-2-5-2 du code pénal, tel que résultant de la loi du 28 février 2017 relative à la sécurité publique, précisait que la consultation n'est punissable que lorsqu'elle *« s›accompagne d›une manifestation de ›adhésion à ›idéologie exprimée sur ce service »* et lorsqu'elle est faite sans motif légitime (notion qui remplaçait le référence à la bonne foi) tout en dressant une liste non exhaustive de ce qui constitue un tel motif. La répression, quant à elle, restait inchangée.

Saisi de cette nouvelle rédaction, **le conseil constitutionnel l'a également déclarée inconstitutionnelle par décision du 15 décembre 2017** (n° 2017-682 QPC) pour le même motif, à savoir qu'elle porte une atteinte à l'exercice de la liberté de communication qui n'est pas nécessaire, adaptée et proportionnée.

Au regard du principe de nécessité de la peine, le conseil constitutionnel souligne, comme il l'avait fait dans sa décision du 10 février 2017, l'existence de nombreuses incriminations pour lesquelles les magistrats et enquêteurs disposent de prérogatives d'enquête étendues et le renforcement des pouvoirs de police administrative, notamment par la loi n° 1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, en vue de prévenir la commission d'actes de terrorisme.

S'agissant de la proportionnalité de l'atteinte, le conseil constitutionnel, alors qu'il semblait avoir dégagé un critère alternatif dans sa décision du 10 février 2017, considère que l'ajout, au titre des éléments constitutifs de l'infraction, de la manifestation de l'adhésion à l'idéologie exprimée est insuffisant pour établir la volonté de commettre des actes terroristes. Il a également conclu que *« la portée de l'exemption tenant au motif légitime de la consultation ne peut être déterminée en l'espèce, faute notamment qu'une personne adhérant à l'idéologie véhiculée par ces sites paraisse susceptible de relever de l'un des exemples de motifs légitimes énoncés par le législateur »*.

Cette déclaration d'inconstitutionnalité a pris effet immédiatement.

2.2.3.2 Les escroqueries

Dans le domaine des escroqueries en ligne, les modes opératoires n'ont pas connu d'innovations majeures. Les cybercriminels ont toutefois de plus en plus recours aux outils d'anonymisation (VPN, Proxy, réseau Tor, téléphones équipés d'application de cryptage, applications de type Whatsapp, utilisation de numéros virtuels de type ON/OFF…). On peut noter que l'année 2017 a eu comme spécificité un net recul des faits de faux ordres de virement en France et la recrudescence d'autres types d'escroquerie comme celles par exemple, de sites frauduleux proposant des placements indexés sur le cours du diamant.

Les institutions publiques font également l'objet de fraudes récurrentes : certaines Caisses d'allocations familiales ont, par exemple, été ciblées par des séries de tentatives d'intrusions préparées par des opérations de social engineering, l'objectif final étant la création de faux dossiers permettant de générer le versement de prestations. Pôle emploi, dont la mission repose sur une large diffusion des profils de demandes et d'offres, a de son côté entrepris de lutter contre l'augmentation des offres frauduleuses en ligne, souvent d'origine internationale (de nombreux cas recensés en provenance du Bénin).

L'escroquerie aux faux ordres de virement internationaux (FOVI)

L'escroquerie aux FOVI consiste à tromper intentionnellement une personne, physique ou morale, en recourant à des moyens frauduleux (notamment l'usage d'un faux nom ou d'une fausse qualité, une mise en scène destinée à corroborer le mensonge…), pour obtenir la remise volontaire de fonds par virement bancaire. Ce phénomène criminel se situe au sommet de la délinquance astucieuse. Les auteurs conçoivent une multitude de stratagèmes pour réaliser leur projet criminel en toute sécurité : recueil de renseignements par ingénierie sociale, sollicitation du système bancaire international, constitution de sociétés fictives étrangères, recours aux différents vecteurs de cybercriminalité (moteurs de recherches, adresses de messagerie, société de-fax, ligne VOIP permettant d'appeler une ligne fixe à partir d'un ordinateur connecté et même intrusion dans les systèmes d'information d'une entreprise…).

Les faits de faux ordres de virement sont en net recul en France tant au niveau du nombre qu'en termes de montants, comme le montre les histogrammes ci-dessous.

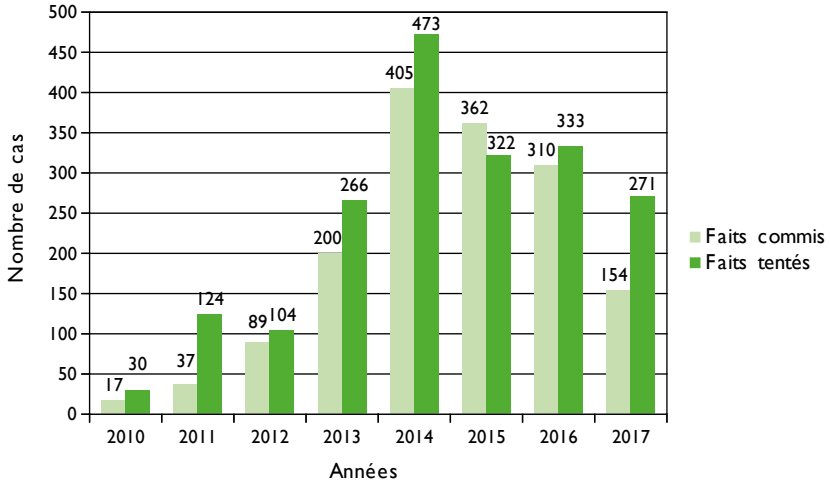


Figure 6 : FOVI – Nombre de faits, source OCRGDF

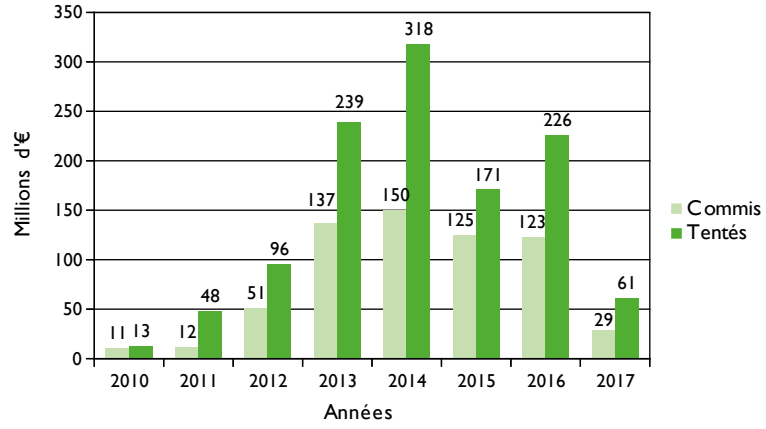


Figure 7 : FOVI – Montants en jeu, source OCRGDF

L'office central pour la répression de la grande délinquance financière (OCRGDF) de la direction centrale de la police judiciaire (DCPJ) a recensé depuis le début du phénomène en 2010 près de 2 300 sociétés et entités administratives victimes ; le préjudice est estimé à près de 639 millions d'euros pour les faits commis et 1,2 milliard d'euros pour les tentatives.

Une série de démarches ont permis d'inverser la courbe du préjudice subi par les sociétés, administrations et quelques particuliers fortunés. D'une part, la prévention mise en place par la DCPJ depuis 2013, via des partenariats, a porté ses fruits ; on peut citer

notamment la coopération avec le Mouvement des entreprises de France (MEDEF), le Club des directeurs de la sécurité et de la sûreté des entreprises (CDSE), et la Fédération bancaire française (FBF)[58]. D'autre part, les enquêtes diligentées en France, en Europe et en Israël notamment, ont contribué au recul du phénomène des FOVI[59].

Cette diminution significative est cependant nuancée par l'apparition de nouvelles tendances :

– les fraudes liées à l'investissement dans le diamant, développées par des groupes criminels organisés franco-israéliens. Concrètement, des sites frauduleux proposent des placements indexés sur le cours du diamant, présenté comme un investissement "sûr", "toujours rentable", "une valeur refuge", "à capital garanti", promettant un placement sérieux. L'année 2017 a vu une recrudescence de ces fraudes qui génèrent un nombre conséquent de victimes pour des montants importants. Les services de gendarmerie ont recensé près de 450 fraudes de ce type en 2017. Le préjudice reste cependant difficile à évaluer car de nombreuses victimes pensent avoir effectué un placement sûr et rentable, et de fait, ne déposent pas plainte. Toutefois, les dossiers en cours, principalement traités par l'OCRGDF, font apparaître des flux financiers dépassant plusieurs dizaines de millions d'euros.

La prévention apparaît encore comme le meilleur rempart face à ce type d'escroqueries opérées depuis l'étranger. L'Autorité des Marchés Financiers (AMF) a édicté de nouvelles règles plus restrictives applicables notamment aux sociétés d'investissement dans le diamant et réalise d'importantes campagnes d'information et de sensibilisation du public, en publiant notamment une liste noire des sites proposant ce type d'investissement.

– L'escroquerie aux faux investissements (FOREX - *foreign exchange*) constitue une autre tendance.

Par un démarchage téléphonique intensif ou publicité sur le web, les particuliers sont invités à s'inscrire sur des services en ligne fictifs ou à appeler des call-centers et à procéder eux-mêmes à du « trading ». Ils ont alors l'impression de suivre l'évolution de leurs investissements en ligne et peuvent même retirer une partie des gains supposés, mais il s'agit d'un leurre. Une fois le piège en place, l'escroc n'a plus qu'à attendre que la victime investisse tout ou partie de ses économies pour récupérer la mise. De nombreux artifices sont utilisés (bonus, compte premium, privilèges) afin d'inciter la victime à persévérer. Ce n'est qu'après plusieurs mois que le particulier s'aperçoit de la supercherie.

Le montant est aujourd'hui difficile à évaluer, mais dépasse plusieurs centaines de millions d'euros en France. Des phénomènes similaires ont été constatés en Israël, aux Etats-Unis et en Belgique notamment.

Des actions de prévention face aux escroqueries au FOREX ont été mises en place, à l'instar des campagnes d'information et de sensibilisation du public réalisées par l'Autorité des Marchés Financiers. S'agissant des sanctions, elles sont difficilement applicables à ce jour. Les sites frauduleux ne sont identifiés qu'après le dépôt de plainte des victimes et sont très souvent remplacés par de nouveaux, ce qui neutralise les effets des blocages des sites identifiés.

(58) Création de module de e-learning sur le FOVI au faux président et sur les escroqueries au changement de coordonnées bancaires.
(59) L'« initiateur de l'escroquerie aux faux ordre de virement a été extradé en France en novembre 2017.

Fin 2017, la Brigade des Fraudes aux Moyens de Paiement (BFMP) était saisie par la section F1 du Parquet de Paris d'une première affaire de Bitcoins. L'escroquerie s'apparentait en fait aux escroqueries de type FOREX. L'auteur détournait la ligne téléphonique de « la maison du bitcoin » ainsi que son site Internet, et proposait à des clients des investissements en monnaie virtuelle. Ceux-ci versaient des sommes en euros sur un compte bancaire en Hongrie dont l'escroc leur avait communiqué le RIB.

Escroquerie à la fausse amitié (Scam Romance)

À la suite de l'interpellation en septembre 2015, dans un bureau de poste d'Évry (91), d'un ressortissant béninois qui tentait de récupérer un mandat avec un passeport falsifié, les investigations diligentées par l'OCLCTIC permettaient de déceler une fraude à grande échelle. L'enquête établissait un préjudice global d'environ 450 000 euros aux dépens de 126 victimes identifiées. La fraude reposait sur de fausses annonces de vente en ligne ou d'escroqueries « à la romance » sur des sites de rencontre. Afin ne pas éveiller les soupçons, les escrocs sollicitaient des paiements sous forme de mandats au profit de personnes résidant en France qui récupéraient l'argent et le remettaient ensuite à des complices chargés de l'acheminer au Bénin. L'affaire se terminait en juin 2017, à la suite d'investigations techniques et à une analyse détaillée des encaissements, par l'interpellation de 7 individus en possession de faux documents, de mandats postaux, de sommes d'argent et de produits de luxe acquis frauduleusement. Le jugement est attendu en 2018.

Escroquerie au faux support technique …

L'escroquerie au faux support technique consiste à effrayer la victime par l'affichage intempestif de fenêtres indiquant la présence d'un virus sur l'ordinateur, afin de la pousser à contacter un prétendu support technique pour le dépannage de son matériel informatique. Le but recherché est d'extorquer de l'argent à la victime pour un dépannage fictif. Une nouvelle campagne d'escroquerie a été détectée en novembre 2017.

Autres escroqueries

En novembre 2016, la société SFR-NUMERICABLE identifiait 423 commandes frauduleuses de Box, opérées en quelques semaines, dont 255 livrées dans des points relais de l'agglomération lyonnaise. Elle constatait des similitudes troublantes dans ces commandes (patronymes, courriels de contact) qui utilisaient de faux RIB. Les box servaient à lancer des appels surtaxés et le préjudice était évalué à plus de 240 000 euros. L'OCLCTIC établissait que ces appels surtaxés étaient émis vers des sites de jeux en ligne pour générer des codes de micros paiements dont le virement était ensuite effectué sur un compte bancaire. La perquisition au domicile de l'auteur de cette escroquerie, en juin 2017, permettait de récupérer les 255 Box dont 6 branchées et en cours de fonctionnement. En janvier 2018, l'auteur était condamné à 2ans de prison dont un an ferme.

Pour la BFMP de la préfecture de Police, un nouveau type d'escroquerie, particulièrement lucratif a émergé en 2017 ; il s'agit de la **fraude à la re-facturation de crédits.** Générant

des préjudices particulièrement importants, elle s'appuie sur des opérations techniques et informatiques élaborées permettant de générer des opérations de remboursement via des cartes bancaires.

Les fonds, crédités sur les cartes bancaires prépayées françaises et étrangères, sont immédiatement retirés en distributeurs ou virés vers d'autres comptes.

Le montant des préjudices sur l'ensemble des dossiers est très inégal : de 100 € à plus de 200 000 €. A ce jour, en fonction des différents stades d'avancement des enquêtes, l'ensemble du préjudice comptabilisé atteint 3 millions d'euros.

Fin 2016, la brigade des fraudes aux moyens de paiement (BFMP) de Paris recevait la plainte d'une grande enseigne de bricolage, à la suite d'opérations de remboursements par carte bancaire non justifiées. Il apparaissait ainsi que depuis novembre 2016, la somme globale de 37 000 € avait été créditée sur une carte bancaire par le biais d'un terminal électronique de paiement non répertorié par l'enseigne.

Les investigations et un rapprochement avec le GIE Cartes Bancaires révélaient l'existence d'une seconde carte bancaire bénéficiaire de remboursements ainsi que d'autres enseignes victimes sur l'ensemble du territoire national. Le préjudice s'élève à 750 000 €.

L'enquête mettait en cause trois ressortissants sri-lankais de la même famille domiciliés sur Paris, qui étaient interpellés en mars 2017. Les perquisitions permettaient la saisie de 4 terminaux de paiement, une encodeuse, plusieurs cartes de domiciliation contrefaites et de cartes bancaires prépayées. Déférés au parquet de Bobigny (93), l'un a été incarcéré et un autre placé sous contrôle judiciaire.

2.2.3.3 Extorsion de fonds

Intrusion, extraction de données et tentative d'extorsion de fonds

En mai 2017, une société financière britannique était victime d'une extorsion de fonds par des hackers français. Après avoir décelé une intrusion dans son système informatique qui causait l'extraction des données de 1 400 comptes clients, cette société était contactée par un individu francophone prétendant être apparenté au groupe de pirates « Rex Mundi » qui revendiquait l'attaque et exigeait pour la non diffusion des données, le versement de 510 000 £ ou de 730 000 £ pour la correction de la faille de sécurité. Une enquête conjointe était ouverte entre la Metropolitan Police de Londres, saisie des faits, et l'OCLCTIC. Grâce au fichier Cyborg d'Europol/EC3, un rapprochement était réalisé avec une enquête du C3N initiée en avril 2016 pour la vente de services cybercriminels sur le darkweb. Sous la direction de la section F1 spécialisée cyber du parquet de Paris, une opération d'interpellations et de perquisitions conjointes avait lieu le 8 juin en Île-de-France, visant 4 suspects. Les enquêteurs établissaient que l'individu, auteur de la tentative d'extorsion (qui reconnaissait son implication dans la procédure de 2016), s'était procuré le code informatique permettant l'extraction frauduleuse des données sur le darknet, grâce à un intermédiaire qui assurait l'interface avec un pirate informatique localisé en Thaïlande. L'intermédiaire était identifié et interpellé à Mâcon (71) en octobre 2017. Il révélait l'identité du hacker français concepteur du code. Ce dernier a été localisé par la police thaïlandaise et interpellé en mai 2018.

2.2.3.4 La lutte contre la fraude à la carte bancaire

La lutte contre la compromission des moyens de paiement non liquides reste une priorité en termes de cybercriminalité, au regard de la constance des attaques directes sur les réseaux bancaires pour en manipuler les comptes et en détourner les fonds. Les phénomènes d'escroquerie à la carte bancaire poursuivent leur évolution avec des outils de skimming de plus en plus sophistiqués, déployés souvent par des groupes criminels d'Europe centrale ou balkanique, à l'occasion de véritables raids visant tout le continent. Les données de cartes européennes collectées sont ensuite revendues, tant sur le darknet que via des sites internet classiques. Plusieurs affaires opérées par la police judiciaire ont montré que ces données acquises frauduleusement étaient réutilisées dans des retraits bancaires opérés principalement en Amérique et en Asie du Sud-est.

L'OCLCTIC garde pour objectif la mise en œuvre de dispositifs de coordination et d'analyse également sur ces questions. Les atteintes aux DAC font par exemple l'objet d'un protocole qui doit renforcer la sensibilisation des services de proximité (police et gendarmerie), et permettre la remontée des signalements des compagnies privées. En 2017, 35 faits ont été recensés, dont 24 élucidés. L'office s'investit enfin activement dans la coopération européenne, en participant aux plans d'actions opérationnelles d'Europol liés au programme EMPACT « moyens de paiements non liquides ». Ceux-ci visent, par exemple, à développer la coopération avec les agences Aseanpol et Ameripol, ou à participer aux opérations coordonnées du Centre de Cybercriminalité Européen (EC3) sur la lutte contre les fraudes au e-commerce ou bien contre les « mules » financières.

En janvier 2017, la banque BNP PARIBAS portait plainte après avoir constaté une recrudescence de retraits frauduleux dans ses distributeurs automatiques de billets du nord de la région parisienne, opérés à l'aide de cartes dépourvues de puces. L'analyse de certaines cartes ré-encodées retenues par les DAB permettait d'établir qu'il s'agissait de cartes cadeaux d'achat de jeux vidéos. L'examen des DAB piégés laissait apparaître des traces de dispositifs de micro caméras devant filmer le clavier (trou de fixation). La vidéosurveillance des agences amenait l'OCLCTIC à repérer 3 individus qui débutaient une nouvelle série d'attaques en mars 2017. Début avril, un dispositif de surveillance sur un DAB permettait d'interpeller à Paris (4ème) deux des malfaiteurs, de nationalité roumaine, en train d'apposer leur dispositif de skimming. La fouille de leur véhicule immatriculé au Royaume-Uni permettait d'appréhender un lot de carte de jeux NINTENDO, prêtes pour l'encodage. Le préjudice global s'élevait à 20 000 euros de retraits réussis et à 80.000 euros de retraits tentés. Les individus ont été écroués.

En février 2016, un signalement de la direction régionale de la Banque postale de Rouen, amenait le SRPJ Rouen à entreprendre en commission rogatoire, des investigations sur des faits de retraits frauduleux dans des DAB en Normandie, région parisienne et à l'étranger. L'analyse des données bancaires utilisées frauduleusement permettait l'identification du point de compromission ayant servi à la collecte de ces données, aboutissant à un préjudice de 16.000 euros effectifs et de 240.000 euros en tentatives infructueuses. Grâce à la vidéosurveillance de l'agence bancaire et à l'appui d'Europol pour identifier le propriétaire d'une carte bulgare utilisée au même moment que l'opération, ce dernier était identifié comme l'un des 5 individus du groupe impliqué. L'individu était interpellé à l'aéroport de Roissy CDG en juin 2017. L'exploitation de données techniques permettait de localiser son domicile parisien où les enquêteurs

découvraient un atelier de confection de cartes bancaires frauduleuses (2 500 cartes à encoder, 36 skimmers, 260 cartes conditionnées...). Il reconnaissait avoir récupéré près de 70 000 euros depuis 2015. Il était écroué.

Opération Europol « Global Airport Action Day »

Du 16 au 20 octobre 2017, les forces de sécurité de 61 pays, 63 compagnies aériennes et 6 agences de voyages en ligne ont participé à la dixième édition des « Global Airport Action Days » qui ont eu lieu dans plus de 226 aéroports à travers le monde. Il s'agit d'une opération horizontale et multidisciplinaire visant à lutter contre les achats frauduleux en ligne de billets d'avion avec des données de carte de crédit compromises. 298 transactions suspectes ont été signalées et 195 personnes ont été arrêtées.

Pour la France, la gendarmerie des transports aériens (GTA) prend part à ces opérations. Durant ces deux journées, 146 militaires de la GTA ont été pré-alertés sur l'ensemble du territoire national. L'opération a donné lieu à 19 signalements de suspicions de fraudes, 10 personnes ont été contrôlées à l'embarquement conduisant au placement en garde à vue de deux individus et à l'audition libre de quatre personnes mises en cause. Trois enquêtes judiciaires sont poursuivies par les BGTA[60].

Jackpotting

En réponse au phénomène du « jackpotting » (cf. supra §2.2.1.3), l'OCLCTIC a développé des mesures de sensibilisation des services de proximité et de coordination opérationnelle (remontée d'information notamment), à l'occasion de trois enquêtes d'envergure régionale (concernant près de 20 faits en Alsace et en région parisienne). Plusieurs autres procédures ont été diligentées en parallèle par les DIPJ de Lyon et Marseille, le SDPJ 92 (PP) et la SR de Toulouse. Outre son rôle de coordination opérationnelle sur ce phénomène, l'OCLCTIC entretient des contacts étroits avec les partenaires du secteur bancaire dont la coopération est essentielle pour l'efficacité de toute action entreprise.

Le 13 décembre 2016, une première attaque de type Black-box était constatée sur une agence de la Caisse d'épargne à Mulhouse, pour 51 000 euros de préjudice. L'OCLCTIC était co-saisi des faits avec la DIPJ Strasbourg. Parallèlement, des faits similaires commis sur d'autres DAB d'agences Caisse d'épargne à Saint-Remy (71) et Condrieu (69) étaient rapprochés. Tous ces faits, antérieurs à ceux de Mulhouse, présentaient le même mode opératoire mais demeuraient de simples tentatives. D'autres faits étaient rapprochés par la suite : Savigny sur Orge (91) et Orléans (45) [La Banque Postale], Valence (26) [Caisse d'épargne]. En février 2017, trois ressortissants Roumains étaient interpellés en Norvège lors de la commission d'un « Jackpotting » au même mode opératoire et faisaient l'objet d'un signalement Europol. Les vérifications permettaient de les relier aux faits de décembre

Entre le 14 janvier et le 12 février 2017, une série d'attaques de type « Jackpotting » ciblaient 6 agences de la Caisse d'épargne à Paris et Montreuil pour un préjudice de plus de 335 000 euros. Les recherches effectuées par l'office sur la téléphonie, via Europol et en national, ne permettaient pas d'identifier les auteurs.

(60) BGTA : Brigade de gendarmerie des transports aériens

2.2.3.5 Les marchés criminels en ligne

Alphabay, Hansa

La mise hors ligne du site AlphaBay le 4 juillet 2017, puis quelques jours après, celle du site Hansa Market à la suite d'une opération conjointe des polices américaine et néerlandaise avec Europol, a porté un coup d'arrêt à deux des plus grands sites de revente de produits stupéfiants (cocaïne, cannabis, drogues de synthèse, héroïne, fentanyl, etc.) du darknet, moins de trois ans après la fermeture du site « *Silk Road* » par le FBI.

S'agissant de l'activité du site AlphaBay notamment, le FBI a pu établir les données suivantes, reflets de la réalité des trafics qui s'opèrent actuellement sur les darknets et de leur volume d'activité :

- Entre 600 000 et 800 000 dollars de chiffre d'affaires quotidien (tous biens confondus) ;
- 250 000 références de produits stupéfiants, soit 71 % des annonces illégales du site ;
- Plus de 40 000 vendeurs et 200 000 acheteurs, toutes nationalités confondues ;
- Une part de la vente de stupéfiants équivalente à 80 % du chiffre d'affaires ;
- 29 % du chiffre d'affaires réalisés dans les pays européens (soit 46 millions € contre 116 millions € pour le reste du monde - estimation).

Cette opération a également mis en exergue la volatilité des cryptomarchés : après la disparition d'Alphabay, le nombre d'inscrits a considérablement augmenté sur Hansa Market. Dans le cadre de coopération policière, l'OCRTIS a reçu d'Europol la liste d'une centaine d'acheteurs domiciliés en France, permettant la transmission des signalements aux services locaux compétents (opération Gravesac).

Concernant les serveurs hébergeant les cryptomarchés, il est techniquement difficile de déterminer leur localisation précise et d'en identifier les administrateurs. On peut néanmoins citer deux cryptomarchés d'origine française, « la main noire » et le « bon coin » (parodiant le site commercial bien connu). Ces sites, rédigés en français, proposent une offre plus limitée de produits en comparaison des sites étrangers.

Les différents sites rivalisent souvent de « garanties » en matière de qualité des produits, de prix et de fiabilité des services en raison de la forte concurrence entre vendeurs. Globalement, les prix semblent légèrement supérieurs à ceux constatés dans la rue, exception faite des drogues de synthèse. Pour les commandes importantes, des précautions supplémentaires peuvent être mises en place.

Les vendeurs sont très attachés à leur réputation qui leur sert de caution, tant sur les délais d'expédition, la sécurité des envois que sur la qualité du produit. Les cryptomarchés proposent tous des outils permettant l'évaluation des vendeurs : avis de consommateurs, nombre de commandes honorées, nombre de conflits commerciaux… On observe un professionnalisme similaire à celui des grands acteurs du commerce en ligne : avis de consommateurs, promotions, suivi des commandes, prix dégressif en fonction de la quantité commandée, échantillons gratuits avec certaines commandes, relance de clients réguliers…

Affaire de trafic de stupéfiants sur un Darknet.

Le 19 juillet 2016, le centre de lutte contre les criminalités numériques du service central du renseignement criminel (SCRC/C3N) repère des éléments d'identification d'un pseudonyme sur le Darknet, vendeur de stupéfiants prétendus « *in door* » et de numéros détournés de cartes bancaires. Le magasin en ligne de l'intéressé affiche un historique de 59 000 avis consommateurs, permettant d'estimer un chiffre d'affaire minimal de 800 000 €. Le 17 octobre 2017, les suspects sont interpellés chez eux ; sont saisis une Ferrari, un Porsche Cayenne et quatre autres véhicules enregistrés à leur nom, ainsi que 30 000 euros en espèces. Le principal auteur des faits a été incarcéré puis relâché en attendant l'examen de l'ensemble des pièces du dossier.

Vente de données sensibles sur le darkweb.

Dans le cadre de sa veille permanente en sources ouvertes, le C3N a découvert la mise en vente sur le darkweb d'un service francophone payant de consultation du fichier TAJ (traitement des antécédents judiciaires)[61]. La petite annonce est agrémentée de copies d'écran de la fiche TAJ d'une personnalité. Le 19 septembre 2017, l'auteur et un complice sont librement entendus et leurs équipements numériques saisis. L'auteur est un mineur défavorablement connu et déjà condamné pour une fausse alerte à la bombe sur la Tour Eiffel et obtention frauduleuse de données personnelles par faux appels téléphoniques à un commissariat de police.

2.2.3.6 Les atteintes aux mineurs

L'espace internet demeure le lieu de manifestations de comportements dangereux. La plateforme PHAROS a traité 256 cas d'urgence vitale en 2017, aidée notamment par un partenariat renforcé avec les modérateurs du site Jeux vidéo.com.

L'année 2017 a notamment été marquée, de mars à avril, par le phénomène du Blue Whale Challenge (BWC) qui a fait l'objet de nombreux signalements qui ont été traités en procédures d'urgence vitale à l'instar des autres signalements de comportements à risque (tels que le « jeu du foulard »).

L'influence des médias sociaux : Blue Whale Challenge (BWC)[62]

Origine et fonctionnement

Apparu en Russie fin 2015 sur le réseau social russe Vkontakte[63], le Blue Whale Challenge fonctionne sur le principe du parrainage. Les cinquante défis à relever sont ordonnés par des tuteurs, également en charge de valider ces défis sur la base de l'examen des vidéos et des photos qui leur sont envoyées par les participants en guise de preuve. Le niveau de dangerosité des défis s'élève après chaque étape franchie (isolement, visionnage de vidéos prônant le suicide, scarifications, ascension d'une grue…). Le cinquantième défi est le suicide en sautant du haut d'un immeuble ou par pendaison. La Russie est particulièrement touchée par le phénomène[64].

(61) *Le « Traitement d'antécédents judiciaires » est un fichier géré par les services de police et de gendarmerie.*
(62) *Le défi de la baleine bleue tire son nom d'une légende populaire selon laquelle le cétacé serait capable de se donner volontairement la mort en s'échouant sur une plage.*
(63) *« Concurrent russe » de Facebook.*
(64) *130 Russes auraient trouvé la mort suite à leur participation au BWC.*

Un impact limité sur le territoire national

Le *BWC* a fait son apparition dans les collèges et lycées français fin 2016. En mars 2017, les faits constatés ont connu une forte augmentation. Le phénomène touche des **adolescents de 11 à 15 ans,** majoritairement de sexe féminin, en détresse psychologique, faisant face à des difficultés dans leur milieu familial ou scolaire et pour lesquelles le BWC représente l'opportunité de mettre en scène leur projet de suicide. Au total, on recense plus de trente signalements sur le mois de mars contre quelques remontées isolées dans les mois précédents. Ces faits ont été notifiés par des parents, des responsables d'établissements scolaires ou des camarades inquiets. La gravité des faits est très variable, du simple intérêt manifesté par l'adolescent pour le jeu à la réalisation des premiers défis. Le cas le plus alarmant a été constaté à Saint Omer où une jeune fille de 17 ans, domiciliée au centre d'accueil pour mineurs, a été retrouvée sur le point de mettre fin à ses jours suite à sa participation au *BWC*.

Toutefois, l'explosion des signalements en mars ne s'est pas confirmée en avril. L'augmentation constatée concorde avec la couverture médiatique consacrée au *Blue Whale Challenge* en mars, susceptible d'avoir généré une réaction immédiate de l'entourage des victimes présumées. L'association e-enfance[65], spécialisée dans la protection des mineurs contre le cyber-harcèlement estime à une cinquantaine le nombre d'appels traités en lien avec le *BWC* en France métropolitaine. En 2017, on estime à une trentaine, le nombre de cas avérés de participation active au BWC sur le territoire.

Prise en compte du phénomène

Sur le plan judiciaire, 32 enquêtes préliminaires et une ouverture[66] en flagrance pour des infractions relevant des articles 223-6, 223-13 et 223-14 du code pénal (non-assistance à personne en péril, provocation au suicide et propagande de méthodes préconisées comme moyen de se donner la mort[67]) sont à signaler. Par ailleurs, la réaction face à la propagation du *BWC* s'est orchestrée autour de campagnes de sensibilisation entreprises indépendamment par les forces de l'ordre (Police[68] et Gendarmerie), les académies, des associations spécialisées : des initiatives personnelles sur les réseaux sociaux (Youtube), rencontres organisées par des unités territoriales avec les établissements scolaires visés, messages sur les comptes Facebook de groupements de gendarmerie ou de directions départementale de sécurité publique (DDSP).

Sur internet, la riposte s'organise également par le biais d'initiatives de contre-propagande. Un internaute propose de participer au *Pink Whale Challenge*. Calqué sur le modèle du BWC, les défis[69] ont pour but de promouvoir la vie plutôt que la mort. Enfin, identifié comme l'un des canaux de diffusion du BWC, Facebook supprime les contenus relatifs aux défis et envoie des messages de prévention aux participants.

(65) Créée en 2005, l'association e-enfance, reconnue d'utilité publique, et agréée par le ministère de l'Éducation nationale.
(66) La victime a été hospitalisée après s'être scarifiée « F57 » sur la hanche. Le parrain a été identifié sur le ressort territorial de l'unité.
(67) Sanctionnés respectivement de 5 ans d'emprisonnement et 75 000 euros d'amende et de 3 ans d'emprisonnement et 45 000 euros d'amende.
(68) La Police nationale a publié deux messages d'alerte sur le Blue Whale Challenge par le biais de son compte Twitter.
(69) Exemple de défis du Pink Whale Challenge : Rends un service à quelqu'un, prends soin d'un membre de ta famille, fais un compliment...

La lutte contre la pédopornographie

L'exploitation sexuelle des enfants en ligne

Le phénomène de l'exploitation sexuelle des mineurs en ligne continue de croître au travers du nombre de pédophiles, du nombre de victimes et du volume de matériel illicite disponible et échangé sur Internet.

On note une **diversification de l'origine** des images et vidéos à caractère pédopornographique qui mettent en scène des victimes de plus en plus jeunes (notamment des nourrissons) et des actes de plus en plus graves et violents, les producteurs s'attachant de plus en plus à les « anonymiser » en occultant tout élément d'identification.

Ces images et ces vidéos illicites sont issues de la production personnelle des abuseurs sexuels qui photographient ou filment leurs propres abus commis sur des mineurs, mais également de la production des victimes elles-mêmes, souvent pré-adolescentes ou adolescentes, soumises ensuite à des chantages et exposées à des diffusions sur Internet à leur insu et/ou sans leur consentement (phénomène dit de « *sextorsion* »).

Fixation, détention et diffusion d'images à caractère pornographique de mineur de 15 ans et corruption

Suite à un signalement de l'Association Française des Prestataires de l'Internet concernant des faits de téléchargement d'un fichier pédopornographique sur un site référencé, la plateforme Pharos identifiait l'adresse IP incriminé sur Paris.

La Brigade de Protection des Mineurs de la préfecture de Police était saisie. En octobre 2017, la perquisition au domicile, permettait la saisie de 26 supports de stockage. L'épouse entendue librement, qualifiait la sexualité de son couple comme libertine en précisant que son époux n'était pas attiré par les enfants. Toutefois, l'analyse du matériel saisi permettait de constater la présence de 80000 images et vidéos pédopornographiques, dont certaines impliquant des nourrissons), ainsi que des fichiers personnels mettant en scène les filles du couple, adoptant des positions sexuellement explicites, sans qu'aucun passage à l'acte ne soit révélé dans ces documents.

Le couple était mis en examen et incarcéré.

Il convient également de mentionner la pérennisation des faits d'abus sexuels d'enfants commis à distance (« ***live streaming*** »), apparus il y a quelques années et consistant pour des délinquants sexuels à acheter, pour une somme modique, des séquences vidéos d'abus sexuels commis sur des mineurs et perpétrés pour la plupart en direct par des adultes, sur ordre de l'acheteur. Ces séquences sont visualisées par l'intermédiaire de plateformes de partage de vidéos telles Skype, Yahoo Messenger, Zoom, et d'autres, et sont payées via des virements Western Union, au moyen de systèmes de paiement en ligne tel Paypal ou quelquefois en bitcoins. Initialement réalisée exclusivement aux Philippines, la production de ce type de vidéos s'étend à d'autres pays et notamment en Europe. Plusieurs enquêtes relatives à des faits de "live streaming", initiées par l'OCRVP[70], ont notamment concerné de très jeunes victimes roumaines, abusées par des membres de leur entourage proche, sur ordre et contre rémunération d'internautes européens et parfois français.

(70) OCRVP de la DCPJ : Office Central pour la Répression des Violences aux Personnes

D'autre part, **l'augmentation significative du nombre et des types de support utilisé** pour commettre ces infractions est particulièrement préoccupante. Les réseaux de pair à pair publics (E-Donkey, E-Mule, Ares, Gnutella), mais aussi privatifs (GigaTribe), restent des moyens privilégiés pour les pédophiles de consulter, d'acquérir et d'échanger du matériel illicite.

De même, certains sites de partage d'images – tel le site russe Imgsrc.ru, bien que très surveillés par leurs administrateurs, restent très fréquentés par la communauté pédophile mondiale, qui y voit un moyen de nouer des contacts avec d'autres internautes, avant d'échanger ultérieurement, de manière plus sécurisée, des clichés et/ou vidéos pédopornographiques.

Depuis plusieurs années, nombre de sites et forums pédopornographiques dédiés à l'échange et à la diffusion sont également hébergés sur les darknets et notamment sur les réseaux TOR. Le fait pour les internautes de surfer avec davantage de sécurité et de masquer l'origine de leurs connexions contribue à l'augmentation du nombre d'utilisateurs pédophiles du darknet, dont une part importante d'individus à profils élevés, producteurs et/ou abuseurs sexuels. Malgré l'action des services répressifs et l'utilisation de techniques spécifiques telle que l'enquête sous pseudonyme, qui amènent à la fermeture de ces forums après identification et interpellation de leurs administrateurs, modérateurs et utilisateurs, il est constaté que, très rapidement, d'autres sites sont recréés et que leur nombre est en augmentation constante. On relève également l'usage d'outils d'anonymisation (VPN, proxys). De même, les applications de communication mobiles (Whatsapp, Snapchat, Viber, Instagram) sont aussi un moyen pour ces délinquants d'échanger de manière sécurisée et crypté du matériel pédopornographique ou de se livrer à la corruption de mineurs. Les réseaux sociaux, les sites/forums destinés aux adolescents et les réseaux de jeux en ligne sont également un moyen pour les prédateurs sexuels d'entrer en contact avec des victimes potentielles.

Vision statistique des faits portés à la connaissance de la gendarmerie

À partir de la base des comptes rendu de police judiciaire (CRPJ) tenue par la Gendarmerie (cf. explications §2.4.1.1), une augmentation de 15 % des faits concernant l'exploitation sexuelle des enfants en ligne est constatée : 1 631 CRPJ en 2017, contre 1 420 en 2016.

Les filles sont nettement plus touchées par l'exploitation sexuelle des mineurs que les garçons avec une période critique entre 13 et 16 ans.

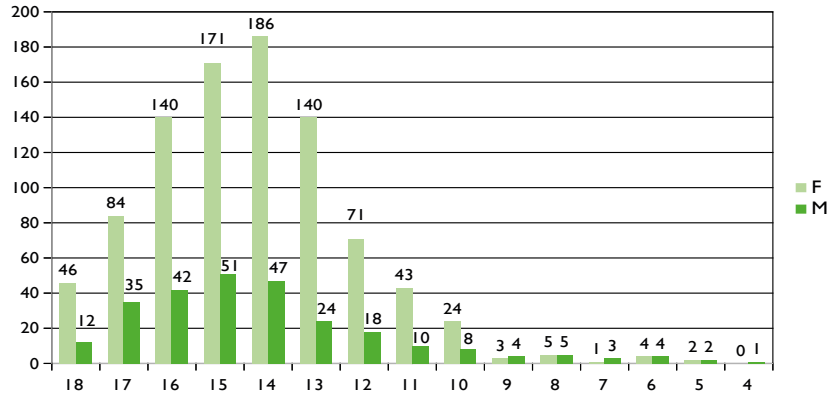


Figure 8 : Répartition des infractions par âge et sexe de la victime

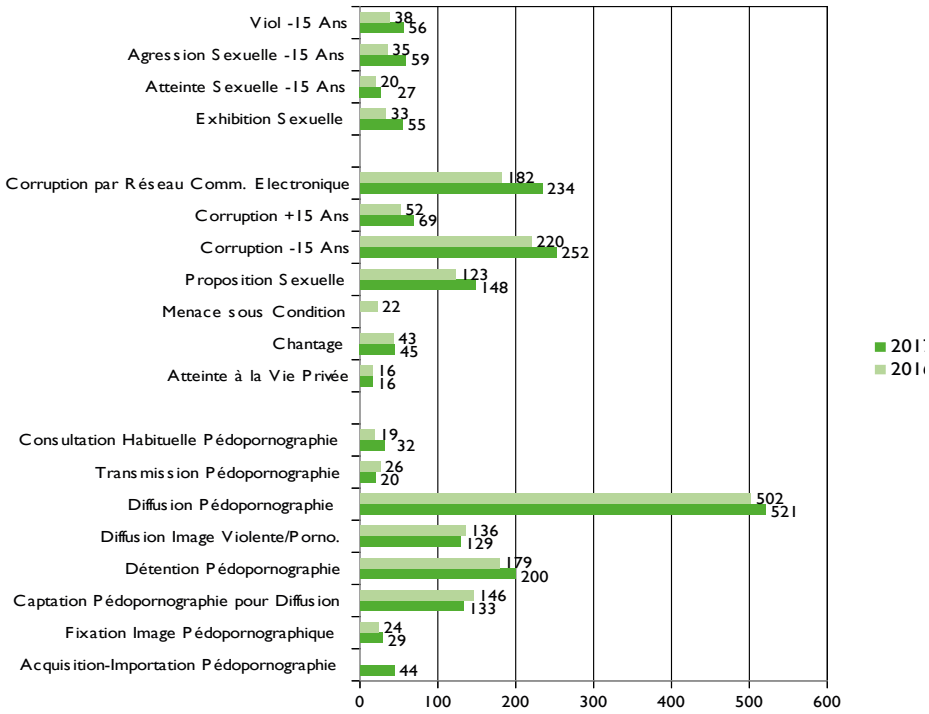


Figure 9: Répartition des infractions spécifiques à l'exploitation sexuelle des mineurs
NB : Le nombre global d'infractions est supérieur au nombre de CRPJ (nombre de fait) car un même fait peut être constitutif de plusieurs infractions

Données sur la base Caliope du CNAIP

Le Centre National d'Analyse d'Images de Pédopornographie (*CNAIP*) du PJGN administre la base nationale CALIOPE (Comparaison et Analyse Logicielle des Images d'Origine Pédopornographique). Toute donnée à caractère pédopornographique découverte au cours d'une enquête doit être transmise au CNAIP pour intégration avec les éléments suivants :

- référence d'enquête ;
- identité du mis en cause et de la victime (si identifiée et présente sur les données) ;
- listing des matériels photographiques en possession du mis en cause.

Les personnels du CNAIP disposent d'un accès direct à la base internationale ICSE (International Child Sexual Exploitation) administrée par INTERPOL. Cette base centralise toutes les données de victimes identifiées ou contenant des éléments pouvant conduire à une identification ou, a minima, à déterminer le pays d'origine. De plus, le CNAIP fournit les données à caractère pédopornographique utilisés pour les enquêtes sous pseudonymes.

Outre le fait de centraliser, d'intégrer et de catégoriser les images pédopornographiques, le CNAIP effectue un travail sur l'environnement des photos pour constituer des séries et trouver des éléments d'identification des victimes.

	Nombre total en base	Intégrées en base en 2017
Images	10 389 489	100 000
Vidéos	76 658	2 500

Figure 10 : Vision chiffrée de la Base Caliope

À titre d'illustration en 2017, dans un dossier mettant en cause un enseignant ayant procédé à des actes sexuels avec des mineurs et réalisé des montages photos et vidéos, l'analyse des images fait ressortir 20 victimes dont 8 ont pu être formellement identifiées.

Le CNAIP participe à la « Victim IDentification Task Force », une force d'intervention qui a été mise en place depuis 2014 sous l'égide de EUROPOL et INTERPOL. Regroupant 25 experts internationaux pendant deux semaines à Europol, elle procède à l'identification de victimes et d'auteurs à partir des données transmises à EUROPOL par tous les pays impliqués dans cette lutte (volume de 15 millions d'images et vidéos). Lors de la quatrième session en 2017, 10 auteurs et victimes ont été identifiés ; un auteur était localisé en France.

Une formation organisée par EUROPOL est dispensée chaque année à environ 70 stagiaires. Appelée COSEC[71], elle permet la bonne connaissance des différents outils utilisés par les agresseurs sexuels de mineurs et l'utilisation de logiciels dédiés à l'identification de ces agresseurs. Par ailleurs, les stagiaires sont formés à l'analyse des images et vidéos en vue de l'identification des victimes et des auteurs.

(71) COSEC : Combating Online Sexual Exploitation of Children

2.2.3.7 La lutte contre les contrefaçons des œuvres de l'esprit

Plusieurs actions ont été menées ces deux dernières années en matière de lutte contre les contrefaçons des œuvres de l'esprit, notamment vis-à-vis d'importants sites de téléchargement illégaux.

Zone téléchargement

Zone Téléchargement était une des principales plateformes de téléchargement direct. Le 28 novembre 2016, les autorités françaises faisaient fermer le site Zone Téléchargement au terme d'une enquête menée par la gendarmerie depuis 2014, suite à une plainte de la Société des auteurs, compositeurs et éditeurs de musique (Sacem)[72].

Torrent 441

En 2014, la Sacem porte plainte contre Torrent 411, plateforme de peer-2-peer francophone sur laquelle des millions de Français s'échangent dans l'illégalité des contenus musicaux et cinématographiques. Après 3 ans d'enquête internationale, 6 personnes sont interpellées en 2017[73].

2.2.3.8 « cyberinfluence » et atteintes à la démocratie

Les systèmes d'information liés aux élections comme cibles

Plusieurs technologies liées aux élections ont été victimes d'attaques au cours des périodes récentes.

En 2014, le système d'enrôlement des électeurs tunisiens avait subi une attaque en déni de service et le site de la Commission centrale des élections ukrainienne également au moment de l'affichage des résultats. L'année 2016 fut elle marquée par l'actualité de la campagne électorale américaine, avec la révélation d'informations issues des systèmes d'information des partis politiques, en particulier le parti démocrate en mai[74].

En France, le vendredi 5 mai 2017 à l'avant-veille du scrutin présidentiel, le site PasteBin a publié de nombreux liens vers des fichiers « torrent », soit plusieurs gigaoctets d'archives d'e-mails, provenant du mouvement « En Marche ». Ces documents ont été ensuite largement diffusés sur les réseaux sociaux, notamment des comptes twitter, et également sur des sites apparentés à l'extrême droite américaine. Les fichiers ont été obtenus quelque temps auparavant suite au piratage de boîtes mail de plusieurs responsables du mouvement. Ces fuites, dite « Macron Leaks », organisées dans un but de déstabilisation n'ont finalement pas eu l'effet escompté.

Ayant constaté ces agissements contraires aux dispositions du code électoral, la Commission nationale de contrôle de la campagne électorale a saisi le procureur de la République de Paris, en application de l'article 40 du code de procédure pénale.

Les campagnes de désinformation sont devenues un sérieux problème. En raison de leur nature, elles sont difficiles à identifier et à contrer. Elles sont souvent rendues possibles par la multiplication des agences exploitant des données collectées dans des conditions

(72) http://www.europe1.fr/faits-divers/zone-telechargement-mise-en-examen-dun-administrateur-presume-2915456
(73) https ://www.numerama.com/politique/270988-t411-lenquete-internationale-qui-a-mis-fin-a-un-des-plus-importants-reseaux-de-piraterie.html
(74) http://edition.cnn.com/2016/06/21/politics/dnc-hack-russians-guccifer-claims

sujettes à caution[75]. Les sociétés humaines devront développer une résilience contre de telles attaques, en particulier celles qui visent potentiellement à affecter les processus démocratiques tels que les élections, les procédures législatives, l'application de la loi et la justice.

Fake news

Fake news, hoax et *swatting,* ces nouvelles pratiques se développent sur Internet à partir d'un point de départ commun : la diffusion d'une rumeur, d'une fausse information dont les conséquences dépendent de la cible visée. Ces anglicismes nourrissent des débats sur le plan politique, juridique ou sociétal. Le volet sécuritaire est aussi impacté en matière d'ordre public, de sécurité économique et financière, de lutte contre le terrorisme, d'atteinte à l'intégrité physique des personnes, d'allocation des forces de police sur le terrain.

Pour les forces de l'ordre, l'identification des auteurs est un défi important compte tenu du caractère viral et anonyme d'Internet. La prévention des troubles à l'ordre public passe également par le développement d'une capacité de détection des campagnes d'information mensongères et la construction d'un contre-discours accessible au plus grand nombre.

■ Fausses informations et rumeurs : quelles incidences en matière de sécurité ?

Visant à influencer l'opinion publique en saturant le cyber espace, les fake news sont transférées et reproduites par des réseaux de petite main exécutant des tâches pour quelques centimes d'euros par clic, posant la question du travail illégal qui peut en découler[76]. Les campagnes les plus perfectionnées utilisent des **réseaux de bots** (programmes automatisés) qui créent des centaines de milliers de comptes sur les réseaux sociaux. Un ou deux messages sont envoyés à partir de chaque compte générant une campagne de désinformation massive.

La manipulation de l'opinion n'est toutefois pas l'apanage d'auteurs aux moyens démesurés. La technique de l'*astroturfing,* notamment pratiquée par les activistes, consiste à déformer l'amplitude d'un mouvement pour lui donner un plus grand retentissement. Ainsi, des pétitions reçoivent un nombre de signatures qui ne reflète pas l'adhésion à la cause défendue, bien plus limitée. En se penchant sur la liste des signataires, les identités fictives sont légion et correspondent à des faux comptes créés pour l'occasion. Des plateformes (change.org, mesopinions.com) se sont spécialisées dans la constitution de pétitions en ligne et sont parfois le vecteur de l'*astroturfing*.

À l'autre bout de la chaîne des auteurs, une poignée d'individus mal intentionnés peut occasionner des troubles à l'ordre public en diffusant des messages anxiogènes comme ce fut le cas à l'occasion des manifestations anti-gouvernementales en Guyane, en marge de la manifestation de Kourou qui avait rassemblé plus de 10 000 personnes en avril 2017. Un message Instagram annonçait le déploiement de trois escadrons de gendarmes

(75) *Cambridge Analytica, société britannique soupçonnée d'avoir collecté des données personnelles de dizaine de millions d'américains sur Facebook, dans le cadre de la campagne présidentielle de Donald Trump.*

(76) *Les sites upwork.com, fiverr.com ou encore taskrabbit.com proposent de mettre en relation travailleurs du web et employeurs. Dans ce cadre, des « cliqueurs » peuvent être recrutés pour influencer une tendance sur Internet (générer un like, un partage, la rédaction d'un fake news, l'élaboration d'un slide).*

mobiles, pour répondre au mouvement social. Dans la perspective de l'arrivée des troupes, il était recommandé à la population de « *rester chez elle le 5 avril et de faire des provisions* », entretenant un climat de défiance vis-à-vis de l'État et anticipant une action qui consisterait pour le gouvernement à organiser une réponse violente au mouvement social en cours.

La toile est également le vecteur de fausses annonces d'attentats et du relais de communiqués soi-disant rédigés par des groupes terroristes appelant à la commission d'attentats sur le territoire. Des sites et des forums se sont spécialisés dans la diffusion d'informations fantaisistes ou parodiques relayées par des internautes ou d'autres sites d'informations peu scrupuleux dans la vérification de leurs sources. Initialement diffusées dans le but de distraire, ces informations peuvent trouver un écho inattendu. Le 15 juillet dernier, un article publié sur actualités.com a relaté un attentat-suicide dans un cinéma de Rouen faisant état de 17 morts et 47 blessés. Le lien a été partagé 45 000 fois en quelques heures. Les services de police ont ouvert une enquête sur la qualification de publication de nouvelle fausse. La saturation des standards téléphoniques des unités de police et gendarmerie, associée au déploiement de ressources sur le terrain pour vérifier l'information ont diminué momentanément la capacité opérationnelle des forces de l'ordre.

La sphère économique et financière est également vulnérable. Fin 2016, des faux communiqués de presse, annonçant des erreurs dans le bilan du groupe Vinci et le licenciement du directeur financier, avaient fait dévisser le cours de l'action de 18 points en dix minutes, occasionnant une perte de plusieurs milliards d'euros, recouvrée dans les minutes qui ont suivi grâce à un démenti officiel. Les auteurs avaient dupé des agences de presse spécialisées en achetant des noms de domaines proches du nom officiel (typosquatting). La réputation des entreprises est également touchée par le truchement de dénonciations calomnieuses publiées via des réseaux sociaux et provenant généralement d'anciens employés. Une gestion dégradée de sa e-réputation peut avoir des conséquences désastreuses sur l'activité économique d'une entreprise et dans certains cas, menacer sa pérennité.

■ **Stratégies de lutte contre le risque sécuritaire : détection, dissuasion, sensibilisation.**

En parallèle de la réponse pénale, les opérateurs privés de l'Internet prennent progressivement conscience de leur rôle dans la détection et de leur capacité à fermer des canaux de diffusion de fausses nouvelles ou de rumeurs. Facebook contribue à un fond destiné à lutter contre les fausses informations et rémunère des *fact checkers*, en charge de valider des articles postés par les utilisateurs pour contrer une fausse information. La fondation Mozilla a récemment lancé un programme de lutte contre les *fake news* dont les deux principaux volets sont la sensibilisation des utilisateurs et l'amélioration de l'arsenal technologique via la création d'extensions dédiées (Firefox).

La détection ne constitue pas en elle-même une réponse suffisante dans la mesure où les potentielles conséquences sur la sécurité des personnes physiques ou morales peuvent intervenir dans un délai très court suivant la diffusion d'une fausse information. Les forces de l'ordre, en première ligne en cas de risque sécuritaire lié à la diffusion d'une fausse nouvelle, intègrent dans leur processus de gestion de crise, la réponse à une diffusion de fausse information susceptible d'impacter les divers domaines de la sécurité. L'anticipation est un volet essentiel de ce travail, consistant à communiquer sur les dangers des fausses nouvelles, leur impact et leurs conséquences en matière pénale dans le but de dissuader les auteurs. Le Service d'informations et de relations publiques des

armées – Gendarmerie (SIRPAG) et le service d'information et de communication de la police nationale (SICOP) déploient ce type de stratégie par le vecteur de leurs comptes officiels sur les réseaux sociaux[77].

La Commission européenne a organisé une réunion de travail le 30 novembre 2017 puis une consultation publique afin d'envisager les meilleurs moyens de lutter contre la propagation de fausses nouvelles au niveau de l'Union.

2.3. Perception de la menace

La mesure de la menace cyber, lorsqu'elle est réalisée par les éditeurs de solutions de sécurité peut être discutée et parfois manquer d'objectivité. En effet, ils pourraient avoir tendance à souligner de façon exagérée les risques encourus par leurs parcs de clients ou de prospects. Surtout, leur mesure peut être faussée par la répartition de leur clientèle dans les différentes régions du monde.

Le fait que les victimes d'actes de cybercriminalité déposent peu de plaintes auprès des forces de l'ordre induit l'existence d'un chiffre noir dans les statistiques ; il constitue également un obstacle pour la compréhension du niveau de la cybercriminalité et de son coût.

De nombreux angles de mesure et d'évaluation de la menace sont proposés dans les pages qui suivent.

2.3.1 Vision des cybermenaces par les services du ministère de l'Intérieur

2.3.1.1 Données statistiques sur les infractions constatées

Les fonctionnaires de police et les militaires de la gendarmerie nationale reçoivent les plaintes des victimes d'infractions cyber en application du code de procédure pénale. Ces plaintes font l'objet d'un enregistrement statistique qui permet de produire les statistiques de la délinquance, c'est-à-dire, sous leur forme actuelle, l'état 4001 des faits qualifiés de crimes et délits, état qui n'est pas adapté à la mesure de la cybercriminalité.

Cet enregistrement, traditionnellement effectué en application d'un guide de méthodologie statistique commun aux deux forces de sécurité intérieure, se modernise dans le cadre de la mise en œuvre d'un nouvel environnement informatique, notamment structuré autour de logiciels de rédaction des procédures (LRP) déployés dans la gendarmerie nationale (LRPGN) et dans la police nationale (LRPPN).

Depuis fin 2015, le service statistique ministériel de la sécurité intérieure (SSMSI) a élaboré, conjointement avec les directions et leurs services spécialisés, des agrégats regroupant les catégories d'infractions liées à la cybercriminalité. Il a été choisi de distinguer les infractions ciblant les systèmes et les infractions commises via les systèmes. Ce travail permettra de fiabiliser et de stabiliser enfin la statistique, et de s'inscrire dans le contexte de la nomenclature internationale.

Légère diminution du nombre d'atteintes aux systèmes de traitement automatisé de données (STAD) déclarées en 2017 (SSMSI).

Parmi les infractions relevant de la cyber-délinquance, les atteintes aux systèmes de traitement automatisé de données (S.T.A.D.) font l'objet d'un repérage rigoureux et permettent des statistiques fiables. Depuis 2017, les systèmes d'enregistrement du

(77) *Facebook, Twitter, Instagram.*

ministère de l'intérieur permettent de suivre l'évolution des dépôts de plaintes pour les atteintes aux S.T.A.D. en fonction de leur date de prise en compte.

Au cours de l'année 2017, la police et la gendarmerie ont enregistré 9250 infractions d'atteintes aux S.T.A.D., soit une moyenne de 771 infractions par mois. L'évolution de la série se situe en léger retrait par rapport à 2016 : -3 % en annuel.

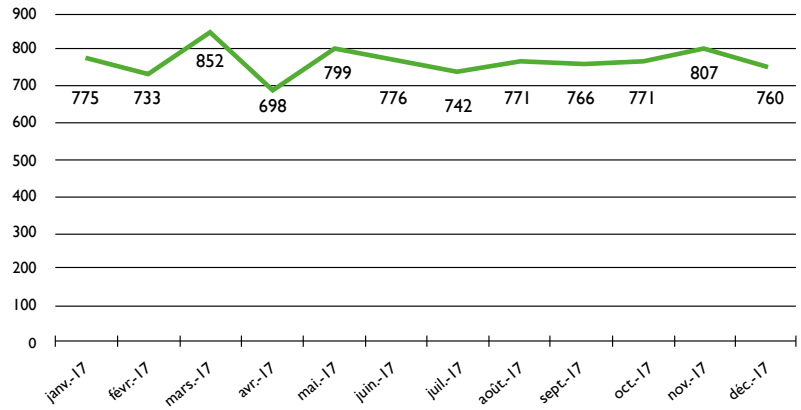


Figure 11 : Atteintes aux S.T.A.D. – Nombre d'infractions mensuelles.

Champ : France - Dates d'enregistrement des faits
Source : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie. (BI4 ORUS)
Lecture : 807 infractions d'atteintes aux S.T.A.D. ont été enregistrées par la police ou la gendarmerie en France en novembre 2017

Les principales atteintes aux S.T.A.D.

Les accès frauduleux sont stables et représentent en 2017 toujours la grande majorité (79 %) des atteintes aux S.T.A.D. Viennent ensuite les atteintes aux données (14 %) qui sont en hausse de 55 % par rapport à 2016. Les altérations et entraves au fonctionnement sont en forte baisse (-55 %) ne représentent que 6 % du contentieux des S.T.A.D. en 2017 contre 13 % en 2016. Viennent enfin les infractions de détention de moyens d'atteinte aux S.T.A.D. en forte baisse (- 46 %) : elles ne représentent que 1 % des atteintes aux S.T.A.D. en 2017.

Catégorie d'infractions	Année 2016	Part en 2016	Année 2017	Variation 2017/2016	Part en 2017
1 - Accès frauduleux	7 287	*76 %*	7 308*	< 1 %*	*79 %**
2 - Altérations ou entrave au fonctionnement	1 233	*13 %*	555*	- 55 %*	*6 %**
3 - Atteintes aux données	834	*9 %*	1 295*	55 %*	*14 %**
4 - Détention de moyens	214	*2 %*	93*	- 57 %*	*1 %**
Total général	9 568	*100 %*	9 250	- 3 %*	*100 %*

Figure 12 : Atteintes aux S.T.A.D. – Nombre et part d'infractions par catégories

Champ : France – Dates d'enregistrement des faits - Source : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie. (BI4 ORUS)

Pour en savoir plus :

INSEE-INHESJ/ONDRP-SSMSI – « Rapport de l'enquête Cadre de Vie et Sécurité », décembre 2017. https ://www.interieur.gouv.fr/Interstats/Actualites/Rapport-d-enquete-cadre-de-vie-et-securite-20172

INSEE – « Sécurité numérique et médias sociaux dans les entreprises en 2015 » Insee Première – N°1594, paru le 10/05/2016 https ://www.insee.fr/fr/statistiques/2121545

Vision statistique des infractions constatées en gendarmerie

À l'issue de chaque plainte, le gendarme établit un écrit relatant de manière synthétique le mode opératoire utilisé pour commettre l'infraction. Ce compte rendu de police judiciaire (CRPJ) rédigé à l'aide d'un logiciel de rédaction de procédure (LRPGN) remonte automatiquement en base pour analyse dès lors qu'il concerne un phénomène Cyber. La remontée est automatique dès lors que le gendarme indique que l'infraction a lieu sur internet, qu'il coche la case cyberespace ou qu'il utilise des mots clés dans la synthèse en question. Sans avoir un caractère exhaustif, cette remontée d'informations permet d'avoir une bonne visibilité du phénomène « cyber » en gendarmerie, notamment en terme qualitatif. Intégrées en base, ces manières d'opérer, peuvent ensuite être interrogées par le C3N pour effectuer des rapprochements judiciaires et de la détection de phénomène. C'est en partie sur cette source d'informations que le Service Central de Renseignement Criminel produit des fiches d'analyse de phénomènes « cyber » avec des orientations opérationnelles pour les unités et des fiches d'analyse stratégique pour sensibiliser les autorités sur des phénomènes émergents.

Augmentation de la moyenne du nombre de CRPJ par mois

Le volume de faits portés à la connaissance de la gendarmerie, soit plus de 63.500 sur l'année 2017, offre une vision globale des tendances constatées. Ce chiffre est en hausse de 32 % par rapport à 2016, ce qui illustre d'une part une augmentation de l'activité cybercriminelle et d'autre part les prémices d'une prise de conscience citoyenne de la nécessité d'accompagner le processus de remédiation d'un signalement aux forces de police en cas d'attaque avérée ou de tentative.

Année	Nombre de CRPJ Cyber	Augmentation
2016	48 089	+ 32 %
2017	63 562	

Il est constaté une augmentation du nombre de CRPJ par mois sur l'année 2017 avec une moyenne de 5297 CRPJ cyber par mois contre 4007 CRPJ par mois en 2016. La tendance est haussière avec plus de 6000 CRPJ cyber en décembre 2017.

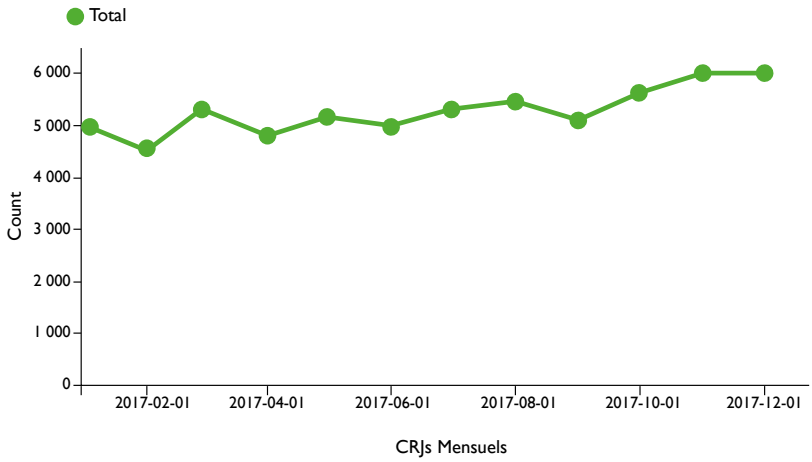


Figure 13 : Evolution du nombre de CRPJ cyber en 2017

Répartition des infractions cyber les plus représentées par NATINF

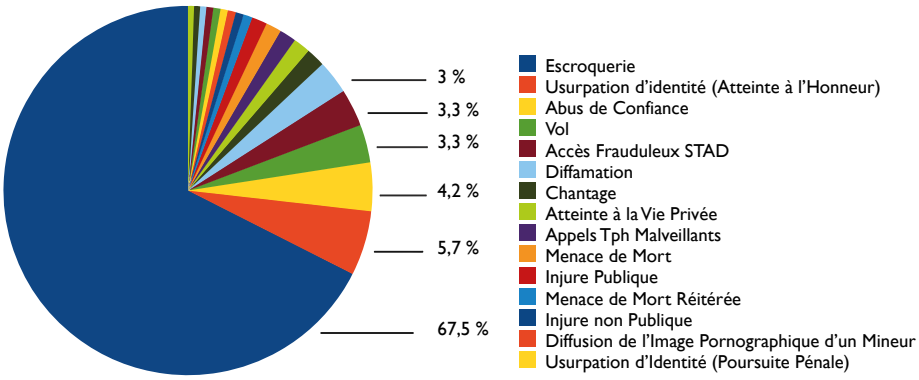


Figure 14 : Etude CRPJ – Source : GN – C3N

Focus sur les escroqueries et infractions assimilées (SSMSI)

En 2017, les services de police et de gendarmerie ont relevé 320.000 victimes d'escroqueries et infractions assimilées, chiffre en augmentation de 5,6 % en moyenne par an depuis 2012. Cette croissance, régulière sur toute la période, est principalement due à la hausse de deux catégories d'infractions : les falsifications et usages de cartes de crédit (+57 % en 5 ans) qui touchent 57 800 victimes en 2017, bien que ce nombre ait peu varié par rapport à 2016 ; et les escroqueries et abus de confiance (+34 % en 5 ans) qui concernent 218 500 victimes en 2017. Avec un taux de victimisation supérieur à 5 pour 1 000 personnes, ce sont les adultes de moins de 50 ans qui sont les plus touchés par les escroqueries. En réponse à ce contentieux, les services de police et de gendarmerie ont mis en cause 75 000 personnes en 2017.

Les auteurs d'escroqueries utilisent souvent l'Internet et des technologies d'information et de communication pour entrer en contact avec leurs victimes. Parmi les 158.000 escroqueries[78] enregistrées, au moins 66.000 escroqueries, soit 42 %, ont été commises ou facilitées par des moyens informatiques ou une connexion en ligne.

Les modes opératoires enregistrés en 2016 et 2017 par la police pour les escroqueries[79] de cyber-délinquance font ressortir en particulier une réponse à une annonce frauduleuse (22 %) et l'utilisation d'une annonce passée par la victime (11 %). Le prétexte d'une transaction est fréquent : vente (8 %), achat ou location (4 %), offre de service (2 %), et les attaques aux comptes bancaires cumulent 14 % des escroqueries : virement bancaire informatique (3 %), usage frauduleux d'un numéro de carte bancaire (4 %), collecte par ruse des données bancaires (3 %), scamming-arnaque à l'obtention de virement (2 %), usage frauduleux d'un numéro de compte bancaire (1 %) et retrait d'argent liquide (1 %). Viennent ensuite les escroqueries aux sentiments : demandes d'aide (4 %) et les escroqueries à la romance (2 %) et les liens d'amitié noués avec la victime (1 %).

Fréquence en %	Mode opératoire
22	Réponse de la victime à une annonce
11	Réponse à une annonce passée par la victime
8	Prétexté une vente
7	Prétexté la fourniture d'un emploi
4	Usage frauduleux d'un numéro de carte bancaire
4	Prétexté un achat ou une location
3	Virement bancaire informatique
4	Prétexté une demande d'aide
3	Collecté par ruse des données bancaires
3	Usage frauduleux de chèque volé
2	Prétexté une offre de service
2	Scanning arnaque obtention virement
3	Contact téléphonique avec la victime
2	Usurpation d'adresse mel
1	Hacking piratage accès non autorisé

(78) Au sens de la NATINF « 7875 » du ministère de la Justice.
(79) ?????

2	Scam escroquerie à la romance sur réseaux sociaux
1	Usage d'un moyen de communication mobile
1	Attaque d'une boîte aux lettres informatique
1	Usage frauduleux d'un numéro de compte bancaire
1	Usurpation d'identité sur réseau social
1	Amené la victime à retirer de l'argent
1	Prétexté un accord de prêt
1	Lien d'amitié noué avec la victime

Figure 15 : Fréquence des modes opératoires les plus cités comme principale manière d'opérer dans les escroqueries relevées en cyberdélinquance enregistrées par la police en 2016 et 2017. Champ : France entière – Police.
Source : SSMSI—Base des crimes et délits enregistrés par la police et la gendarmerie. France entière police Orus-LRPPN.

Par ailleurs, les débits frauduleux sur comptes bancaires ont, selon l'enquête « Cadre de vie et sécurité »[80], touché 3,4 % des ménages et causé un préjudice annuel moyen de 747 millions d'euros sur la période 2010-2015.

2.3.1.2 Activité de la plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements

La plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) de l'OCLCTIC exploite les signalements émis sur le site https ://www.internet-signalement.gouv.fr/ par des internautes et des professionnels du numérique décrivant des comportements ou contenus de l'internet qu'ils estiment illégaux.

En termes d'activité de recueil et de traitement de signalements, l'année 2017 s'inscrit dans un retour à la volumétrie de 2014, après deux années atypiques marquées par des événements terroristes majeurs et une augmentation importante des signalements liés à la discrimination. PHAROS a reçu et traité 153.586 signalements en 2017 (contre 170.721 en 2016, 188.055 en 2015, 137.456 en 2014 et 123.987 en 2013).

(80) L'enquête de victimation Cadre de vie et sécurité (CVS) est conduite chaque année, depuis 2007, par l'Institut national de la statistique et des études économiques (Insee), en partenariat étroit avec l'Observatoire national de la délinquance et de la réponse pénale (ONDRP). Le Service statistique ministériel de la sécurité intérieure (SSMSI) est associé au pilotage, à la conception et à l'exploitation de cette enquête.

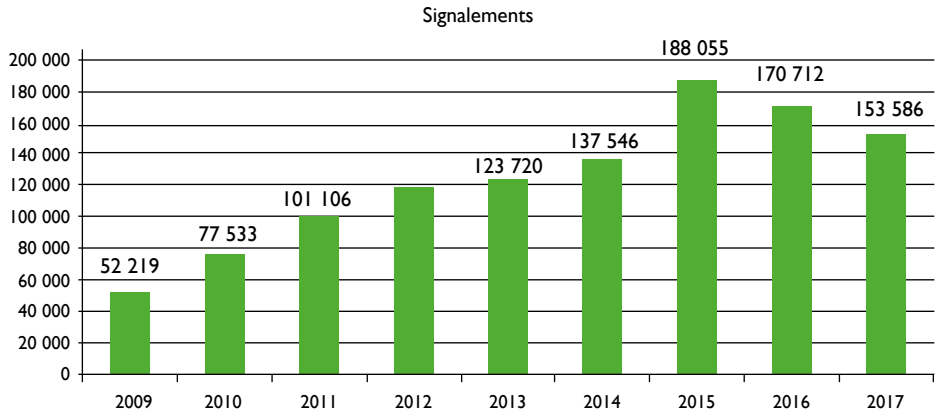


Figure 16 : Nombre de signalements à la plateforme Pharos

Ces signalements concernent majoritairement les escroqueries (51 %), les atteintes aux mineurs (13 %), les discriminations (8,6 %) et l'apologie ou provocation au terrorisme (4 %). Les signalements liés à la pédopornographie représentent 20 172 faits en 2017. 4 346 d'entre eux ont été envoyés aux partenaires étrangers via Interpol, du fait d'éléments (lieux d'hébergement ou adresse IP de l'internaute diffuseur) situés hors de France. La haine en ligne demeure axée sur la haine et la discrimination raciale, ethnique ou religieuse (54,5 % des signalements « discriminations »). Les injures et diffamations connaissent quant à elles une forte progression, représentant 35 % des discriminations totales.

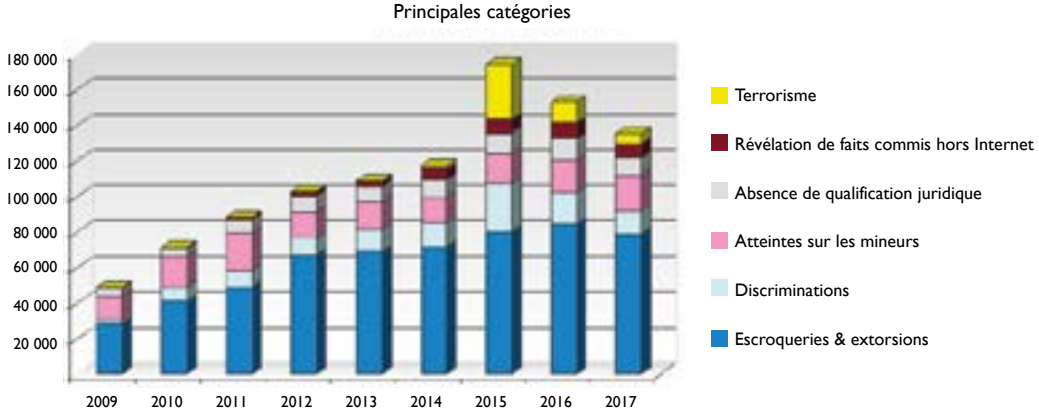


Figure 17 : Principales catégories de signalements à la plateforme Pharos

Pour ce qui concerne l'application de l'article 6-1 de la loi du 21 juin 2004 pour la confiance dans l'économie numérique, 32 017 demandes de retrait, 743 demandes de

blocage et 2 650 demandes de déréférencement ont été adressées aux professionnels de l'internet au cours de l'année. Pour les mesures de blocage, ce sont ainsi 2 860 686 connexions à des pages pédopornographiques et 21 547 connexions à de la propagande terroriste qui ont été empêchées.

L'approche partenariale développée avec les associations et le secteur privé a permis de renforcer les signalements, pour constituer désormais 3,3 % de la totalité des signalements reçus. La coopération avec l'Association Française des Prestataires de l'Internet (Point de Contact) a été renforcée conduisant au doublement du nombre de ses signalements (3.331 contre 1.478 en 2016, sur des faits d'atteintes aux mineurs essentiellement).

La plate-forme Pharos doit connaître en 2018 une évolution de son architecture informatique (virtualisation) qui devrait améliorer sa capacité de traitement des signalements.

2.3.2 Perception de la menace par les entreprises françaises

Le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) a produit en janvier 2018 une enquête intitulée « baromètre de la cyber-sécurité des entreprises ». 142 entreprises[81] membres y ont participé.

La majorité des entreprises sont touchées par des cyber-attaques : 79 % en ont constatées au moins une en 2017 (plus de 10 pour 28 %). Le nombre de cyber-attaques constatées augmente encore pour près d'une entreprise sur deux, par rapport à 2016.

Le rançongiciel est cette année encore la **cyber-attaque la plus fréquente** (73 %), loin devant les attaques virales génériques (30 %) et la fraude externe ou les « vols » d'information (30 %). Dans le même temps, deux types d'attaques sont moins fréquentes qu'en 2017 : les attaques par déni de service et la défiguration de site web.

Les techniques d'ingénierie sociale et les vulnérabilités résiduelles touchent une entreprise sur deux et viennent compléter le tableau des cyber-risques auxquels les entreprises sont les plus exposées.

Face à ces risques, de nombreuses solutions techniques sont implantées. Au-delà des antivirus, VPN, filtrage web et AntiSPAM, on note aussi la souscription de plus en plus courante aux cyber-assurances (40 % ont souscrit un contrat).

Dans ce contexte, la transformation numérique induit également des risques liés aux usages des salariés de l'entreprise, en particulier la multiplicité des dispositifs. L'Internet des objets génère plusieurs défis à relever, et tout d'abord les failles de sécurité.

Malgré la prégnance des cyber-attaques, la sécurité représente moins de 5 % du budget IT dans près des deux tiers des entreprises.

(81) Répartition : 3 % de moins de 250 salariés, 29 % entre 250 et 5 000, 41 % entre 5 000 et 50 000, 27 % de plus de 50 000 salariés.

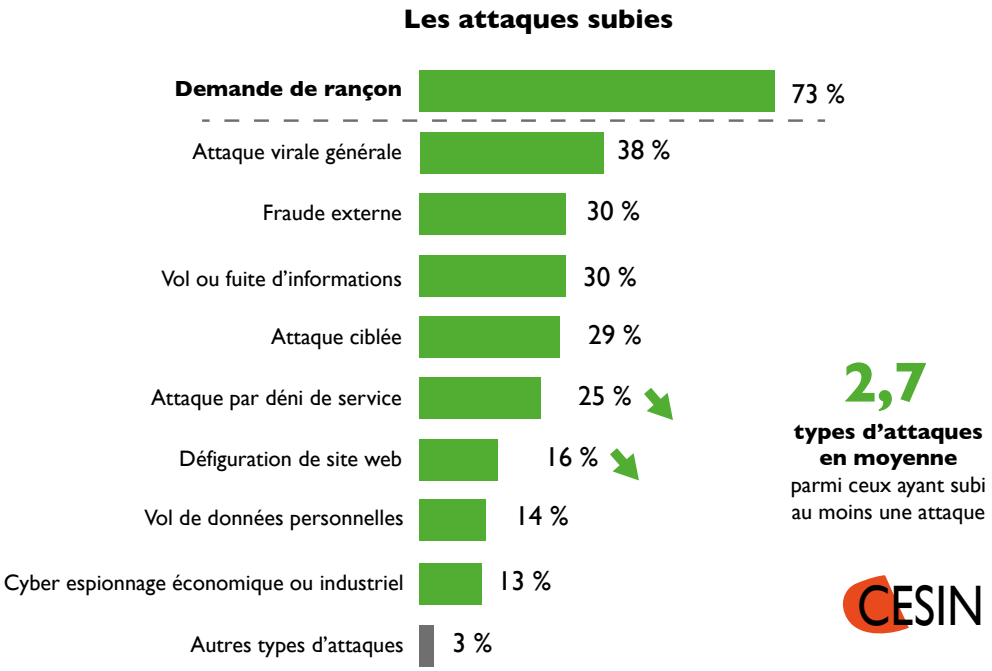


Figure 18 : Type d'attaque subies par les entreprises

Sur l'origine des incidents cyber, une étude menée par le cabinet d'audit et de conseil Deloitte[82] auprès de ses clients révèle que « 63 % des incidents de sécurité proviennent d'un collaborateur actif au sein des effectifs. En effet, le système informatique hautement sécurisé d'une entreprise peut être mis à mal très rapidement par une action malintentionnée ou une erreur de la part d'un salarié ». Ce facteur humain est clairement à prendre en considération.

En termes de nouvelles tendances, la perspective du règlement européen sur la protection des données, RGPD/GDPR, qui entrera en application le 25 mai 2018, provoque une prise de conscience salutaire chez les entreprises quant aux enjeux de la cybersécurité. Ce règlement rend tout professionnel ou prestataire de service responsable des données à caractère personnel qu'il détient. Les amendes pouvant aller jusqu'à 4 % du chiffre d'affaires mondial consolidé, une incitation forte repose maintenant sur l'écosystème des services et produits de cybersécurité. Selon l'étude du CESIN, alors que les enjeux pour demain seront plus humains que techniques, la mise en conformité au RGPD a déjà permis de refonder la gouvernance de la cyber-sécurité dans une entreprise sur deux.

(82) Cabinet Deloitte : L'évolution de la menace Cyber, janvier 2018

2.3.3 Vision européenne proposée par Europol

Le rapport d'Europol sur l'évaluation de la cybercriminalité de 2017 *(Internet Organised Crime Threat Assessment* dit « *iOCTA* ») ne fait que confirmer la tendance dégagée dans le rapport précédent.

La cybercriminalité continue de croître et d'évoluer. Certains domaines de la cybercriminalité ont connu une recrudescence d'activité, notamment les attaques de grande ampleur. Elle continue de prendre des formes nouvelles et de nouvelles orientations.

Les grandes tendances observées sont :

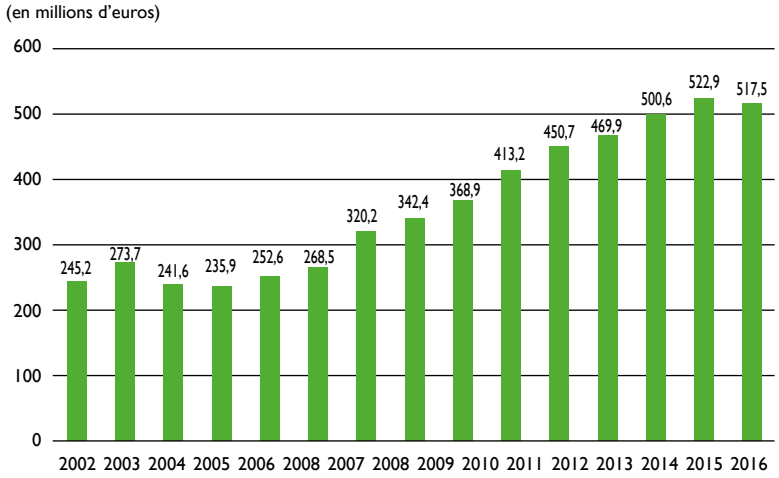
- La cybercriminalité continue de prendre des formes nouvelles et de nouvelles orientations.
- **Le succès des différentes variantes de rançongiciels chiffrants**
  Les attaques de ransomwares qui ont suscité de vives préoccupations de la part du public, ont masqué des menaces cybernétiques plus importantes auxquelles l'Europe est désormais confrontée.
- **La vulnérabilité d'un large éventail d'infrastructures critiques** aux cyber-attaques génériques.
- Une réorientation des malfaiteurs vers des logiciels malveillants alternatifs aux kits d'exploitation **en raison de l'action conjointe des services répressifs et du secteur de l'industrie.**
- **La vulnérabilité de l'Internet des objets** et la multiplication des attaques en déni de service (DdoS) générées à partir d'une variété d'objets connectés non sécurisés
- Le recours accru aux médias sociaux **par les auteurs de pornographie enfantine** pour le partage et la distribution de matériel pédopornographique.
- L'augmentation de **la fraude bancaire qui se caractérise notamment par :**
  - **La persistance des logiciels malveillants** tels que les chevaux de Troie bancaires.
  - L'émergence **des attaques directes contre les réseaux bancaires** pour manipuler les soldes correspondant aux cartes, pour prendre le contrôle des guichets automatiques ou pour transférer directement les fonds.
- La **confirmation que le darknet** est un lieu de marchés illicites florissants. La disponibilité des outils et des services propres à la cybercriminalité (par exemple des malwares) semble augmenter rapidement.
- **Le défi du cryptage** tant en raison de **l'utilisation des crypto-monnaies par les cybercriminels** que des obstacles à l'enquête liés à **l'utilisation d'outils de chiffrement.**
- **La convergence du cyber et du terrorisme**
  Alors que les terroristes continuent à utiliser Internet principalement à des fins de communication, de propagande et de partage des connaissances, leurs capacités à lancer des cyber-attaques restent limitées. Des échanges entre terroristes sont aussi détectés dans le Darknet. Cela concerne principalement les campagnes de collecte de fonds, l'utilisation de marchés illicites et la propagande hébergée.
- Les **techniques d'ingénierie sociale** sont une tactique essentielle pour la commission de nombreux crimes, souvent complexes, liés au cyber et facilités par lui.

2.3.4 Le coût de la cybercriminalité

L'évaluation du coût de la cybercriminalité reste encore un exercice complexe et repose pour l'instant sur des études évaluatives ou des sondages. Très souvent, elles se basent sur l'impact économique pouvant affecter les entreprises plutôt que les particuliers, sachant que le coût global d'une attaque informatique ne peut être précisé immédiatement. En voici quelques exemples récents :

- L'impact financier des incidents informatiques est encore mal connu et dans plus de la moitié cas, il n'est pas évalué (Etude « Menaces informatiques et pratiques de sécurité » du Clusif 2016). Selon l'étude du CESIN (cf. infra), dans près d'un cas sur deux, les attaques ont des impacts concrets sur le business des entreprises touchées : indisponibilité du site Internet, arrêt significatif de la production, perte de CA, retard de livraison….
- Pour les entreprises[83], le coût moyen d'un détournement de données serait de l'ordre de 3,62 millions de dollars, avec un coût par enregistrement évalué à 141 dollars (en baisse de 10 % par rapport à 2016) ;
- Selon un sondage effectué auprès de 1.000 entreprises[84], le coût estimé d'une violation de sécurité serait en moyenne de 330.000 euros pour une entreprise de 1.000 salariés ou moins, et 1,3 millions d'euros pour une entreprise de plus de 5000 salariés.
- L'Observatoire de la sécurité des moyens de paiement (OSMP) publie chaque année le volume précis des montants frauduleux, les préjudices étant portés selon les cas aux banques, aux commerçants ou parfois aux clients. Dans le schéma ci-après, on observe que le montant global de la fraude, liée aux cartes de paiement, s'élève, concernant les transactions traitées dans les systèmes français (cartes françaises et étrangères), à 517,5 M€ en 2016 (dont 318,7 M€ réalisée sur des transactions sur Internet), en baisse de 1 % par rapport à 2015.
- Enfin, la gendarmerie nationale réalise depuis 2014 une étude des dossiers se rapportant à la cybercriminalité et qui font l'objet d'une remontée des « comptes rendus de police judiciaire ». Relevé dans ce contexte, le préjudice approximatif est estimé à 363 millions d'euros contre 286,6 millions pour l'année 2016 (+26 %).

(83) Etude Ponemon Institute pour IBM 2017 - https ://www.ibm.com/security/infographics/data-breach//
(84) NTT Com Security, « Brèches de sécurité - quel est le coût réel pour votre business? », octobre 2016



Source : Observatoire de la sécurité des moyens de paiement

Figure 19 : Montant de la fraude sur les transactions traitées dans les systèmes français, cartes françaises et étrangères

Partie III

Les actions du ministère de l'Intérieur

Parallèlement à l'action des services opérationnels, la politique de lutte contre les cybermenaces a connu un renouveau et a gagné en visibilité avec la parution du décret n° 2017-58 du 23 janvier 2017 instituant un délégué ministériel aux industries de sécurité et à la lutte contre les cyber menaces (DMISC) au ministère de l'Intérieur.

Par son rôle de coordination de l'ensemble des acteurs concernés au sein du ministère et son action en lien avec les acteurs de la filière industrielle de sécurité, la délégation ministérielle a vocation à jouer un rôle de pilotage stratégique en matière de lutte contre les cybermenaces.

Pour l'exercice de ses missions, elle fait appel à l'ensemble des services placés sous l'autorité du ministre de l'Intérieur, à l'exclusion des services d'inspection.

Elle initie des partenariats et définit des plans d'action au niveau du ministère, mais assure aussi le dialogue entre l'Intérieur et les différents ministères impliqués, ainsi qu'avec les acteurs publics et privés concernés.

3.1. Prévenir et protéger

Le ministère de l'Intérieur, par sa présence dans les territoires, est un acteur majeur de la sensibilisation des particuliers, des acteurs économiques et des collectivités territoriales.

3.1.1. Les actions de prévention

3.1.1.1 Grand public

Les services du ministère de l'Intérieur ont participé tout au long de l'année 2017, à de nombreux salons, rencontres et conférences, ouverts au public, au cours desquels les problématiques liées aux cybermenaces sont abordées. Il peut s'agir d'événements à connotation professionnelle comme le Forum international de la cybersécurité de Lille (FIC) ou le Forum du Rhin supérieur sur les cybermenaces de Strasbourg, mais aussi d'évènements destinés au grand public ou à un public plus ciblé, comme le salon des séniors à la Porte de Versailles.

L'opération « Permis Internet », initiée en 2014 et conduite par les services de police et de gendarmerie, est un programme national de prévention pour un usage d'Internet vigilant, sûr et responsable à l'attention des enfants de CM2 et de leurs parents. Ce sont à ce jour plus de 950 000 élèves qui ont pu bénéficier de cette sensibilisation et acquérir les gestes réflexes de la navigation sur le Net.

Des actions à destination d'un public de seniors sont également menées au niveau local par certaines unités territoriales. Ces pratiques doivent encore être développées.

La police et la gendarmerie nationales délivrent des messages de manière proactive et maîtrisée afin d'informer la population. Le pilotage de cette stratégie relève de leurs services d'information et de communication (SICOP et SIRPA), qui organisent la communication via les réseaux sociaux (Facebook, Twitter, Instagram) et de leurs sites Internet.

Enfin, des actions de sensibilisation aux risques de cybermalveillance sont aussi mises en œuvre par un certain nombre d'associations partenaires du ministère de l'Intérieur, telles que le CECyF (Centre Expert contre la cybercriminalité Français), Antibot, Signal Spam, Phishing Initiative, la plateforme 33 700 qui permet de lutter contre les spam sms et spam vocaux, l'association « Point de Contact » notamment dans le cadre de sa mission de lutte contre les contenus odieux sur Internet, ou encore l'association e-Enfance.

3.1.1.2 Sensibilisation du monde économique

Les mesures préventives ont pour objectif d'anticiper les menaces et de protéger les acteurs économiques a priori contre les risques et dangers numériques auxquels ils sont exposés.

La sensibilisation de tous les acteurs économiques aux risques encourus et moyens de protection existants constitue aussi un élément essentiel de la stratégie, puisqu'elle contribue à réduire les risques encourus et à les motiver à participer activement au renforcement de leur propre cybersécurité.

Le ministère de l'Intérieur a renforcé les compétences des référents sûreté de la préfecture de police, de la gendarmerie et de la police nationales, présents au niveau territorial, afin qu'ils permettent aux entreprises qu'ils conseillent, de mieux se prémunir également contre la cybercriminalité.

En 2017, la direction générale de la sécurité intérieure (DGSI) a organisé près de 1 550 conférences sur la protection de l'information et la sécurité numérique, notamment à l'endroit des entreprises et institutionnels. Environ 80 000 auditeurs ont ainsi été sensibilisés, à des thématiques abordant le risque cyber, la sécurité économique, la menace terroriste ou les questions de radicalisation en entreprise. Les sujets abordés évoluent progressivement en fonction des nouvelles menaces ou des nouveaux dispositifs juridiques, nationaux ou européens. Ainsi, en 2017, un accent a été porté sur les ingérences étrangères, les tentatives de déstabilisation mais aussi sur la conformité et les impacts du Règlement européen sur la protection des données (RGPD).

Les publics sensibilisés demeurent très divers (acteurs institutionnels ou privés, PME ou groupes, agents, salariés, comité exécutif, etc.) et la sensibilisation peut faire l'objet d'une conférence généraliste ou d'ateliers plus spécifiques pour des directeurs des affaires juridiques ou des directeurs sûreté.

La sous-direction de lutte contre la cybercriminalité (SDLC) de la direction centrale de la police judiciaire (DCPJ) participe aussi activement à cet effort de sensibilisation.

En termes d'évolutions structurelles au niveau des acteurs de la cybersécurité, la montée en puissance des centres de réponse à incident (Computer security and incident response team - CSIRT) doit être soulignée. Ces entités rendent des services à différents bénéficiaires en matière de cybersécurité. Les CSIRT peuvent être nationaux, tel le CERT-FR de l'ANSSI, internes (CERT-SOCIETE GENERALE) ou commerciaux (CERT-WAVESTONE). Existants depuis 30 ans, ils constituent, avec les forces de l'ordre et les autorités de cybersécurité, des acteurs incontournables dans la lutte contre la cybercriminalité. Organisés en réseau et outillés pour partager les informations qualifiées de manière automatique, les CSIRT disposent d'une grande expertise et d'une très forte réactivité.

Le CERT-FR de l'ANSSI coordonne l'InterCert français qui comprend l'ensemble des centres de réponse à incident français que le nouveau CSIRT-PJ de la SDLC a intégré en septembre 2017. L'InterCert permet à l'ensemble des CSIRT français de s'organiser et d'échanger de la manière la plus transparente et efficace possible. Pour la SDLC, il s'agit également d'une forme de partenariat privilégié qui produit des résultats au quotidien.

Ces actions de sensibilisation du CSIRT-PJ recouvrent à la fois les risques techniques et organisationnels connus en matière de cybersécurité, les bonnes pratiques, mais surtout une présentation approfondie en matière de cybercriminalité. Les entreprises se voient détailler les modes opératoires des cybercriminels, ainsi que leurs motivations

et organisations. L'objectif est de relever le niveau d'appréhension du phénomène en démystifiant l'univers des cybercriminels.

La division de l'anticipation et de l'analyse (D2A) de la SDLC, auquel appartient le CSIRT-PJ, est pilote sur deux actions opérationnelles d'Europol (EMPACT), visant à développer la coopération des forces de l'ordre avec les CSIRT. La première se situe au niveau stratégique et vise à déterminer les bonnes pratiques en matière d'échange d'information. La seconde porte plus spécifiquement sur la coopération en cas de crise majeure de type Wannacry et requérant une réactivité particulière.

Par ailleurs, les services opérationnels réalisent et diffusent un certain nombre de supports de prévention à destination des entreprises, comme le livret « réagir à une attaque information : 10 préconisations »[(85)] de la SDLC, le flyer « Cybermenaces : comment protéger votre entreprise » ou la fiche « Sensibiliser les entreprises (RGPD) » de la Section sécurité économique et protection des entreprises de la DGGN, ou encore la plaquette « cybersécurité / cybervigilance » présente sur le site Internet de la préfecture de Police dans l'espace dédié aux entreprises.

3.1.1.3 Intelligence économique territoriale

Grâce à son maillage territorial, le service central de renseignement territorial (SCRT) joue un rôle de soutien et de capteur au profit des services spécialisés en charge de l'intelligence économique, dans le respect des attributions des services de l'État, de celles des ministères compétents et en lien avec les préfets de région, au cœur du dispositif.

L'action du SCRT s'effectue via un pôle « Intelligence économique » (IE), chargé de transmettre aux échelons départementaux des éléments de langage adaptés, d'animer et de consolider un réseau de référents IE, d'exploiter et de valoriser les notes d'information transmises par les services territoriaux.

Ces notes de valorisation sont transmises aux ministères concernés et au Service de l'information stratégique et de la sécurité économique (SISSE), rattaché à la Direction générale des entreprises au Ministère des Finances.

Le pôle IE anime un réseau de 102 référents en intelligence économique, issus des services départementaux du renseignement territorial.

Les référents IE participent aux réunions des comités de sécurité économique organisés par les secrétariats généraux à l'administration régionale (SGAR). Le pôle IE du service central du renseignement territorial, concoure aux groupes de travail spécialisés des services du haut fonctionnaire de défense, du secrétariat général de la défense et de la sécurité nationale et du service de l'information stratégique et de la sécurité économique (SISSE).

L'analyse « hors atteintes de sécurité » des entreprises, au niveau national, a concerné 3 431 notes depuis la création du pôle IE en février 2014.

Parmi celles-ci, le pôle IE a distingué et valorisé 234 notes de fond relevant d'atteintes à la sécurité économique. La part des atteintes de cybercriminalité représente 25,80 %, ce qui positionne la cybercriminalité à la seconde place des atteintes relevées, juste derrière les prédations économiques (27,91 %), à égalité avec les prédations financières,

(85) https ://www.cybermalveillance.gouv.fr/operations/reagir-a-attaque-informatique/

et devant les fraudes de la famille des FOVI (8,71 %) et les captations de savoir-faire (8,34 %).

3.1.2. Protection des systèmes d'information du ministère

Chaîne fonctionnelle de sécurité des systèmes d'information (SSI)

L'organisation de la sécurité des systèmes d'information du ministère est structurée par le réseau des responsables de la sécurité des systèmes d'information (RSSI)(86), présents dans chaque administration centrale et dans chaque préfecture. Ce réseau est animé par le fonctionnaire des systèmes d'information (FSSI), placé auprès du haut fonctionnaire de défense et de sécurité adjoint.

Au plan national, la détection, la qualification et la réaction aux incidents SSI est assurée par le centre de cyberdéfense du ministère de l'intérieur (C2MI) à Toulouse. Ce centre maintient et développe également les systèmes contribuant à la détection, à l'analyse et au traitement de ces incidents.

Enfin, différentes actions de sensibilisation ont eu lieu auprès de l'ensemble des agents du ministère. En particulier, cinq campagnes de sensibilisation au risque de phishing ont été réalisées par le centre de cyberdéfense, avec l'envoi au total de 20 000 courriels de test.

3.2. Enquêter

3.2.1 L'accueil des victimes d'actes de cybercriminalité

La prise en compte des victimes passe avant tout par la capacité d'un dispositif à accueillir, écouter, analyser et orienter vers le service idoine.

Toute victime de cybercriminalité doit être accueillie par le ministère, comprise et pouvoir déposer plainte si elle le souhaite, ou fournir des informations qui seront exploitées.

Outre la formation de tous les acteurs chargés de l'accueil des victimes, les services opérationnels finalisent les dispositifs de recueil de plaintes pour mieux partager et exploiter certaines données relatives à la cybercriminalité (escroqueries sur Internet et usages frauduleux de cartes bancaires avec les outils THESEE et PERCEVAL – *cf §3.3.4*). Les victimes peuvent déjà être orientées par certains services télématiques existants.

En 2017, la plate-forme Info-escroquerie de l'OCLCTIC a reçu 28.287 appels, soit une augmentation de 24 % entre 2016 et 2017. 65 % d'entre eux étaient liés à des escroqueries sur Internet (escroqueries à l'achat et à la vente, escroqueries à la téléphonie, usurpation de messagerie, phishing…). Beaucoup étaient consécutifs aux événements liés aux attaques Wannacry et NotPetya (en mai et juin), ainsi qu'à la révélation d'une faille de sécurité Microsoft (novembre). Les signalements de phishing (15 % du total) et de malwares (8 %) ont, quant à eux, doublé.

3.2.2 L'action des services spécialisés : investigation, formation, coopération

Les services spécialisés dans la lutte contre la cybercriminalité poursuivent leur développement tant en matière d'investigation que d'analyse numérique (forensic). Le schéma général tend, dans ces deux domaines, vers la mise en place d'un réseau territorial animé ou piloté par les services centraux.

(86) La nomination d'un RSSI donne lieu à son inscription à une formation obligatoire, réalisé par le centre de formation de l'ANSSI.

OCLCTIC

La section opérationnelle de l'OCLCTIC a ouvert 72 nouvelles enquêtes en 2017 (contre 88 en 2016, 160 en 2015 du fait des contenus de terrorisme en ligne), et procédé à 39 gardes à vue (60 en 2016, 32 en 2015) qui ont abouti à 17 écrous (25 en 2016, 18 en 2015). PHAROS a transmis, de son côté, 303 procédures (228 en 2016) aux services territoriaux de police ou gendarmerie, principalement pour des faits d'atteintes aux mineurs (66 %) ou de faits constatés de discrimination (15 %).

La section d'assistance technique de l'OCLCTIC a analysé 1.239 supports numériques en 2017 (1.001 en 2016), tant pour les unités de la SDLC (234), que pour l'ensemble des autres services d'investigation (700) et la SDAT (305). L'exploitation de ces contenus a pu apporter une plus-value décisive à 65 enquêtes.

Développant une dynamique au niveau territorial, la police nationale déploie 13 laboratoires d'investigation opérationnelle numérique (LION)[87] afin de permettre un traitement déconcentré des supports numériques collectés. Leur montée en puissance se poursuit. Par ailleurs, la SDLC est en charge de l'animation du réseau des investigateurs en cybercriminalité (ICC) déployés dans les différentes directions centrales de la police nationale.

En matière de coopération internationale opérationnelle, l'année 2017 a été marquée par une augmentation notable des dossiers traités avec Interpol (1981 contre 1326 en 2016), du fait d'une amélioration des circuits de remontée d'information en provenance de PHAROS et d'une politique renforcée de signalements. 808 messages ont été échangés avec Europol (901 en 2016) et 239 avec le réseau 24/7 de la Convention de Budapest (132 reçus de la part des partenaires étrangers et 107 émis vers l'international). 101 demandes de gels de données ont été émises vers l'étranger (principalement vers les États-Unis, les Pays-Bas et la Russie) et 115 ont été reçues et traitées par le point national 24/7 (dont 44 demandes américaines, 19 britanniques, 5 suisses et 5 israéliennes).

C3N et IRCGN/INL

Deux départements du Centre de lutte contre les criminalités numériques (C3N) conduisent des enquêtes judiciaires, souvent sur la base de constatations dressées d'initiative. 127 enquêtes ont été ouvertes en 2017, 53 concernant des atteintes aux systèmes d'information. Outre le suivi des phénomènes cybercriminels, le C3N assure l'appui opérationnel du réseau décentralisé « Cybergend », comprenant tous les enquêteurs spécialisés, qu'il anime et coordonne. Il leur apporte une assistance en temps réel pour les investigations en téléphonie ou sur Internet (GUTI) ; 2120 assistances ont été traitées en 2017, ainsi que 7800 appels sur la « hotline » dédiée. Par ailleurs, 35 missions d'appui spécialisé ont été effectuées en 2017 par la projection de personnels spécialisés au profit des unités judiciaires territoriales.

Les experts du département Informatique-Electronique de l'Institut de recherche criminelle de la gendarmerie nationale (IRCGN) ont traité en 2017, 370 dossiers provenant des unités (contre 318 en 2016). Demandant un haut niveau de compétence, ces dossiers ne peuvent être traités par les enquêteurs spécialisés NTECH au niveau départemental. Plus de 600 supports numériques ont été analysés ; 165 contenus chiffrés ont été décryptés et 176 téléphones ont été déverrouillés.

Au niveau départemental, les cellules d'identification criminelle et numérique (CICN) mises

(87) au sein des sous-directions de la DCPJ (SDAT, SDLCODF, SDLC), de la DRPJ de la Préfecture de Police, des directions interrégionales ou régionale de la police judiciaire (DIPJ et DRPJ).

en place en octobre 2016 permettent de concentrer au sein d'une même structure les compétences liées à la criminalistique classique (traces et indices physiques) et numérique. Le regroupement progressif d'enquêteurs spécialisés NTECH sur ces plateaux techniques équipés en matériels d'analyse adaptés permet un engagement dans une démarche d›assurance qualité pour faire face à la volatilité de la preuve numérique. Plusieurs dizaines de milliers de supports numériques y ont été analysés en 2017.

BEFTI

Outre la formation, la BEFTI de Préfecture de Police de Paris a pour mission d'enquêter et d'apporter son assistance aux unités de la plaque parisienne.

En 2017, la BEFTI a ouvert 222 enquêtes et en a clôturé 188. Elle a un important portefeuille de 253 enquêtes en cours. Sur les 61 mis en cause de 2017, 38 ont été placés en garde à vue et 23 entendus librement. Ces enquêtes ont débouché sur 1 déferrement et 13 COPJ/CRPC.

Par ailleurs, elle a réalisé 218 assistances au profit des services de la DRPJ et, en moindre importance, de la DSPAP. 687 supports numérique ont été analysés. La fonction de guichet unique de la BEFTI fluidifie les demandes souvent complexes des services de la Préfecture de Police de Paris.

DGSI / PJ

La DGSI dispose, au sein de sa sous-direction des affaires judiciaires, d'une section spécialisée dans le traitement des affaires liées à la cybercriminalité. Ce service dispose d'une compétence exclusive pour évoquer toutes les infractions résultant d'une violation des articles inscrits au chapitre 3 du Code pénal (articles 323-1 à 323-7), dans la mesure où ces actions sont directement menées contre les intérêts fondamentaux de la Nation. Il s'agit de toutes les attaques informatiques dirigées contre les systèmes et réseaux gouvernementaux, les attaques contre les systèmes et réseaux appartenant à des opérateurs d'importances vitales (OIV) ou des établissements disposant de zones à régimes restrictifs, et enfin, toute atteinte à un système susceptible de porter atteinte aux intérêts fondamentaux de la nation.

Le partenariat avec les opérateurs de l'Internet

En 2017, les structures de dialogue mises en place ont été consolidées.

Piloté par la DMISC, le Groupe de contact permanent (**GCP**), mis en place par le ministère après les attentats terroristes de 2015, poursuit le travail d'amélioration du signalement et du retrait des contenus illicites par les opérateurs (Apple, Google, Twitter, Microsoft, Facebook) et veille à une meilleure prise en compte des demandes adressées par les enquêteurs français pour obtenir un certain nombre de données (données de connexion ou de profil), prioritairement dans le cadre des affaires de terrorisme. Le GCP s'est réuni en formation plénière à 12 reprises entre mai 2015 et janvier 2018.

Par ailleurs, la sous-direction de la lutte contre la cybercriminalité de la direction centrale de la police judiciaire a été chargée d'organiser des réunions technico-opérationnelles en bilatéral avec chacun des cinq acteurs de l'Internet et les guichets uniques de chacune des directions opérationnelles, afin de traiter des difficultés propres à chacun. Les guichets uniques mis en place au sein des directions sont chargés des relations opératives avec les prestataires privés. Ils sont composés d'enquêteurs spécialisés et offrent un service d'astreinte. En 2017, la SDLC

a organisé les 4e et 5e journées d'information, au cours desquelles les sociétés OVH, La Poste, La Maison du Bitcoin, iBrowse, Ethereum, Blockchain et Verizon ont présenté leurs modalités de fonctionnement respectives et les informations techniques qu'ils sont en mesure de fournir à des enquêteurs. Chacune des journées a réuni près d'une centaine de personnes issues des différents services de la Police Nationale, de la Gendarmerie Nationale, de la brigade d'enquête des finances publiques, la « Cyberdouane », les référents « cyber » du parquet de Paris, etc.

Au niveau tant européen qu'international, la structuration des échanges avec le secteur privé au sein des groupes de travail a été favorisé encore cette année. Le ministère de l'Intérieur, dans une démarche coordonnée par la DMISC et co-pilotée avec le Secrétariat d'État au Numérique, soutient les travaux qui sont menés avec les opérateurs de l'Internet par Europol et dans le cadre de l'EU Internet Forum. L'objectif premier de ces travaux est d'obtenir des opérateurs de l'Internet qu'ils s'engagent à retirer les contenus terroristes dans l'heure qui suivent leur publication, pour éviter leur dissémination sur la toile (on parle de la Golden Hour).

La formation des enquêteurs

Les évolutions technologiques permanentes conduisent les services de police et les unités de gendarmerie à adapter leurs méthodes de travail et la conduite des investigations.

Outre la formation de policiers et gendarmes spécialisés dans l'investigation numérique (505 investigateurs en cybercriminalité [ICC] et 320 enquêteurs en technologie numérique [NTECH]), le ministère forme aussi des premiers intervenants, policiers et gendarmes. A titre d'illustration, des formations de premier niveau pour des référents dans les commissariats de la préfecture de Police sont proposées pour une meilleure compréhension de l'attente des victimes, l'amélioration de la prise de plainte et la collecte des éléments techniques nécessaires.

Enfin, le ministère veille aussi à intégrer des modules d'enseignement en matière cyber à la formation initiale dans les écoles de police et de gendarmerie. En effet, quelle que soit l'infraction traitée, toutes les enquêtes présentent désormais un volet lié à l'investigation numérique.

Au niveau international, le ministère de l'Intérieur a aussi concouru au renforcement des compétences des services partenaires africains dont certains des pays demeurent le foyer de groupes criminels régulièrement impliqués dans les faits d'escroquerie en ligne (formation dispensée en Côte d'Ivoire, au Mali, Cameroun, Sénégal).

3.3. Innover

3.3.1 Recherche et développement

La DGGN a identifié un axe « cyber » comme prioritaire dans son plan stratégique de recherche et d'innovation à 5 ans, s'appuyant sur des développements internes, des expérimentations, des doctorats et des partenariats académiques.

La Mission Prospective et Management de l'Innovation de la préfecture de Police mène avec un consortium d'entreprises européen dont le commissariat à l'énergie atomique (CEA), un projet de développement de traitement de données recueillies en masse au profit d'investigateurs numériques ; c'est le projet européen ASGARD

Les échanges techniques et technologiques avec le ministère des Armées se développent également, notamment avec le commandement cyber de l'état-major des armées et la Direction générale de l'Armement (DGA). De même, les échanges avec le monde académique se densifient progressivement, en particulier avec le CNRS, l'Institut national de recherche en informatique et en automatique (INRIA) et le CEA.

Pour le ministère de l'intérieur, un objectif important sera d'établir une feuille de route technologique dans le domaine de la lutte contre la cybercriminalité.

3.3.1.1 Outils d'investigation et de « forensics »

Les enquêteurs et les techniciens travaillant dans l'investigation ou l'analyse numérique (« forensics ») ont besoin d'outils spécifiques, adaptés à leur environnement de travail. Toutefois, les différents produits disponibles sur le marché ne répondent pas toujours à l'ensemble des spécifications souhaitées.

Aussi, les services centraux spécialisés des directions opérationnelles développent régulièrement un certain nombre d'outils pour répondre à ces besoins ; ces outils logiciels ou matériels sont alors partagés par les différents services intéressés.

Engagés dans le soutien opérationnel des enquêteurs, les personnels du Pôle Judicaire de la Gendarmerie (IRCGN, C3N) ont ce rôle ; les outils spécialisés réalisés sont destinés à être diffusés auprès des unités de terrain, ou à être mis en œuvre par les experts du pôle pour traiter des demandes des services d'enquête territoriaux.

Ainsi, le département Informatique et électronique (INL) de l'IRCGN a développé et diffusé un outil, dénommé GendExtract, permettant l'extraction et l'exploitation rapides de données contenues dans un ordinateur de type PC ou MAC, sans modifier son contenu, afin de préserver la preuve numérique. Cet outil avait été rendu nécessaire pour pouvoir faire face aux perquisitions administratives dans le cadre de l'état d'urgence suite aux événements de novembre 2015. Dès fin novembre 2015, GendExtract a été diffusé aux services spécialisés du ministère. Une nouvelle version du logiciel a vu le jour en 2017.

Le C3N a développé un outil appelé ARTIST, permettant de collecter automatiquement et de pré-analyser les éléments d'une page web et du serveur l'hébergeant, pour mettre en évidence les éléments potentiellement intéressants pour l'enquêteur dans un rapport. De même, pour les besoins d'analyse et de renseignement, il a été réalisé un logiciel dénommé SORTINGHAT, permettant en premier lieu de catégoriser les messages d'information judiciaire (CRPJ cyber) et dans un second temps, d'effectuer des rapprochements criminels sur la base de mots clés relatifs à la manière d'opérer. Cet outil permet également d'avoir une vision statistique du phénomène cyber en gendarmerie.

De son coté, dans ce cadre de développement d'outils « forensiques » au service de l'investigation numérique, la section d'assistance technique de l'OCLCTIC a développé une nouvelle version (3.7) du pack « DARWIN » (pour Discrimination, Analyse, Recherche, Windows). Il s'agit d'une clé USB autonome qui, connectée à un ordinateur éteint, analyse son disque dur sans l'altérer, garantissant la fiabilité de la preuve en cas de découverte d'une infraction. Elle s'adapte à tous les systèmes d'exploitation : Windows, Linux et Mac. Mis à disposition des enquêteurs, cet outil a été décliné en deux configurations distinctes adaptées aux deux niveaux de technicité que sont l'ICC et le PICC (primo-intervenant).

Par ailleurs, une nouvelle version du rapport semi automatisé d'analyse numérique a été diffusée à l'ensemble de la communauté ICC en octobre 2017. Cet outil permet de récupérer l›ensemble des informations relatives à l›affaire traitée et au scellé examiné afin d›établir directement une trame de rapport d›analyse en détaillant la succession des étapes à respecter pour chaque support analysé.

3.3.1.2 Projet de recherche académique

Le Pôle Judicaire de la Gendarmerie accueille régulièrement des étudiants et élèves ingénieurs dans le cadre de stage de recherche.

En 2017, un projet de recherche académique a porté sur le chiffre noir de cybercriminalité. Le rapport de stage de l'ENSAI Rennes rédigé par Mélanie Drégoir portait sur l'effet Iceberg : définition, mesures et méthodes de traitement et applications aux données cybercriminelles.

« En général, pour avoir une vision globale de l'impact d'un phénomène criminel, la Gendarmerie Nationale peut se fier à son canal de dépôt de plaintes qui lui permet de connaître le nombre de victimes et le préjudice que ces dernières ont subi.
Cependant, en cybercriminalité, un effet iceberg prononcé existe du fait de l'absence de dépôt de plainte, ou, dans les cas les plus graves, à l'absence même de détection du problème par les entités atteintes. Par conséquent, pour les forces de l'ordre, le dépôt de plaintes ne représente que la partie visible d'un phénomène criminel et ne permet en aucun cas d'accéder à la vérité de terrain.
Pendant 5 mois, au centre de lutte contre les criminalités numériques (C3N), nous avons tenté de caractériser l'effet iceberg en cybercriminalité en nous focalisant sur les phénomènes des rançongiciels. Ce rapport porte sur l'étude de l'effet iceberg (définition et causes), la proposition de méthodes pour le mesurer et enfin l'application de ces méthodes aux données cybercriminelles liées aux ransomwares. Il conclut sur des propositions pour améliorer les estimations.
Les différents travaux ont conduit à envisager deux approches. La première propose des méthodes permettant l'estimation de taille de population ("German Tank Problem" et Capture-Recapture) uniquement à partir de la partie émergée. La deuxième approche décrit des méthodes faisant appel à des données externes.
Il en ressort que, malgré un état de l'art actuel assez complet sur l'effet iceberg, la première approche reste complexe à appliquer et propose des estimations qui restent difficilement défendables d'un point de vue statistique. La seconde approche semble plus prometteuse et nous permet d'estimer que sur 267 victimes d'une cyberattaque, la Gendarmerie Nationale ne parvient à capter seulement qu'une plainte. » [(88)]

3.3.2 Partenariat Public-Privé

3.3.2.1 Travaux de la filière industrie de sécurité

Le Comité de Filière des industries de sécurité (CoFIS) a été créé, d'une part, pour faire face aux menaces contre la sécurité des biens et des personnes, et d'autre part, pour soutenir la compétitivité des acteurs français sur le marché mondial de la sécurité. La DMISC représente le ministre de l'Intérieur dans les travaux du Comité de la Filière des industries de sécurité (COFIS) et assure le suivi des actions engagées dans ce cadre. En lien avec les travaux de la filière, la délégation assure la coordination des actions menées par les services du ministère de l'Intérieur en matière de recherche de sécurité.

Le CoFIS s'attache notamment à soutenir la recherche et l'innovation. Ainsi, en liaison avec le Commissariat général à l'investissement et la banque publique d'investissement Bpifrance, il a lancé, fin 2016, un appel à projets dans le domaine de la sécurité, qui incluait notamment un démonstrateur de gestion de l'identité numérique forte et des

(88) Rapport de stage sur l'Effet Iceberg de Mélanie Drégoir – ENSAI RENNES

briques technologiques pour la cybersécurité des systèmes industriels. Si la démarche n'a pas pu aboutir, elle a néanmoins montré la vivacité du tissu industriel et stimulé les réflexions technologiques.

En complément, le CoFIS a mis en place un observatoire de l'industrie de sécurité : élargissant les travaux antérieurs et l'observatoire de la confiance numérique de l'alliance pour la confiance numérique (ACN), il apporte une vision plus précise sur la filière, et notamment sur le segment « services et produits de cybersécurité ».

Le programme-cadre européen de recherche et d'innovation « **Horizon 2020** » est un vecteur important pour le financement de la recherche en sécurité, d'autant plus que ce secteur bénéficie de spécificités administratives de nature à faciliter la participation industrielle et à intégrer les utilisateurs finaux. Deux domaines concernent plus particulièrement la cybersécurité : Digital Security et Information & Communication Technologies. Les résultats de la France dans ces deux domaines sont toutefois plutôt en-deçà de la moyenne : un travail en profondeur doit donc être entrepris auprès de l'industrie de cybersécurité pour comprendre cette faible participation et motiver les participations. En particulier, l'attention devra se porter sur l'appel à projets de 2018 visant à la mise en réseau des centres de compétences européens en cybersécurité.

3.3.2.2 Cercles de réflexion

Des personnels du ministère de l'Intérieur participent régulièrement à des échanges et présentations au sein de cercles de réflexion, comme l'Institut Montaigne, l'Institut français des relations internationales (IFRI), la Fondation pour la recherche stratégique (FRS) ou encore le Centre d'Etude et de Prospective Stratégique (CEPS), au sein desquels des sujets liés à l'espace numérique et à la sécurité sont développés. Ils prennent part également à des manifestations organisées par ces Think Tank comme les journées d'étude FRS (Objets connectés et défense : quel avenir, quels risques ?) ou des conférences dans d'autres enceintes comme la CyberTaskForce ou le CyberCercle, qui présente un cadre privilégié de rencontre Public-Privé autour des questions de sécurité et organise chaque année depuis 2013, les Rencontres Parlementaires de la Cybersécurité.

Plusieurs associations contribuent aussi aux échanges et à la réflexion, telles le CECyF (Centre Expert contre la cybercriminalité Français) et Cyberlex[89] qui ont produit conjointement début 2018, un rapport sur les évolutions possibles de la procédure pénale pour mieux lutter contre la cybercriminalité.

Des centres de recherche du ministère comme celui de l'école des officiers de la gendarmerie nationale (EOGN) ou de l'école nationale supérieure de la police (ENSP) associent très souvent des entreprises, industriels ou organismes privées à leur réflexion, en particulier lors des séminaires ou les ateliers de recherche qu'ils organisent[90].

(89) Cyberlex - L'association du Droits et des Nouvelles technologies - http://www.cyberlex.org/

(90) Atelier-recherche du CREOGN « Cybersécurité : quelle coopération public-privé? » à l'École Militaire (Paris) le 22 mars 2018. https ://www.alliancy.fr/agenda/atelier-de-recherche-cybersecurite-quelle-cooperation-public %C2 %AD-prive

3.3.3 Transformation numérique ; mieux signaler, mieux communiquer autour du cyber

3.3.3.1 Projet Néo PN/GN

La gendarmerie et la police ont déployé, en 2017, les projets NEO et NEOgend, qui visent à offrir aux personnels en mobilité l'ensemble des outils dont ils ont besoin pour accomplir leurs missions. Depuis les opérations de prévention et de contrôle des flux aux actes d'enquête judiciaire, l'intégralité du spectre missionnel bénéficie sur le terrain de la plus-value apportée par le programme NEO. L›adhérence avec les locaux des brigades et commissariats ainsi réduite, les militaires et fonctionnaires de police peuvent densifier leur présence auprès de la population. En augmentant la capacité opérationnelle des forces et en renforçant le lien avec le citoyen, le programme NEO s›impose comme un vecteur efficace de la police de sécurité du quotidien (PSQ).

Le projet s'appuie en cela sur 95.000 smartphones individuels et tablettes collectives, tous en fonctionnement aujourd'hui. NEO constitue par ailleurs un socle permettant d'intégrer les applications et fonctionnalités produites par la chaîne de l'innovation de l'institution, dont la démarche a d'ores et déjà recueilli un succès certain.

En termes de chiffres, les interrogations de fichiers en mobilité ont été multipliées par deux au niveau de la Gendarmerie, avec environ 1 million d'interrogations par mois avant le déploiement de NEOgend, et 2,5 millions après au mois fin 2017 (+ 150 %).

3.3.3.2 Brigade numérique de la Gendarmerie

Pour définir et animer sa stratégie de transformation numérique et de lutte contre les cybermalveillances, la gendarmerie s'est dotée d'une entité dédiée, la mission numérique de la gendarmerie nationale. L'un de ses premiers projets est la « brigade numérique », lancée le 27 février 2018, qui vise à moderniser l'offre de contact avec les usagers et de développer la notion de proximité numérique.

Cette unité permet aux usagers de contacter un téléopérateur de la gendarmerie par tchat/messagerie instantanée, et reçoit environ 1 200 sollicitations par semaine(91). Fonctionnant 7j/7 et 24h/24 et constituée de 20 gendarmes, cette unité nationale implantée à Rennes a vocation à opérer en ligne les fonctions réalisées dans les brigades territoriales. Les gendarmes bénéficient d'une habilitation judiciaire et réalisent les actes métier d'une brigade territoriale. Leur expertise est complémentaire d'une offre de télé-services sans intervention humaine. D'autres fonctionnalités, comme la prise de rendez-vous en ligne, sont prévus pour 2018-2019.

La brigade numérique s'articule autour de 4 fonctions : contact/accueil, prévention, investigation et intervention. Les deux premières représentent les objectifs principaux de cette unité opérationnelle. La fonction investigation décline la possibilité de recueillir par les canaux numériques des éléments constitutifs d'une infraction. Enfin, pour la fonction intervention, la brigade numérique n'est pas destinée à recevoir des sollicitations d'urgence. Cependant, elle doit être en mesure de faire face à tout cas non conforme (exemples : personne enfermée dans une pièce avec un ordinateur mais sans téléphone et en présence de cambrioleurs dans le bâtiment, personne suicidaire, etc.) et d'initier sans délai la réaction opérationnelle adéquate.

(91) Chiffres de mars 2018

3.3.3.3 La mise en place du réseau des référents cybermenaces zonaux

Le fait que 63 % des cyberattaques visant les entreprises soient liées à une faille humaine souligne l'importance que revêt la sensibilisation des organisations dans la prévention des risques. Dans un souci de prévention, et fort de l'expérience acquise avec les cyberattaques d'ampleur telles que NotPetya et Wannacry, la police nationale a conçu en 2017 un programme d'actions s'inscrivant dans une plus grande protection des données et des atteintes au tissu économique local. Aussi, il a été réfléchi à la constitution d'un réseau de référents territoriaux prolongeant l'action et les capacités partenariales de la division analyse et anticipation de la SDLC (DCPJ) sur le territoire national.

L'expérimentation des référents cybermenaces zonaux a été lancée en mars 2018. Les 3 premières cellules ont été implantées au sein des services chargés de la lutte contre la délinquance financière afin de bénéficier de leur connaissance du tissu local économique et sont constituées de commissaires de police référents, de réservistes civils issus du monde de l'entreprise et de partenaires privés. Placés sous l'autorité des directeurs interrégionaux de la police judiciaire, ces cellules viendront renforcer le dispositif de lutte contre les cybermenaces à l'échelle zonale tout en garantissant une doctrine et une stratégie d'action commune dans ce domaine d'action.

Ce dispositif zonal répond à la nécessité d'une action de proximité dans un objectif de prise de conscience de la menace cyber par l'ensemble des acteurs. Il s'articulera avec les différents acteurs dans ce domaine, à savoir notamment les préfets de la zone de défense et de sécurité, l'ANSSI, la CNIL et se traduira par des actions de diffusion des bonnes pratiques, d'alertes préventives, d'actions de sensibilisation et de prévention auprès des entreprises.

3.3.3.4 Communication de crise : Système Alerte et d'Information des Popula-tions (SAIP) et Médias Sociaux en Gestion d'Urgence (MSGU)

La Direction générale de la sécurité civile et de la gestion des crises est chargée du pilotage d'un certain nombre de mesures facilitant l'information du public en cas de crise. Comme nous l'avons vu lors des récentes attaques terroristes qui ont frappé la France, la gestion des crises prend souvent une dimension cyber et les outils numériques occupent une place croissante dans cette stratégie.

Médias Sociaux en Gestion d'Urgence (MSGU)

La DGSCGC utilise les médias sociaux dans le cadre de la gestion d'événements sur les trois niveaux d'engagement suivants :

- La veille : recherche d'éléments d'intérêt (dégâts, appels à l'aide…). L'acquisition d'un dispositif d'aide à la veille sur les médias sociaux a été mise à l'étude ;
- La diffusion d'information qui nécessite d'impliquer la communication opérationnelle de crise à chaque étape, de la sensibilisation des publics jusqu'aux consignes de sécurité lors d'événements. Elle comprend aussi la capacité des médias sociaux à diffuser des alertes sur demande des autorités de gestion de crise ;
- L'interaction avec la population implique la mise en place de liens avec les communautés d'internautes se fédérant autour de chaque crise pour soutenir les populations touchées, et également une capacité à répondre aux éventuelles sollicitations en situation d'urgence.

Dans les pays francophones, c'est l'association VISOV (Volontaires Internationaux en Soutien Opérationnel Virtuel) qui accompagne le gestionnaire de crise, des conventions ayant été signées avec la DGSCGC et plusieurs EMIZ (états-majors interministériels de zone), SDIS (services départementaux d'incendie et de secours) ou préfectures. VISOV, qui compte plus de 100 bénévoles, peut réaliser un suivi des médias sociaux et fournir des informations sur la situation ou contribuer à la communication de crise par l'intermédiaire d'un nombre important de comptes mobilisés. L'association est mobilisée en moyenne plus de 10 fois par an sur divers types d'événements depuis 2013 (attentats, catastrophes naturelles, accidents, etc.).

3.3.4 Mieux appréhender les phénomènes de masse

3.3.4.1 Projet Thésée

Pour faire face à la massification de la cybercriminalité, faciliter le dépôt de plainte et renforcer l'efficacité des investigations sur Internet, la SDLC a développé le projet THESEE (Traitement Harmonisé des Enquêtes et Signalements pour les e-escroqueries), destiné à permettre aux usagers de déposer une plainte en ligne sans avoir à se déplacer dans un commissariat ou une brigade de gendarmerie. Ces plaintes pour escroqueries commises sur Internet seront ensuite analysées par un service de police spécialisé, basé à Nanterre au sein même de l'OCLCTIC. La mise en place d'une plate-forme dédiée aux e-escroqueries permettra de centraliser le traitement du contentieux tout en s'intégrant dans la stratégie du ministère de l'Intérieur de modernisation et de dématérialisation des démarches.

Les travaux informatiques et les tests conduits sur les différents systèmes d'information nécessaires au dispositif devraient s'achever au premier semestre 2018. La CNIL examine actuellement ce projet dont la mise en place nécessitera un arrêté. L'objectif est d'ouvrir ce télé service dès la fin 2018, avec les premiers déploiements du futur logiciel de rédaction de procédure (LRP4).

3.3.4.1 Projet Perceval

Les usages frauduleux de cartes bancaires[92] lors de ventes à distance sur internet représentent :

- 245 M€ par an (pour des transactions en France concernant des cartes émises en France) ;
- 900 000 faits en 2014, 1,3 million de faits en 2015, 1,9 million de faits en 2016 ;
- 1,3 million de cartes bancaires mises en opposition en 2016.

Selon une étude de l'ONDRP, 37 % des foyers victimes réalisent une démarche policière, essentiellement sous une forme de renseignement judicaire ou de main courante. Le contentieux est ainsi peu connu des forces de l'ordre, éclaté territorialement et fait l'objet d'un classement sans suite quasi-systématique par les parquets.

Suite aux développements effectués par la Gendarmerie nationale, une plateforme internet permet depuis fin mai aux particuliers de signaler en ligne toute transaction par carte bancaire dont ils ne sont pas à l'origine (carte toujours en leur possession). Il s'agit d'un télé-service accessible exclusivement à travers le site internet service-public.fr.

(92) Chiffres de l'Observatoire de la Sécurité des Moyens de Paiement (OSMP) de la Banque de France

Grâce à la centralisation des signalements, la plateforme permet d'initier des enquêtes concernant des préjudices cumulés importants et ainsi repositionner activement les forces de l'ordre sur ces atteintes qui touchent tous les Français. La démarche est simple pour le citoyen et pourra servir de guide pour la demande de remboursement par la banque.

3.3.5 Aider à la remédiation

Plateforme d'assistance aux victimes de cybermalveillance

La stratégie nationale pour la sécurité du numérique présentée en octobre 2015 a annoncé la mise en place d'un dispositif national d'assistance aux victimes d'actes de cybermalveillance.

Le programme gouvernemental « cybermalveillance.gouv.fr » assume aujourd'hui un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française. Il accompagne les particuliers, les entreprises et les collectivités territoriales qui pensent être victimes d'un acte de cybermalveillance pour l'établissement d'un diagnostic précis de leur situation, la mise en relation avec les spécialistes et organismes compétents proches de chez eux et la mise à disposition d'outils et de publications dispensant de nombreux conseils pratiques.

Le dispositif national d'assistance, animé par le groupement d'intérêt public (GIP) Action contre la cybermalveillance (ACYMA) et porté par une démarche interministérielle associant l'ANSSI, les ministères de l'Intérieur, de l'Économie et des Finances, de la justice et le secrétariat d'État en charge du numérique, est accessible depuis octobre 2017 pour toutes les régions de France.

L'expérimentation du dispositif dans la région Hauts-de-France avait permis, entre mai et octobre 2017, plus de 700 mises en relation entre prestataires en cybersécurité et victimes. Fin mars 2018, le nombre de prestataires référencés s'est établi à 1500, permettant un maillage territorial complet pour l'ensemble des menaces recensées. Il y a eu au total près de 7 000 mises en relation victimes/prestataires depuis le lancement national.

En 2018, l'effort principal du GIP ACYMA portera sur la communication afin de faire connaitre le dispositif auprès des citoyens, des entreprises et des collectivités territoriales. L'objectif est d'augmenter la visibilité de la plateforme et son utilisation en terme de « parcours victimes », mais aussi d'impliquer un plus grand nombre de partenaires privés ou public dans la sensibilisation de tous ces publics. Un kit de sensibilisation est en cours de réalisation ; son objectif est d'adresser le particulier à travers le canal professionnel. Plus de 3 000 entités se sont préinscrites pour recevoir ce kit, qui sera disponible avant l'été 2018, représentant plus de 11 millions de collaborateurs potentiellement adressés.

Ce dispositif devra aussi permettre d'apporter des éléments d'information sur les incidents de sécurité informatiques rencontrés par les victimes. Les informations techniques et mode opératoires ainsi recueillis seront analysés au sein du futur observatoire du risque numérique, notamment pour informer et alerter les autorités et le public sur l'état de la menace. Les premiers mois ont d'ores et déjà permis l'identification comme phénomène de masse, des arnaques au faux support technique, relayé par les services judiciaires.

3.3.6 L'identité numérique

Le Premier Ministre a confié conjointement au Ministre de l'Intérieur et au Secrétaire d'État chargé du numérique le soin de proposer l'élaboration de solutions d'identité numérique effective pour la rentrée 2019. Aussi, une inspectrice générale de l'administration a été nommée début janvier 2018 comme directrice du programme interministériel pour la conception et la mise en œuvre du parcours d'identification numérique.

Le déploiement d'un tel parcours a pour objectif de permettre à chacun, qu'il s'agisse de citoyens, de résidents étrangers en France ou de personnes morales, de justifier de son identité, de façon sécurisée, ergonomique et accessible, aussi bien lors d'échanges de données ou de consentements liés à des démarches administratives, que pour des usages plus étendus telles que des transactions économiques.

Ce parcours d'identification numérique sécurisé pourra ainsi être ouvert à l'ensemble des acteurs publics ou privés qui souhaiteront en bénéficier, afin de simplifier et d'améliorer encore la sécurité de la vie numérique des usagers, en préservant leur identité et en contribuant à la lutte contre la fraude et l'usurpation d'identité. Il devra être fluide, simple d'utilisation et devra s'intégrer au sein du dispositif FranceConnect dans une logique d'interopérabilité.

Il comportera au moins deux niveaux de garantie, dont le niveau élevé, au sens du règlement « eIDAS » n° 910/2014 du Parlement européen et du Conseil en date du 23 juillet 2014, et ce avec toutes les garanties de protection des données personnelles pour la conformité avec le RGPD.

Afin de prioriser les enjeux et déterminer les étapes des travaux à venir pour mettre en place des solutions d'identité numérique, un « Programme interministériel « pour la conception et la mise en œuvre d'une identification numérique de niveaux faible et élevé », dit PReNIUM, a par ailleurs été mis en place.

S'inscrivant dans ce cadre, une demande d'information (DI) relative aux solutions innovantes d'identité numérique sécurisées[93] a été lancé. Elle s'adresse aux opérateurs compétents de l'Union Européenne. Les réponses sont attendues fin mars.

À ce jour, il convient de préciser que le cadre juridique de l'identité numérique en France est le suivant.

Sur le plan européen, le règlement n° 910/2014/UE du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur, dit règlement « eIDAS » et ses actes d'exécution établissent un socle commun pour les interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques. Il a pour ambition d'accroître la confiance dans les transactions électroniques au sein du marché intérieur.

Sur le plan national, l'article 86 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, complété par l'ordonnance n° 2017-1426 du 4 octobre 2017 relative à l'identification électronique et aux services de confiance pour les transactions électroniques, a créé en droit français la notion de « moyen d'identification électronique présumé fiable ». Cet article codifié à l'article L.102 du code des postes et des communications électroniques permet que la preuve de l'identité aux fins d'accéder à un service de communication au public en ligne puisse être apportée par un moyen d'identification électronique présumé fiable dès lors qu'il répond aux prescriptions du cahier des charges établi par l'autorité nationale en matière de sécurité des systèmes d'information (ANSSI).

(93) https ://www.marches-publics.gouv.fr/index.php?page=entreprise.EntrepriseDetailsConsultation&refConsultation=368025&orgAcronyme=g6l

Ce cahier des charges est fixé par décret pris après avis de la CNIL et du Conseil d'État, il est en cours d'élaboration par l'ANSSI en lien avec le ministère de l'Intérieur. Le moyen d'identification électronique présumé fiable devra correspondre a minima au niveau élevé prévu par le règlement « eIDAS ». La liste des titres d'identité à partir desquels pourra être émise une identité numérique présumée fiable sera précisée.

Pour compléter l'article L. 102 du code des postes et des communications électroniques précité, l'ordonnance n° 2017-1426 du 4 octobre 2017 crée une possibilité de certification, sur une base volontaire et au-delà du seul champ de l'accès aux télé-services de l'administration prévu par le règlement « eIDAS », des moyens d'identité électronique autres que « présumés fiables jusqu'à preuve du contraire ».

À quels défis faut-il se préparer

De l'ensemble des constats abordés précédemment, on peut tirer une liste de défis auxquels les États et notamment la France sont confrontés et doivent se préparer :

Des débats publics à venir

- **Le débat relatif au chiffrement des données reste complexe,** la protection des données à caractère personnel devant être garantie inconditionnellement et la lutte contre la criminalité devant s'adapter aux nouveaux usages pour protéger les français.
- **La lutte contre les contenus illicites** constitue un défi à plusieurs titres. Sur le plan de la lutte contre le terrorisme, il convient de poursuivre les efforts de retrait rapide et durable des contenus radicaux. La propagation sur les grandes plateformes numériques américaines de contenus relevant du discours de haine reste un défi. Par ailleurs, la viralité de l'information sur les réseaux sociaux pose question, tant en matière de désinformation que d'enfermement cognitif des usagers. Ces situations interrogent la société et peuvent rendre nécessaires des mécanismes de régulation spécifiques.
- **La gestion des crises non majeures d'origine cyber doit être mieux organisée.** La place des systèmes d'information dans le fonctionnement des institutions, de l'économie et de la société est désormais centrale.
- Une **gouvernance spécifique de l'éthique en intelligence artificielle (IA)** devrait être adoptée pour faire émerger des technologies conformes à nos valeurs et nos normes sociales[94]. Il existe des risques d'**utilisation à des fins malveillantes de l'IA**[95] par des cybercriminels. L'IA élargit les menaces existantes et en introduit de nouvelles : détournement de drones et véhicules autonomes, cyberattaque plus efficace, plus ciblée et plus difficile à attribuer ou encore usurpation sophistiquée de l'identité d'autrui en ligne…

La transformation numérique, vers l'homo digitalis

- **L'augmentation de la surface d'attaque** est soutenue par l'apparition permanente de nouvelles technologies et de nouveaux usages : **objets connectés,** domotique, smartphones accédant à des applications sensibles, informatique en nuage, nouveaux systèmes de paiements ou construction de villes intelligentes…
- **La protection des espaces intelligents** constitue un défi. Cela concerne particulièrement le ministère de l'Intérieur, compte tenu la **volumétrie et de la sensibilité de leurs données,** de la **dimension territoriale de cette thématique,** alors même que les collectivités territoriales sont encore peu nombreuses à être sensibilisées aux risques cyber, et enfin, en raison de **l'impact d'une attaque** cybernétique dirigé contre eux.
- **Les cryptomonnaies sont devenues un nouveau champ d'action pour les cybercriminels.** Le Bitcoin évolue sur un marché très concurrentiel, où d'autres cryptomonnaies affichent des caractéristiques très prometteuses pour les criminels, en particulier en matière d'**anonymisation**. Outre l'utilisation de Bitcards, ces derniers peuvent être intéressés par des usages sans encadrement réglementaire à ce stade, comme les **levées de fonds en cryptomonnaie** (ICO -Initial Coin Offering), qui comportent un risque de schémas du type « exit scam »[96]. Enfin, les **attaques des plateformes d'échanges,** les vols de portemonnaies électroniques et les botnets de minage sont forts lucratifs pour les cybercriminels.

---

(94) Rapport de Cédric Villani « Donner un sens à l'intelligence artificielle » - 29 mars 2018

(95) Rapport publié 20 février par trente universitaires (Yale, Stanford, Cambridge, Oxford…), et experts ONG : The Malicious Use of Artificial Intelligence : Forecasting, Prevention, and Mitigation, https ://arxiv.org/pdf/1802.07228

(96) L'auteur, après avoir collecté des fonds en cryptomonnaies sur la base d'un faux projet, décide de disparaître.

- **La maîtrise de la sécurisation de l'identité numérique des citoyens** dans leur relation avec l'administration ou les entreprises, est une préoccupation majeure, pour le développement des usages numériques, la protection des données et la confiance.
- L'importance de l'**échange d'information avec l'ensemble des acteurs concernés,** entreprises, associations et monde académique, détenteurs de l'information et partenaires dans le développement de solutions qui préservent la souveraineté des États.
- **L'accompagnement du développement de l'offre de cybersécurité,** y compris dans sa dimension assurancielle.

Des formes de criminalités actuelles

- L'enjeu de la gestion et de la protection de l'information reste particulièrement important ; les cas de **détournements de données** se multiplient au point que la France est un des pays les plus touché au monde par le vol des données à caractère personnel. Dans l'U.E., la mise en œuvre du RGPD devrait pousser les différents acteurs à y faire face.
- **La prolifération des outils offensifs cyber** a pris une ampleur inédite ces dernières années avec la diffusion, sur Internet, d'outils particulièrement avancés. Contrairement aux armes cinétiques, la nature immatérielle des logiciels, vulnérabilités et codes informatiques malveillants avancés facilite leur acquisition par des attaquants informatiques et leur dissémination. La conséquence directe de ce phénomène est de rendre des logiciels malveillants évolués toujours plus accessibles et d'augmenter la probabilité des attaques et la gravité de leur impact.
- **Les espaces cachés de l'Internet (les darknets) restent très utilisés par les criminels.** Cette tendance complexifie le travail des services d'enquête et confirme la nécessité d'une veille technologique permanente.
- Outre l'émergence de **nouvelles formes de criminalité organisée,** l'importance de la **dimension sérielle** de la cybercriminalité induit la nécessité de collecter et d'analyser une grande masse d'informations auprès des victimes et des partenaires.
- **L'augmentation des attaques dans la chaine logistique de logiciels légitimes** est inquiétante, comme l'illustre la crise virale NotPetya de juin 2017 avec le logiciel de comptabilité ukrainien *MeDoc,* ou l'attaque en septembre 2017 contre le logiciel *CCleaner*.
- L'émergence d'**attaques directes contre les réseaux bancaires et de paiement,** notamment pour prendre le contrôle de distributeurs automatiques ou pour transférer directement des fonds, apparait dans un contexte déjà sensible. Les virus bancaires persistent, les logiciels malveillants ciblant les points de vente poursuivent leur développement et le système de traitement des opérations bancaires internationales SWIFT subit régulièrement des attaques[97]. Il faudra veiller à ce que la confiance en ces systèmes ne soit pas entamée.

(97) Février 2018 : vol de 6 millions de dollars lors d'une attaque contre une banque russe au travers de SWIFT. Février 2016 : la Banque centrale du Bangladesh est victime d'un piratage informatique et se fait dérober 81 millions de dollars.

LEXIQUE

Terme/Acronyme	Définition
ANSSI	Agence nationale de la sécurité des systèmes d'information
APT	Advanced persistant threats - menaces persistantes avancées, auxquelles on pourra préférer la notion d'attaque en profondeur ou ciblée, souvent via des RAT
BEFTI	Brigade d'enquête sur les fraudes aux technologies de l'information (Préfecture de police de Paris)
C2MI	Centre de cyberdéfense du ministère de l'intérieur
C3N	Centre de lutte contre les criminalités numériques (PJGN)
CJUE	Cour de justice de l'Union européenne
CLUSIF	Club de la sécurité de l'information français
CNIL	Commission nationale informatique et libertés
Cryptlocker	Rançongiciel chiffrant : le logiciel malveillant chiffre les documents personnels de la victime et réclame le paiement d'une rançon pour obtenir la clé de déchiffrement
CyberGend	Réseau des enquêteurs spécialisés en technologies numériques (Gendarmerie)
DDoS	*distributed denial-of-service attacks* **:** attaques par déni de service distribuées
FOVI	escroquerie aux faux ordres de virement internationaux
EC3	European Cybercrime Centre (Europol)
GCP	Groupe de contact permanent (Etat - prestataires de l'Internet)
GIP ACYMA	Le groupement d'intérêt public (GIP) ACYMA anime le dispositif national d'assistance aux victimes d'actes de cybermalveillance (plateforme www.cybarmalveillance.gouv.fr)
ICC	Investigateurs en cybercriminalité (police)
IoT	Internet des objets - réseaux permettant de relier les objets connectés. Il s'agit parfois de connexions via Internet ou via des réseaux dédiés
IRCGN	Institut de recherche criminelle de la gendarmerie nationale
NATINF	code correspondant à la « nature d'infraction » dans la nomenclature du Ministère de la Justice.
NIS - directive	Network and Information Security - directive UE sur la sécurité des réseaux et des systèmes d'information
NTECH	Enquêteurs en technologies numériques (gendarmerie)
OCLCTIC	Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (DCPJ/SDLC)

OCRTIS	Office central pour la répression du trafic illicite des stupéfiants
ONDRP	Observatoire national de la délinquance et des réponses pénales
OSMP	Observatoire de la sécurité des moyens de paiement, de la Banque de France
PABX	Autocommutateur téléphonique privé
PHAROS	Plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (OCLCTIC)
Proxy	Un proxy est un programme servant d'intermédiaire pour accéder à un autre réseau. Par extension, il s'agit un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services.
PJGN	Pôle judiciaire de la gendarmerie nationale
Rançongiciel *Ransomware*	logiciel malveillant ou virus qui bloque l'accès au système ou aux données et réclame le paiement d'une rançon en échange du retour à l'état initial. Existe des versions avec chiffrement
RAT	*Remote administration trojan* : logiciel malveillant permettant un contrôle complet de la machine infectée (ou *remote administration tool* lorsqu'il s'agit uniquement d'un outil d'administration)
RGPD - *GDPR*	Nouveau règlement européen sur la protection des données. Entrera en application le 25/05/18
SCRC	Service central de renseignement criminel (PJGN)
SDLC	Sous-direction de lutte contre la cybercriminalité (DCPJ)
SISSE	Service de l'information stratégique et de la sécurité économiques
SSMSI	Service statistique ministériel de la sécurité intérieure
STAD	Systèmes de traitement automatisé de données
TOR	The onion router - système d'anonymisation sur Internet reposant sur une succession de rebonds via des serveurs (appelés nœuds) librement accessibles, combiné à un chiffrement de la communication
VPN	*virtual private network :* réseau privé virtuel. Une connexion inter-réseau permettant de relier deux réseaux locaux différents par un protocole de tunnel.

ÉQUIPE ÉDITORIALE

Le présent rapport a été établi grâce aux contributions de la Préfecture de police, de la Direction générale de la police nationale, de la Direction générale de la gendarmerie nationale, de la Direction générale de la sécurité intérieure, des services du Secrétariat général du ministère de l'Intérieur (SHFD/FSSI et Mission intelligence économique), de la Direction des libertés publiques et des affaires juridiques, de la Direction générale de la sécurité civile et de la gestion des crises, du Service statistique ministériel de la sécurité intérieure et de l'Observatoire national de la délinquance et des réponses pénales (INHESJ/ONDRP).

Sa rédaction a été réalisée sous la direction de M. Thierry Delville, commissaire général de la police nationale, Délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces, par le colonel Philippe Baudoin, le commissaire divisionnaire Adeline Champagnat, le commissaire divisionnaire François Thierry, et madame Alexandra Ketcheyan, attachée d'administration.

Pour toute question, contactez dmisc@interieur.gouv.fr
Ministère de l'Intérieur, DMISC, Place Beauvau, 75800 PARIS Cedex 08

CONCEPTION RÉALISATION

MI-SG/DICOM