Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE
L'INTÉRIEUR

ÉTAT DE LA MENACE LIÉE AU NUMÉRIQUE EN 2019

LA RÉPONSE DU MINISTÈRE DE L'INTÉRIEUR

MALWARE

ATTACK

INFECTED

SPAM

DARKNET

HACKER

INTRUDER

TROJAN

Rapport n° 3
Mai 2019

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

Sommaire

Le mot du ministre

Regardons le monde autour de nous : depuis nos communications jusqu'à nos moyens de transport, depuis nos achats jusqu'à nos relations personnelles, le numérique est présent partout.

Il a décuplé les opportunités, facilité les échanges. Il nous permet d'aller plus vite, de nous informer en temps réel, d'innover et de repousser les frontières de notre imagination.

Le numérique est présent dans le quotidien de notre ministère. Nos forces de l'ordre sont de plus en plus connectées, la procédure pénale se dématérialise et il est désormais possible de signaler des infractions en ligne. Ce sont autant d'avancées qui facilitent le travail de nos policiers et de nos gendarmes et offrent aux victimes une réaction et un accompagnement plus simple, plus accessible, plus rapide.

Le numérique est une chance et je souhaite que le ministère de l'Intérieur soit à l'avant-poste de la transition numérique de l'État. Mais notre volonté numérique assumée ne doit pas nous rendre naïfs.

Aujourd'hui, d'un clic, on peut voler, espionner, pirater nos systèmes d'information.

Aujourd'hui, des hackers avancent masqués, attaquent, et, en une seconde, peuvent changer un téléphone en micro, bloquer une gare, tenter de changer le cours d'une élection.

Aujourd'hui, Internet est devenu aussi la libre tribune de toutes les haines et, trop souvent, une école de radicalisation.

Comme ministre de l'Intérieur, mon devoir est de protéger les Français face à toutes les menaces. Aussi, avec nos services de police et de gendarmerie, nous sommes résolus à ne pas laisser le cyberespace devenir une zone de non-droit.

Notre feuille de route cyber est claire : les auteurs doivent être retrouvés, les délits empêchés et notre protection augmentée.

Nous nous sommes dotés de moyens importants, à la hauteur de nos ambitions. Ainsi, chaque jour, plus de 8 600 policiers et gendarmes veillent sur internet, traquent les délinquants, mènent l'enquête, en un mot protègent nos concitoyens. Ils luttent contre les escroqueries, surveillent les contenus illicites, empêchent les cyberdélinquants d'agir : ces femmes et ces hommes sont en première ligne pour notre sécurité et notre liberté numérique.

La liberté, justement, voilà tout le paradoxe d'internet. L'anonymat protège tous ceux qui répandent des contenus haineux et permet à des faux-comptes de se multiplier pour propager toutes sortes de contenus.

Nous ne pouvons pas laisser les publications illicites se multiplier. Nous devons donc relever le défi de l'identité numérique pour que chaque Français, dès 2020, puisse prouver son identité et savoir avec qui il correspond vraiment.

Mon objectif, avec Laurent Nuñez, est de bâtir une France sûre pour toutes et tous. Une France où les libertés sont garanties. Une France où le numérique reste une source d'opportunités et jamais un danger. Nous voulons bâtir la sécurité du XXIe siècle et celle-ci passe, résolument, par notre cybersécurité.

Christophe CASTANER
Ministre de l'Intérieur

Ce document est la troisième édition de l'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).

Qui ce document concerne-t-il ?

Tout le monde ! Les citoyens et l'État, les acteurs publics et privés, les usagers et les administrations, les particuliers et les entreprises… Ce document a été décliné en deux versions : l'une est publique, l'autre est classifiée.

De quoi parle-t-il ?

Ce rapport dresse, en premier lieu, un panorama complet des enjeux stratégiques liés aux cybermenaces – sociétaux, économiques, juridiques, technologiques et institutionnels. Il recense et explique ensuite les différentes menaces liées au numérique, puis rappelle les réponses apportées par le ministère de l'Intérieur. C'est un document de veille, d'analyse et de prospective.

Quelle période couvre-t-il ?

Le document couvre principalement la période 2018 – 2019. Des références aux années précédentes peuvent illustrer certains usages et phénomènes, afin de les contextualiser. Le rapport inclut quelques considérations d'ordre prospectif et identifie également les défis liés au numérique à venir.

Comment a-t-il été réalisé ?

Il s'agit d'un travail collectif, collaboratif, et il faut remercier ici l'ensemble des services contributeurs du ministère. Les forces de police, gendarmerie, renseignement et sécurité civile se sont particulièrement investies, tout comme les services du secrétariat général du ministère. Les acteurs de terrain ont été sollicités, ainsi que nos partenaires – le dispositif cybermalveillance.gouv.fr, le ministère de la Justice et l'Agence nationale de sécurité des systèmes d'information. Ce rapport n'aurait pas vu le jour sans l'investissement d'hommes et de femmes passionnés, mais aussi le travail quotidien de près de 9 000 personnels « cyber », répartis sur l'ensemble du territoire national.

Quelle est la volumétrie des menaces liées au numérique ?

La mesure de la cybercriminalité, malgré des progrès significatifs, constitue encore une voie de progrès pour le ministère de l'Intérieur. L'absence de dépôt de plainte ou de signalement est un véritable frein à la connaissance fine et précise des faits de cybercriminalité.

Quel est l'objectif de ce document ?

Vous informer, vous prévenir et vous sensibiliser en priorité, mais aussi vous expliquer les méthodes d'investigation numérique des forces de police et gendarmerie, ainsi que leurs travaux en matière de transformation numérique. Bienvenue au ministère de l'Intérieur 3.0 !

La délégation ministérielle aux industries
de sécurité et à la lutte contre les cybermenaces

Synthèse

Partie 1 - Enjeux stratégiques liés aux cybermenaces

L'accélération des transformations induites par le digital bouleverse profondément la société. Dans le même temps, l'irruption de l'Internet s'est accompagnée de la montée en puissance de géants du numérique transnationaux, dont les activités sont devenues systémiques. Aussi, poser des règles de fonctionnement claires et équilibrées pour accompagner la transformation numérique inéluctable de la société est essentiel. De même, l'adaptation des moyens de lutte doit être permanente pour faire face à l'évolution des cybermenaces, l'interconnexion des systèmes devenant la norme.

Enjeux économiques

Le paysage de la criminalité se transforme aussi sous l'impact du numérique. Internet offre de multiples possibilités pour atteindre un grand nombre de victimes à très faible coût et avec de nombreux avantages. Qu'il s'agisse d'opérations très ciblées ou d'actions massives et indiscriminées, ces activités constituent une menace insidieuse mais réelle pour toutes les entités économiques, qu'elles en soient directement la cible ou qu'elles en subissent les dommages collatéraux. Pour se protéger, elles disposent de trois outils principaux et complémentaires : la prévention, la gestion des risques et le transfert de risque par le biais de l'assurance cyber, qui poursuit son développement. Aucun secteur professionnel n'est à l'abri, y compris celui de la santé. Les conséquences négatives du numérique sur l'environnement sont de plus en plus évoquées.

Enjeux sociétaux

La mise en réseau numérique de la société fait émerger un spectre infini de propos d'une grande viralité, notamment porteurs de haine ou susceptibles de travestir la réalité.
Ainsi, le vecteur numérique est au cœur de la stratégie de communication djihadiste. Depuis fin 2017, la propagande de l'État islamique à destination de la mouvance islamiste occidentale a décliné mais ses adeptes sont toujours présents en ligne. Aussi la proposition de la Commission européenne portant sur le retrait, une heure après notification, des contenus terroristes en ligne constitue un enjeu prioritaire pour renforcer notre capacité collective à prévenir et lutter contre le risque terroriste endogène.
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, mais aussi du *carding* (vol et recel de données liées aux cartes bancaires).

Enjeux juridiques, normatifs et de coopération

La dimension internationale de la cybercriminalité implique aussi d'harmoniser les législations nationales et de faciliter la coopération entre les États.
Pour lutter efficacement contre les atteintes portées aux systèmes d'information notamment, le développement d'autres approches en matière d'investigations apparait nécessaire, comme celle de l'enquête sous pseudonyme dont le champ d'application est aujourd'hui élargi par la loi de programmation pour la Justice 2018-2022. Par ailleurs, la LPM 2019-2025 renforce le dispositif de cyberdéfense, notamment en dotant l'ANSSI de nouvelles capacités de détection.
La législation européenne se construit progressivement. Après le RGPD et la directive NIS, plusieurs propositions de règlement concernent ces domaines, notamment celui de l'accès transfrontalier à la preuve électronique pour les autorités pénales.
La coopération technique et opérationnelle se renforce, en particulier avec les pays sources de cybercriminalité, mais aussi au sein des instances comme le centre européen de lutte contre la cybercriminalité (EC3) d'Europol, d'Eurojust ou d'Interpol (IGCI).
Enfin, un arrêt de la Cour de justice de l'UE est venu bousculer les législations encadrant la conservation généralisée des données de connexion et de géolocalisation, fin 2016. Or, la conservation et l'accès aux données nécessaires aux enquêtes constituent un enjeu de premier plan. Les travaux entrepris n'ont, pour

l'heure, pas permis d'identifier de solutions répondant aux exigences de la jurisprudence et préservant les capacités opérationnelles des services de police.

Enjeux technologiques

L'utilisation accrue des outils de chiffrement et d'anonymisation sur Internet soulève des questions techniques, juridiques et opérationnelles dans la lutte contre la criminalité et le terrorisme ; elle rend l'accès à la preuve numérique plus complexe.
De même, l'utilisation de logiciels d'effacement de données, la démocratisation de supports numériques de type SSD ou encore l'emploi de certaines cryptomonnaies peuvent limiter sérieusement les capacités d'investigation.

Partie 2 - Usages et phénomènes

Évolution des usages

Le taux de pénétration de l'Internet continue de progresser en France (88 %) et dans le monde (55 %) ; 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.
La délinquance liée aux cryptoactifs se développe à mesure que le phénomène gagne en popularité : minage clandestin, attaques de plateforme d'échanges, levée de fonds ICO, utilisation de cartes *Bitcoin to Plastic,* escroqueries pyramidales basées sur les cryptoactifs…
Constituant un des symboles de la transformation numérique, l'Internet des Objets a investi de nombreux secteurs (domotique, loisir ou santé…) et permis l'émergence de systèmes complexes, tels que les systèmes de transports intelligents ou la *smart city*. Peu sécurisés, ces objets connectés augmentent considérablement la surface d'attaque pour les cybercriminels.
De nouvelles pratiques telles que les *fake news, hoax* et *swatting*, poursuivent leur développement sur Internet. Les forces de l'ordre intègrent ces éléments dans leur processus.

Phénomènes

Si l'année 2017 a été marquée par des campagnes de rançongiciels *(Wannacry, Notpetya)*, ces attaques n'ont pas poursuivi leur forte croissance, mais persistent en 2018 et touchent de nombreuses entreprises françaises. Toutefois un changement de stratégie des cybercriminels peut être observé. Autrefois indiscriminées, les attaques par rançongiciel semblent davantage cibler les grandes entreprises ayant la capacité de payer des rançons très élevées. La forte médiatisation de ce phénomène rançongiciel pourrait avoir incité les malfaiteurs à privilégier d'autres modes opératoires, plus difficiles à détecter. Ainsi le *spear-phishing* et le *cryptojacking* (minage clandestin de cryptomonnaie) sont en nette augmentation depuis début 2018.
En 2018, les *malwares* bancaires semblent en plein essor sur les *smartphones* et les attaques de distributeurs bancaires par *jackpotting* se sont intensifiées et diversifiées (mode d'accès), principalement commises par des criminels issus d'Europe de l'Est.
Tout un écosystème facilitant la mise en œuvre d'attaques cyber par des individus ou groupes criminels est désormais en place, induisant la notion de *« crime-as-a-service »*. *Malwares,* plateformes d'exploits, de service ou prestataires d'infrastructure se trouvent aisément, notamment sur les *darknets*.
Ces *darknets* demeurent des plateformes essentielles dans l'organisation de nombreux trafics et constituent l'interface de revente des données personnelles acquises à l'occasion de cyberattaques. La fermeture des grands marchés mondiaux *AlphaBay* et *Hansa Market*, à l'été 2017, a entraîné une augmentation du nombre de marchés secondaires plus spécifiques.
Les attaques par déni de service apparaissent en baisse avec un nombre de plaintes en diminution. Les faits de défiguration sont eux en forte réduction.

Les phénomènes criminels en lien avec le piratage des standards et lignes téléphoniques se poursuivent selon deux procédés, le *phreaking* et le *spoofing*.
Les contenus de provocation et d'apologie au terrorisme signalés à la plate-forme PHAROS ont connu une baisse significative pour la troisième année consécutive.

En matière d'escroquerie, l'année 2018 a vu à nouveau un net recul des escroqueries aux faux ordres de virement internationaux (FOVI). Elle a été marquée par la poursuite des escroqueries aux faux investissements sur le marché des changes (FOREX) et la recrudescence des escroqueries liées à des placements indexés sur les cryptomonnaies. Elle a aussi vu l'essor des escroqueries aux faux supports techniques et corrélativement l'arrestation de plusieurs bandes organisées.
Un phénomène de « sextorsion » portant sur un chantage à la webcam prétendument piratée est apparu fin 2018 ; il s'est manifesté par une diffusion massive de mails.
Les fraudes à la carte bancaire poursuivent leur évolution avec des outils de *skimming* de plus en plus sophistiqués, souvent déployés par des groupes criminels d'Europe de l'Est. Touchant désormais tout type de distributeurs automatiques, le nombre de piratages est toutefois en très forte baisse depuis 2015.

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

Concernant l'exploitation sexuelle des mineurs en ligne, il est noté la diversification de l'origine des images et vidéos à caractère pédopornographique mettant en scène des victimes de plus en plus jeunes, mais aussi la pérennisation des faits d'abus sexuels d'enfants commis à distance *(« live streaming »)*, impliquant des ressortissants français.

Données statistiques sur les infractions constatées

Entre 2016 et 2018, le nombre d'atteintes aux systèmes de traitement automatisé de données (STAD), enregistré par la police et la gendarmerie, est en baisse de 9 % (non interprétable en raison d'un faible taux de plaintes pour ce phénomène). Le nombre de harcèlements au moyen d'un service de communication en ligne a doublé entre 2016 et 2018. Enfin le nombre d'infractions à la loi « Informatique et Libertés », stable en 2016 et 2017, est en hausse en 2018 (+14 %), année de l'entrée en vigueur du RGPD.
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 7 % par rapport à 2017 ; plus de 73 % de ces infractions sont des escroqueries liées à Internet.

Perception de la menace et coût de la cybercriminalité

La majorité des entreprises est touchée par des cyberattaques ; près de 80 % en ont constaté au moins une en 2018.
L'évaluation du coût de la cybercriminalité reste encore un exercice complexe, bon nombre de victimes ne déposant pas plainte. Les attaques, dans plus 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 d'euros pour une entreprise de taille moyenne ; le préjudice moyen d'un détournement de données pour chaque entreprise victime est évalué à 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 cybermenaces (DMISC) joue un rôle de pilotage stratégique en matière de lutte contre les cybermenaces. La feuille de route demandée en 2018 par le ministre de l'Intérieur a abouti à un plan d'actions qui permettra de mieux structurer la lutte contre les cybermenaces.
Les directions et services jouent quotidiennement un rôle de prévention, protection, investigation et innovation.

Prévenir

Par sa présence dans les territoires, le ministère est un acteur majeur de la sensibilisation des citoyens, 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 2 000 000 d'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.
La protection des données est prise en compte au ministère par un réseau de correspondants, aujourd'hui animé par un délégué ministériel, nommé en 2018.

Enquêter

Au niveau de l'accueil dans les services locaux de police et de gendarmerie, la prise en compte des victimes passe par la capacité du dispositif à accueillir, écouter, analyser et orienter vers le service idoine.
Les services spécialisés dans la lutte contre la cybercriminalité développent leurs capacités tant en matière d'investigation que d'analyse numérique *(forensic)*. Le schéma général a conduit, dans ces deux domaines, à la mise en place d'un réseau territorial animé ou piloté par les services centraux.

Innover

Le partenariat Public-Privé se développe, en particulier avec les opérateurs de l'Internet grâce à plusieurs instances.
Le ministère s'engage également dans une démarche de recherche et de développement. Les échanges s'intensifient avec le monde académique dans le cadre de conventions ou avec le monde économique dans le cadre du conseil national de l'industrie (CNI) qui regroupe dix-huit filières françaises dont celle des industries de sécurité.
Par ailleurs, 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, à la brigade numérique de la Gendarmerie ou au portail de signalement en ligne des violences sexuelles et sexistes. Afin de mieux appréhender certains phénomènes de masse relevant de la cybercriminalité, la plateforme Perceval, inaugurée en juin 2018, permet à toute victime de signaler un usage frauduleux de sa carte bancaire. De même, le projet Thésée permettra prochainement de porter plainte en ligne pour certaines escroqueries sur Internet.
Enfin l'élaboration de solutions d'identité numérique permettra, à partir de 2020, la mise en œuvre d'un parcours d'identification numérique sécurisée pour les personnes physiques ou morales.

Partie I

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

Enjeux stratégiques liés aux cybermenaces

Au-delà de l'aspect purement cyber, la lutte contre les menaces liées au numérique représente des enjeux stratégiques majeurs pour le ministère de l'Intérieur.
Si les cybermenaces favorisent l'émergence ou le développement de nouveaux comportements délictueux, criminels ou même terroristes, elles revêtent également une dimension économique, à travers le développement du marché de la cybersécurité notamment. Ces évolutions sont étudiées attentivement par le ministère de l'Intérieur, qui veille à l'adaptation régulière des outils, normatifs et technologiques, dédiés à la lutte contre la cybercriminalité. Par ailleurs, de nombreuses cyberattaques étant planifiées et organisées depuis l'étranger, la coopération européenne et internationale est un outil précieux et nécessaire, de même que la coopération entre les ministères de l'Intérieur et de la Justice.
Ces considérations d'ordre sociétal, économique, juridique, technologique et institutionnel seront développées ci-après.

1.1. Enjeux sociétaux des cybermenaces

L'accélération des transformations induites par le digital bouleverse profondément la société. Algorithmes, *Big data,* réalité virtuelle, *machine learning,* robotique, intelligence artificielle (IA), objets connectés, ville intelligente, réseaux sociaux, les espaces et objets numériques sont désormais présents partout, cibles privilégiées des cyberattaquants. Dans le même temps, l'irruption de l'Internet s'est accompagnée de la montée en puissance de géants du numérique transnationaux.
Poser des règles de fonctionnement claires et équilibrées pour accompagner la transformation digitale inéluctable de la société est essentiel.
Un cadre de réflexion général de régulation des acteurs de l'internet mondiaux apparaît aussi indispensable, compte tenu de la taille et de la dimension systémique de leurs activités. La question de la suppression des contenus illicites, et notamment des contenus terroristes, est abordée par le projet de règlement européen relatif à la prévention de la diffusion en ligne de contenus présenté le 12 septembre 2018; la lutte contre les contenus de haine en ligne a fait l'objet d'un rapport remis au Premier ministre le 20 septembre 2018. Elle est également au cœur de l'initiative engagée avec Facebook par le Gouvernement, annoncée par le Président de la République au forum international de la gouvernance de l'Internet le 12 novembre 2018.
Sur les territoires numériques comme ailleurs, la responsabilité de l'État, et au premier chef du ministère de l'Intérieur, est de protéger les citoyens, d'anticiper les menaces, de mettre un terme aux actes délictueux et de présenter leurs auteurs à la Justice. Il est ainsi nécessaire d'adapter les réponses sécuritaires aux nouveaux usages numériques.
Enfin il est à noter un enjeu de féminisation des métiers liés au numérique.

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

La mouvance djihadiste internationale s'est adaptée aux évolutions technologiques des moyens de communication, en particulier avec Internet qu'elle utilise désormais comme une véritable plateforme opérationnelle. La propagande djihadiste s'est ainsi transformée et, depuis 2010, elle utilise le web 2.0, les applications mobiles et les réseaux sociaux. Les progrès réalisés sur les grandes plateformes et la stratégie d'adaptation des cyber djihadistes, qui utilisent désormais de façon préférentielle les réseaux chiffrés, ont provoqué un effet de migration sur les petites plateformes et sur les réseaux chiffrés (Telegram notamment). On constate sur ceux-ci un afflux de contenus terroristes.

L'État Islamique (EI) et Al Qaïda (AQ) sont à ce jour considérés comme étant les deux principales organisations terroristes se disputant l'hégémonie propagandiste sur Internet. Ils utilisent aujourd'hui les mêmes codes et protocoles de diffusion de propagande terroriste sur Internet.

Leurs objectifs peuvent être résumés sous 4 rubriques :

> une fonction de propagande idéologique et de recrutement ;

> une fonction de plateforme opérationnelle ;

> une fonction de financement ;

> une fonction de revendication.

Toutefois, dégradée, aussi bien en termes de qualité que de quantité, la propagande de l'EI à destination de la mouvance islamiste occidentale a décliné. En effet, l'organisation n'a pas diffusé de vidéos mettant en scène des djihadistes francophones depuis la zone syro-irakienne depuis le second semestre de l'année 2017, alors que cette pratique était courante auparavant.

L'EI est passé d'une entité territoriale à un réseau global. Si l'EI a perdu de nombreuses infrastructures et territoires entraînant une baisse de production de contenus de propagande terroriste, ses adeptes sont toujours présents en ligne. Ils sont appelés les « volontaires en ligne ».

Selon Europol, même si les sympathisants de l'EI ont exprimé leur volonté d'acheter des outils et des services aux fins de lancer des cyberattaques, leurs propres capacités offensives internes semblent limitées et non organisées. Les sympathisants de l'EI ont réussi un petit nombre de défacements et des piratages de faible niveau (tel que le piratage de la station de radio suédoise en novembre 2017 durant lequel un *Nasheed*[1] de recrutement pour l'EI a été diffusé). En mars 2018, l'EI a tenté de mettre à disposition de ses sympathisants un réseau social *« Muslim's Network »*, mais sans adhésion de leur part au dispositif, ce fut un échec. Enfin, le recours aux monnaies virtuelles pour financer des attaques terroristes reste marginal.

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

L'émergence d'Internet, puis le développement d'espaces de production de contenus textuels (blogs) et les réseaux sociaux ont considérablement modifié la façon dont les idées sont produites et la façon dont elles circulent et s'échangent. En élargissant la possibilité offerte à chacun de s'exprimer et de participer à de nombreux débats, la mise en réseau numérique de la société ne va cependant pas sans difficulté. En effet, la libération de la parole à une telle échelle se caractérise aussi par un spectre infini de propos d'une grande viralité, des plus haineux (haine en ligne, cyberharcèlement) aux plus sophistiqués (les manipulations informationnelles).

L'usage des technologies s'est démocratisé chez les plus jeunes, de plus en plus équipés de consoles de jeux, dont les ventes ont littéralement explosé en 2018. L'addiction aux jeux et plus généralement aux écrans est aujourd'hui identifiée comme une véritable pathologie, compte tenu de ses effets désocialisants et des conséquences sur la santé. Des propositions doivent être présentées courant 2019 dans le cadre des états généraux des nouvelles régulations numériques[2] (EGRN).

Les réseaux sociaux sont aussi utilisés de manière hybride, en particulier pour organiser des actions de voie publique. Depuis le 17 novembre 2018, Facebook et Twitter constituent des canaux de communication privilégiés pour des internautes aux profils variés (activistes, meneurs ou simples suiveurs) dans le cadre du mouvement des « gilets jaunes ». Ils ont été abondamment utilisés pour annoncer des rassemblements ou pour préciser les détails de rendez-vous et d'itinéraires.

---

(1) Les nachîds ou nasheeds sont des chants religieux musulmans.

(2) EGRN lancés le 26 juillet 2018 par le secrétaire d'État Mounir Mahjoubi. **www.egrn.fr/**

L'expérience opérationnelle montre enfin 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 individus ou ces groupes criminels 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 et chiffrés entre complices, anonymisation, caractère transfrontalier de la fraude, possibilités multiples de blanchiment d'argent provenant de leurs activités illicites.

Les groupes relevant de la criminalité 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 (telles que le *Bitcoin*) sur des marchés parallèles (notamment sur le *Darkweb*).

1.1.3 Un contexte favorable aux trafics illicites sur les *darknets*

D'après le constat de l'Office central pour la répression du trafic illicite des stupéfiants (OCRTIS) 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*[3] 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.

Le *darkweb* est de mieux en mieux connu par les services de l'État, à la suite de plusieurs opérations d'envergure. La chute des grandes places de marché « Alphabay » et « Hansa » à l'été 2017 a été suivie du démantèlement de la plateforme francophone « La Main Noire » en juin 2018. Ces actions ont permis de mieux identifier le spectre de la délinquance numérique sur le *darknet,* qui porte largement sur le trafic de biens illégaux. Pour lutter contre ces trafics massifs, les services d'enquête y maintiennent une veille opérationnelle active.

(3) 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…

Importance du trafic de stupéfiants

La criminalité sur le *darkweb,* polymorphe et diversifiée, est notamment constituée de trafics de stupéfiants et d'armes. Plus de 65 % [4] des annonces retrouvées sur « Alphabay », l'une des principales places de marché anglophone avant qu'elle ne soit fermée en juillet 2017 par le *Federal Bureau of Investigation* (FBI), concernaient la vente de stupéfiants ou de documentation connexe. Les activités liées à la délinquance économique et financière représentaient près de 25 % des annonces sur « Alphabay », avec notamment le vol et recel de données de cartes bancaires dit carding, le trafic de fausse monnaie et de faux documents. Celles liées au trafic d'armes s'élevaient à 5 %. La mise à disposition de logiciels malveillants, de guides méthodologiques ou encore de kits de piratages représentait moins de 2 % des offres. Enfin une activité liée à la pédopornographie[5] était alléguée par les médias.

Produits pharmaceutiques illicites ou détournés à d'autres fins

L'Office central de lutte contre les atteintes à l'environnement et à la santé publique (OCLAESP) réalise sur le *clearweb* et le *darkweb* des veilles relatives au détournement des produits pharmaceutiques. Son action s'inscrit dans le cadre national (veille proactive, signalements de la plateforme PHAROS[6]), européen (*« Task Force »* d'Europol) et international (alertes d'autorités étrangères).

D'innombrables pharmacies en ligne proposent des médicaments, souvent falsifiés, sans aucun contrôle ni prescription. En parallèle, sur les marchés du *darkweb,* les mises en vente concernent tant les produits commerciaux (falsifiés, contrefaits, volés) que les principes actifs, les conditionnements (permettant la revente de faux) ou les excipients.

De nombreuses substances détournées de leur usage initial (prise en charge de la dépendance et de l'addiction aux opiacés) sont également mises en vente, malgré leur dangerosité : la buprénorphine, la méthadone, le fentanyl, le tramadol, etc. En cas de mélange, les effets et les risques de surdose sont multipliés. Aussi, l'Office a informé et sensibilisé les forces de l'ordre, en première ligne sur le terrain.

Par ailleurs, il est constaté une hausse significative de la vente d'hormones de croissance, falsifiées ou non. Détournés à des fins dopantes, ces produits très onéreux sont prisés pour leur efficacité, suscitant l'intérêt des consommateurs et des fournisseurs.

Suite à des investigations sur Internet, une opération judiciaire d'envergure en région parisienne a conduit début 2018 à l'arrestation de cinq suspects de trafic international de stéroïdes anabolisants, la saisie de 20 000 fioles importées illégalement pour une valeur marchande de 400 000 €, ainsi que la confiscation d'avoirs criminels, dont une voiture de sport estimée à 85 000 €. À l'issue, trois des mis en cause ont été placés en détention provisoire et deux sous contrôle judiciaire.

(4) Les chiffres concernant les annonces sur Alphabay ont été établis à partir d'une consultation en date du 22/03/2017.

(5) Détention de l'image d'un mineur à caractère pornographique / diffusion de l'image d'un mineur à caractère pornographique via un réseau de télécommunications.

(6) La plateforme PHAROS permet de signaler en ligne les contenus et comportements illicites de l'internet par le portail ***https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action***

Opération internationale « PANGEA »

Il s'agit de la principale opération coordonnée au niveau international pour lutter contre les trafics en ligne de produits de santé illicites (contrefaits ou falsifiés). Initiée notamment par Interpol et l'Organisation Mondiale des Douanes (OMD), dans l'intérêt des patients et des consommateurs, elle se déroule simultanément dans une centaine de pays, dont la France, à travers l'action de l'OCLAESP.

Du 9 au 16 octobre 2018, cette opération coordonnée « PANGEA XI » a permis des résultats significatifs en France : plus de 466 000 produits de santé illicites et une tonne de produits en vrac saisis provenant majoritairement d'Asie, 116 sites internet illégaux de vente de faux médicaments identifiés et 6 procédures judiciaires ouvertes.

1.2 Enjeux économiques des cybermenaces

Les tentatives d'attaques à l'encontre des systèmes informatiques de l'État, des infrastructures critiques, des entreprises ou des citoyens sont quotidiennes. En effet, les attaquants informatiques conduisent aussi bien des opérations très ciblées que des actions massives et indiscriminées. L'ensemble de ces activités constitue une menace insidieuse mais réelle pour toutes les entités économiques, qu'elles en soient directement la cible ou qu'elles en subissent les dommages collatéraux.

C'est pourquoi, le législateur européen[7] est venu imposer le respect d'obligations de sécurité et de notification à des opérateurs économiques, au seul motif que leur défaillance puisse causer des perturbations importantes sur le tissu économique ou sociétal. Les autorités européennes ont pris pour modèle des réglementations déjà existantes dans le domaine de la défense nationale.

Il convient également de noter que, face à l'amélioration des mesures de cybersécurité prises par certaines entreprises, les attaquants ciblent aujourd'hui les prestataires, fournisseurs et consultants de ces sociétés, car ceux-ci sont souvent moins sensibilisés et dotés de moyens de protection de moindre efficacité.

Au-delà des effets strictement techniques sur un système d'information, une attaque informatique peut avoir des effets délétères sur la vie d'une entreprise. Elle peut engendrer des pertes commerciales ou des surcoûts massifs et induire un engagement de sa responsabilité en cas de défaillances de ses services vis-à-vis de ses clients. Elle peut également avoir des incidences réputationnelles.

Du point de vue étatique, il est essentiel de s'assurer que l'activité économique continue sans interruption et que les impacts globaux des cyber-menaces sur la société civile demeurent limités.

Ainsi pour se protéger, au-delà de l'adoption de mesures de sécurité, les acteurs économiques doivent être incités à mettre en place un double dispositif de prévention et de gestion du risque cyber. En effet, il est pertinent que les acteurs économiques mettent en œuvre :

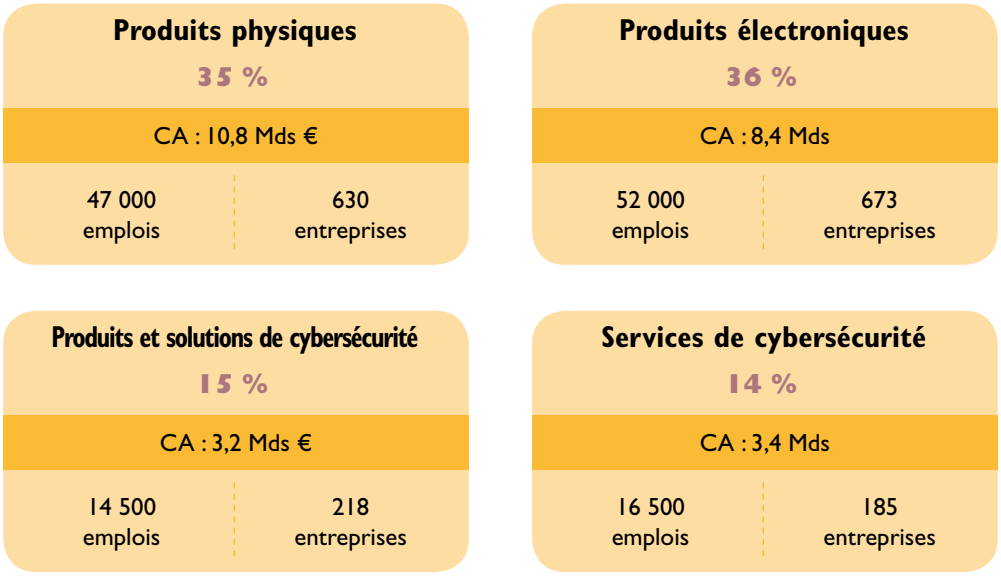
- un plan de prévention, qui se traduit prioritairement par la sensibilisation et la formation des personnels, qui restent le maillon faible de la cybersécurité, mais également par le test régulier des mécanismes de gestion de crise (par exemple ceux liés à la réponse à incident) ;
- une gestion des risques cyber qui permettra aux entités d'identifier leurs ressources critiques, de les protéger ou d'y suppléer en cas de crise.

Les risques résiduels (i.e. les risques identifiés et non assortis de mesures correctives) peuvent faire l'objet d'un transfert de risque par le biais de la souscription d'une assurance cyber.

(7) Cf. §1.3.2 : éléments sur la directive NIS (UE) 2016/1148 et son adaptation en droit français en 2018.

1.2.1 Le développement du marché de la cybersécurité

Répondant à un besoin fondamental des citoyens, la filière des industries de sécurité couvre les secteurs marchand (industriels, services) et public (forces de sécurité, douanes, justice pénale, etc.). Ce sujet est suivi de près par la Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC), qui accomplit, pour le cabinet du ministre de l'Intérieur, des travaux d'analyse stratégique, de veille et de prospective. La filière industrielle de sécurité[8], dont le chiffre d'affaires est évalué à 25 milliards d'euros en 2016 (hors sécurité privée), est organisée en trois segments : les produits physiques de sécurité (35 %), les produits électroniques (36 %) et enfin les produits et services de cybersécurité (29 %).



En marron : pondération dans la filière

Figure 1 : Segmentation du marché de la filière industrielle de sécurité (comprenant la cybersécurité)
Source : Étude Cabinet DECISION - 2017

Ces produits de cybersécurité sont eux-mêmes organisés en sous-segments : gouvernance, gestion des identités et des accès, sécurité des données, sécurité des applications, sécurité des infrastructures et sécurité des produits et services. Cet ensemble[9] représente environ 3,2 milliards d'euros de chiffre d'affaires, 218 entreprises et 14 500 emplois. Quant aux services de cybersécurité, ils représentent également une part conséquente du segment « cyber » : environ 185 entreprises, 3,4 milliards d'euros de chiffre d'affaires et 16 500 emplois. Par ailleurs, les prescriptions de l'État – les obligations des acteurs privés d'utiliser un équipement particulier – sont évaluées, pour l'ensemble de la filière, à 7,5 milliards d'euros ; la cybersécurité constitue un exemple concret, à travers la mise en place de certification des solutions utilisables par les entreprises sensibles, de type opérateurs d'infrastructure vitale (OIV) ou de services essentiels (OSE).

(8) *Données fournies par l'Observatoire de la filière des industries de sécurité (COFIS). Cf. § 3.3.2.2.*
(9) *Les chiffres indiqués dans le rapport 2018 provenaient de l'observatoire de la Confiance Numérique (ACN) qui couvrait un champ d'entreprises plus large.*

La cybersécurité représente un peu moins d'un tiers de l'activité de la filière mais se distingue par une croissance significative : 12 %, soit le double de la croissance annuelle moyenne du secteur marchand. Sa famille d'activité rassemble des entreprises plurielles. Elle se compose de prestataires de services (67 %), de producteurs (24 %) et de distributeurs (24 %), comme de grands groupes, de petites et moyennes entreprises (PME), d'entreprises de taille intermédiaire (ETI) et de start-up. Il convient de relever que l'industrie française compte en son sein des leaders mondiaux, notamment en matière de gestion des identités (Gemalto) et de conseil (Cap Gemini, Atos, Sopra Steria, Orange).

Le marché de la cybersécurité est en pleine expansion. Il est amené à croître davantage, à travers la mise en œuvre des cinq projets industriels structurants élaborés par les industriels et l'État pour la filière à l'horizon 2025 : la cybersécurité et la sécurité des objets connectés en premier lieu, mais aussi la sécurité des grands évènements et des jeux olympiques (JO) 2024, l'identité numérique, les territoires de confiance et le *Cloud* souverain. Ces travaux seront les premiers réalisés, en matière industrielle de sécurité, au sein du Conseil national de l'industrie (voir 3.4.2.2).

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, y compris maintenant sur le segment des PME[10].

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[11].

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 peine encore à être en mesure d'assurer ce type d'actifs de façon standardisée[12].

1.2.2 Contre-ingérence économique

Au-delà des enjeux liés à l'espionnage, au sabotage ou au terrorisme, une attaque informatique peut être une composante d'une attaque plus complexe ou de plus grande ampleur, comme une manœuvre de déstabilisation ou une tentative d'ingérence économique.

Ainsi, une exfiltration de données renseignera une entreprise sur l'état de santé d'un concurrent ou sur les vulnérabilités d'un cadre dirigeant, tandis qu'un déni de service empêchera l'entreprise de fournir un service en ligne en période d'affluence. L'attaquant ou son commanditaire pourra ainsi obtenir plus facilement une position déterminante pour mettre en œuvre son projet (acquisition, délivrance d'une sanction financière, abandon d'un marché, etc.). Il n'est en effet pas rare d'observer une concomitance entre une attaque informatique et des faits plus traditionnels (mouvement de personnel, participation à un marché gouvernemental, etc.).

(10) Les PME face aux enjeux de sécurité informatique, Etude IFOP du 5 au 9 novembre 2018 de nature quantitative auprès de 702 décideurs, réalisée pour Kaspersky et Euler Hermes : 43% déclarent avoir une assurance face au cyber.

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

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

Afin de limiter tout risque d'ingérence, une attention particulière doit donc être portée à la protection des systèmes d'information, lorsque l'entreprise affronte un moment clé de son fonctionnement (acquisition, négociations salariales, réalisation d'audits de conformité[13], bilan annuel, renégociation contractuelle, etc.). En outre, les entreprises doivent prendre conscience des risques d'ingérence économique lorsqu'elles pénètrent sur des marchés stratégiques pour d'autres entités.

1.2.3 « Production d'une pollution numérique »

Pollution numérique, pollution digitale, impact environnemental du numérique… les appellations sont nombreuses pour décrire une même réalité : les conséquences négatives du numérique sur l'environnement, à travers le fonctionnement du réseau Internet, ainsi que la fabrication et l'utilisation d'objets informatiques ou numériques.

Ainsi ce n'est pas seulement l'utilisation des équipements qui pollue, mais toutes les étapes du cycle de vie des objets numériques : l'extraction des minerais nécessaires, le transport des matériels, leur stockage et leur destruction ou absence de destruction (enfouissement, déchets sauvages). Selon les données du Centre national de la recherche scientifique (CNRS)[14], la consommation électrique des nouvelles technologies représente 6 à 10 % de la consommation mondiale et un mail de 1 Mégaoctet consomme autant qu'une ampoule de 60 watts allumée 25 minutes.

Si les technologies de l'information et de la communication étaient initialement perçues, à travers la dématérialisation, comme un progrès environnemental, la réalité est plus nuancée. En effet, le numérique et les menaces qui y sont liées contribuent largement à la pollution de l'environnement.

Par exemple, les pièces jointes de courriels[15], l'envoi massif de *spams,* les transactions liées aux cryptomonnaies, les échanges viraux sur les réseaux sociaux, les jeux vidéo multijoueurs en ligne ou la diffusion de données… génèrent une consommation d'énergie significative, ainsi que des émissions de dioxyde de carbone, ces phénomènes étant amplifiés par les usages illicites (ex.: mails de *phishing*). Les « fermes » de minage des cryptomonnaies ou les centres de données *(data centers)*[16] des opérateurs s'avèrent notamment très polluants.

Les menaces liées au numérique sont encore méconnues aujourd'hui des citoyens, des administrations et des entreprises, et leur coût environnemental encore moins, même si plusieurs administrations et entreprises se sont déjà engagées en faveur des énergies renouvelables, des moteurs de recherche alternatifs, du recyclage et des filtres de *spams*. Le sujet a par ailleurs été abordé à l'occasion d'un colloque « numérique » sur la ville intelligente[17] organisé en septembre 2018 par l'association des maires d'Ile-de-France (AMIF), auquel la DMISC a participé.

Les évolutions numériques à venir, comme le passage de la 4G à la 5G, ne manqueront pas de contribuer au développement des études relatives à la pollution digitale en général et à la prise de conscience des enjeux environnementaux liés aux cybermenaces en particulier.

---

(13) En particulier dans le cas d'une démarche de mise en conformité soutenue par des cabinets de conseil et des sociétés d'investigation numérique étrangers.

(14) ***https://lejournal.cnrs.fr/articles/numerique-le-grand-gachis-energetique***

(15) 10 milliards de mails transitent toutes les heures sur la Toile.

(16) Les besoins en électricité d'un data center sont énormes, classiquement autant qu'une ville de 30 000 habitants.

(17) ***https://www.amif.asso.fr/vie-de-l-association/colloques-debats/1085-colloque-numerique-penser-la-ville-intelligente2***

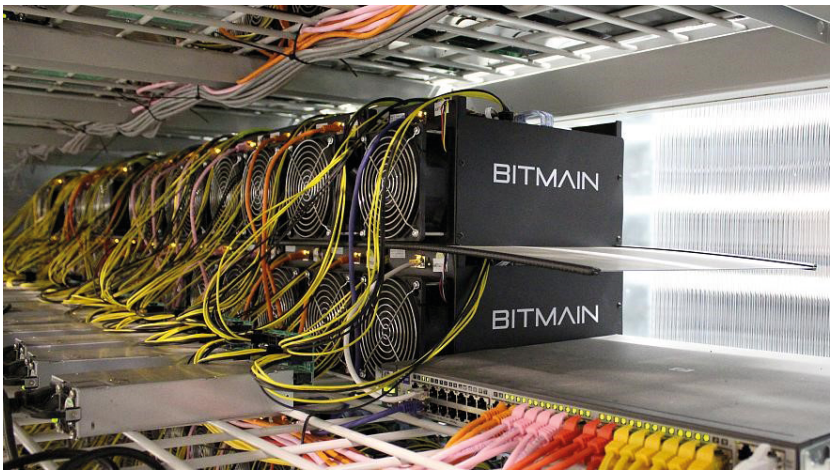


Figure 2 : Une « ferme de minage » de Bitcoins en Islande.
@ Copyright : REUTERS/Jemima Kelly

1.2.4 Fiscalité des entreprises du numérique

Revoir la fiscalité des entreprises du numérique pose de nombreuses questions comme le démontrent les discussions au sein de l'Union européenne (UE) ou de l'Organisation de coopération et de développement économique (OCDE). En l'absence d'accord européen fin 2018, la France a décidé de concrétiser sa proposition au niveau national d'instaurer une taxe de 3 % du chiffre d'affaires à compter du 1er janvier 2019 : Le ministre de l'Économie et des Finances a indiqué que certains revenus réalisés en France par ces entreprises seraient taxés (revenus publicitaires, vente de données…) et espère un vote à l'Assemblée nationale avant l'été.

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 préservant 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 des libertés publiques.

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 2018, le renforcement de l'arsenal juridique national en matière de cybercriminalité s'est poursuivi. Trois textes législatifs sont à signaler :

- Loi n° 2018-607 du 13 juillet 2018 relative à la **programmation militaire 2019-2025.** Cette loi contient des dispositions relatives à la cyberdéfense aux articles 34 à 37, qui ont vocation à renforcer notre dispositif de protection contre les cyber-attaques. En particulier, l'article 34 et son décret d'application renforcent les missions de l'Agence nationale de

sécurité des systèmes d'information (ANSSI), en améliorant ses capacités de détection des événements susceptibles d'affecter la sécurité des systèmes d'information de l'État, des autorités publiques et d'opérateurs publics et privés : mise en œuvre de dispositifs de détection (sondes) par les opérateurs de communications électroniques, possibilité pour l'ANSSI de demander des informations techniques dans certains cas et de mettre en place temporairement des sondes en cas de menace grave et imminente.

- Loi n° 2018-1202 et loi organique n° 2018-1201 du 22 décembre 2018 relatives à la **manipulation de l'information.**

  Ces lois visent à lutter contre la manipulation de l'information et à endiguer la diffusion de fausses informations pendant les périodes de campagne électorale. Elles créent notamment une nouvelle voie de référé civil visant à faire cesser la diffusion de fausses informations durant les trois mois précédant un scrutin national. Quand il est saisi, le juge des référés doit apprécier, sous 48 heures, si ces fausses informations sont diffusées « de manière artificielle ou automatisée » et « massive ».
  Dans sa décision du 20 décembre 2018, le Conseil constitutionnel a précisé que le juge ne pouvait faire cesser la diffusion d'une information que si le caractère inexact ou trompeur de l'information était manifeste et que le risque d'altération de la sincérité du scrutin était également manifeste.
  Les plateformes numériques sont soumises à des obligations de transparence lorsqu'elles diffusent des contenus contre rémunération. Celles qui dépassent un certain volume de connexions par jour doivent avoir un représentant légal en France et rendre publics leurs algorithmes.

- Loi n° 2018-493 du 20 juin 2018 relative à la **protection des données personnelles** a modifié la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés afin de l'adapter au Règlement général de protection des données (RGPD) et de transposer la directive 2016/680 (voir § 1.3.2 ci-après).
  La mise en conformité de la loi nationale à ces textes européens s'est poursuivie par l'adoption de l'ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de cette loi et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel. Cette ordonnance a pour principal objectif de simplifier la lecture de la loi du 6 janvier 1978 susmentionnée et d'en améliorer la cohérence. La nouvelle rédaction devrait entrer en vigueur au plus tard le 1er juin 2019.
  Cette mise en conformité du droit national avec le droit européen a principalement pour conséquence de renforcer les droits des personnes, ainsi que les obligations assignées aux responsables de traitement. Ceux-ci ont par exemple l'obligation de réaliser une analyse d'impact relative à la protection des données lorsqu'il existe un risque élevé pour les droits et libertés des personnes, ainsi que l'obligation de prendre les mesures de sécurité adéquates afin de protéger au mieux les données des personnes concernées.

Jurisprudence

À l'issue d'une procédure en référé initiée par le Parquet de Paris, le tribunal de grande instance (TGI) de Paris, dans une décision rendue le 27 novembre 2018, a ordonné à neuf fournisseurs d'accès à Internet (FAI) français de bloquer, sans limite de temps et dans un délai de 15 jours, l'accès depuis la France au site internet « Démocratie participative », connu pour ses propos racistes, antisémites et homophobes et dont les auteurs, éditeurs et hébergeurs n'avaient pas pu être attraits devant la justice française.

Perspectives

Il convient de noter qu'au niveau national, un plan 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. À 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. Prévu par ce plan, un **rapport** consacré au renforcement de la lutte contre le racisme et l'antisémitisme sur Internet a été remis le 20 septembre 2018 au Premier ministre. Établi par la députée Lætitia **Avia**, l'écrivain Karim Amellal et le vice-président du CRIF[18], Gil Taieb, il vise à répondre à la prolifération des contenus haineux sur Internet. Il présente, entre autres, les propositions suivantes : rendre plus claires et plus simples les procédures de signalement des contenus illicites ; fixer un délai maximal pour le retrait des contenus haineux ; et mettre en place des sanctions financières dissuasives pour les opérateurs qui ne s'acquittent pas de leurs obligations en matière de retrait des contenus haineux. Les propositions du rapport sont approfondies dans le cadre des **EGRN**. Le 20 mars 2019, plusieurs députés dont Lætitia Avia ont déposé à l'Assemblée nationale une proposition de loi visant à lutter contre la haine sur Internet. Celle-ci propose des modifications de la loi en vigueur (LCEN - Loi pour la confiance dans l'économie numérique).

Pour lutter efficacement contre les menaces actuelles ou émergentes, notamment contre les atteintes aux systèmes de traitement automatisé de données (systèmes d'information), il apparaît nécessaire de développer d'autres approches en matière d'investigations, notamment via le recours à la technique d'enquête sous pseudonyme[19]. En effet, son développement opérationnel constitue un enjeu majeur de l'efficacité de l'action des services judiciaires face aux évolutions des modes opératoires criminels sur les *darknets*.
La loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice contenait des dispositions relatives au recours aux interceptions par la voie des communications électroniques, à la géolocalisation, à l'enquête sous pseudonyme et aux techniques spéciales d'enquête. Dans sa décision n° 2019-778 DC du 21 mars 2019, le Conseil constitutionnel a néanmoins censuré les dispositions modifiant les conditions du recours, dans le cadre d'une enquête ou d'une information judiciaire, à des interceptions de correspondances émises par la voie de communications électroniques, ainsi que celles autorisant la généralisation du recours à des techniques spéciales d'enquête, dans le cadre d'une enquête de flagrance ou préliminaire, à tous types de crimes. Concernant les aspects « cyber » du texte, cette loi procède à l'harmonisation du régime de l'enquête sous pseudonyme[20] (nouvel article 230-46 du code de procédure pénale), consacre la plainte en ligne, fournit un cadre adapté aux plateformes Thésee et Perceval (cf. § 3.4.4) et donne une précision sur le régime de la captation judiciaire de données informatiques (périphériques audiovisuels).

(18) *Conseil représentatif des institutions juives de France.*
(19) *Pour certaines infractions limitativement énumérées par la loi (avant la loi du 23 mars 2019), l'enquête sous pseudonyme consiste pour des agents spécialement habilités à interagir avec les suspects par échanges électroniques, en utilisant un pseudonyme, afin de recueillir des éléments de preuve d'une infraction, et ce sans aucune provocation à la commettre.*
(20) *L'enquête sous pseudonyme est autorisée pour tous crimes et délits punis d'une peine d'emprisonnement et commis par un moyen de communication électronique. L'autorisation du procureur de la République ou du juge d'instruction est maintenant nécessaire pour acquérir tout contenu ou transmettre en réponse des contenus illicites..*

1.3.2 L'impact des directives, des règlements et de la jurisprudence européens 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. À ce titre, on peut citer :

- **Le règlement (UE) 2016/679**[21] 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**[22] 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 a été transposée au chapitre XIII de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

- **La directive (UE) 2016/1148**[23] 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, dont le titre I[er] porte diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité. Elle a été complétée par :

  > **le décret n° 2018-384 du 23 mai 2018** relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique ;

  > **l'arrêté du 13 juin 2018** fixant les modalités des déclarations prévues aux articles 8, 11 et 20 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique ;

  > **l'arrêté du 1[er] août 2018** relatif au coût d'un contrôle effectué par l'Agence nationale de la sécurité des systèmes d'information en application des articles 8 et 14 de la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité ;

  > **l'arrêté du 14 septembre 2018** fixant les règles de sécurité et les délais mentionnés à l'article 10 du décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.

- La directive (UE) 2018/1808 a révisé la **directive « Services de médias audiovisuels »** (SMA) 2010/13/UE[24] qui vise notamment à assurer la libre prestation de ces services au sein de l'Union. Si les fournisseurs de SMA étaient déjà tenus de ne pas diffuser de programmes incitant à la haine ou à la violence, le nouveau texte mentionne expressément l'interdiction des contenus constituant une provocation au terrorisme. Par ailleurs, **les fournisseurs**

(21) *http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679*
(22) *http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680*
(23) *http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148*
(24) *http://eur-lex.europa.eu/legal-content/FR/AUTO/?uri=CELEX:02010L0013-20100505&qid=1515675367632*

de plateformes de partage de vidéos sont désormais inclus dans le champ d'application et, à ce titre, ils devront mettre en place des mesures pour protéger le public à l'égard des contenus interdits (comme un dispositif de signalement par les utilisateurs).

- La décision-cadre 2008/913/JAI[25] 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 dans un délai de 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 et 72 % fin 2018).

- 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 le 17 avril 2018 à la publication par la Commission d'une **proposition de règlement, dite *« e-evidence »*,** dans le but de rendre plus facile et plus rapide pour les autorités policières et judiciaires l'accès transfrontalier à la preuve électronique[26] auprès des fournisseurs de services sur Internet[27] en créant des réquisitions spécifiques en la matière[28]. Parallèlement, une **proposition de directive *« e-evidence »*** établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale établit l'obligation pour tous les prestataires de services opérant dans l'Union européenne de désigner un représentant destinataire des injonctions visant à recueillir des preuves dans le cadre de procédures pénales. Ces deux textes sont en cours de discussion devant le Parlement européen.

- La **proposition de directive concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces** vise à adapter les règles européennes applicables en matière de lutte contre la fraude aux moyens de paiements autres que les espèces aux évolutions technologiques (monnaies virtuelles, paiements par mobile, utilisation de rançongiciels etc.). Elle a fait l'objet d'un accord entre le Parlement européen et le Conseil, et sera adoptée prochainement.

- La **directive 2017/541** du Parlement européen et du Conseil du 15 mars 2017 **relative à la lutte contre le terrorisme** prévoit que les États membres doivent prendre les mesures qui s'imposent pour faire supprimer rapidement les contenus en ligne de provocation publique à commettre une infraction terroriste, ou du moins d'en bloquer l'accès.

- Pour aller plus loin, la **proposition de règlement sur le retrait des contenus terroristes en ligne** prévoit que les hébergeurs de contenus offrant leurs services dans l'Union européenne (UE) devront supprimer les contenus terroristes dans le délai d'une heure à compter de la réception d'une injonction de retrait émise par une autorité nationale

(25) ***http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32008F0913***
(26) *Données stockées relatives aux abonnés, à l'accès, aux transactions et au contenu.*
(27) *FSI : hébergeurs de données, réseaux sociaux, fournisseurs d'accès à Internet, etc.*
(28) *L'« ordre européen de production », mécanisme par lequel les autorités d'émission d'un État-Membre seront habilitées à demander la production d'une preuve électronique à un opérateur fournissant des services sur le territoire de l'UE, sans considération du lieu de stockage de ces données ou du siège social de cet opérateur; et l'« ordre européen de préservation » par lequel les autorités d'émission pourront solliciter le gel de la preuve électronique.*

compétente. Le texte a fait l'objet d'une orientation générale au Conseil Justice et Affaires intérieures des 6 et 7 décembre 2018. Le Parlement européen n'a pas encore adopté de position.

- En avril 2018, la Commission a proposé l'élaboration d'un code de bonnes pratiques afin de lutter contre la désinformation en ligne en instaurant, entre autres, des mesures permettant de repérer et fermer les faux comptes sur les réseaux sociaux et en faisant appel à un réseau européen de vérificateurs de faits indépendants.

Jurisprudence

Par un arrêt du 21 décembre 2016[29] la Cour de Justice de l'Union européenne (CJUE) 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 des solutions aux difficultés opérationnelles et juridiques soulevées par cet arrêt. Un état des lieux a été dressé sur des dispositions censées garantir le renforcement des libertés fondamentales[30]. Aucune mesure n'a pu être identifiée pour le moment comme étant pleinement satisfaisante au regard des critères juridiques et opérationnels. Dans ce contexte, le 26 juillet 2018, le Conseil d'État français a mentionné toute l'utilité de la conservation des données, notamment au regard de la sécurité nationale[31].

Dans l'affaire C-207/16 *(Ministerio Fiscal)*, la CJUE a été interrogée sur la notion de « gravité suffisante de l'infraction » permettant de justifier la conservation des données. Elle a jugé le 2 octobre 2018 que l'article 15, paragraphe 1, de la directive vie privée et communications électroniques, lu à la lumière des articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, devait être interprété en ce sens que l'accès d'autorités publiques aux données visant à l'identification des titulaires des cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comporte une ingérence dans les droits fondamentaux de ces derniers, consacrés à ces articles de la charte des droits fondamentaux, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave. Ainsi, bien que ces accès constituent une ingérence, la Cour considère qu'ils sont licites pour des infractions d'une certaine gravité.

*(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***

(30) Limitation des catégories de données conservées, mandats renouvelables de conservation, limitation de la durée, conservation différenciée en fonction de la catégorie de données, stockage sur le sol de l'UE en mode crypté, accès différencié aux données et exemptions de catégories de personnes.

*(31) Requête au contentieux du Conseil d'État par la Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet : **https://www.legifrance.gouv.fr/affichJuriAdmin.do?oldAction=rechJuriAdmin&idTexte=CETATEXT000037253930&fastReqId=208251168&fastPos=1***

Trois questions préjudicielles relatives à la conservation des données de trafic et de localisation demeurent pendantes :

- 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.
- Dans les affaires jointes C-511/18 et C-512/18 (Quadrature du Net et autres), le Conseil d'État interroge la CJUE sur la conformité au droit européen des textes règlementaires applicables en matière de conservation des métadonnées et de conservation des données de connexion, que ce soit pour des fins judiciaires ou de renseignement[32], ces textes prévoyant une obligation de conservation généralisée et indifférenciée.
- Dans l'affaire C-520/18 (Ordre des barreaux francophone et germanophone), la législation belge est attaquée, notamment sur le fait qu'elle ne prévoit pas de dispositions spécifiques pour les personnes bénéficiant d'une protection de la confidentialité de leurs communications.

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. En octobre 2017, la Commission a présenté ses conclusions au conseil Justice-Affaires Intérieures (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, de mettre en place un réseau de points d'expertise et d'installer un observatoire du chiffrement. Ce réseau européen des experts en chiffrement s'est réuni pour la première fois le 7 décembre 2018 à Europol. Le 11 janvier 2019, Europol et Eurojust ont publié conjointement un premier rapport sur les usages du chiffrement.

Depuis l'entrée en vigueur le 25 mai 2018 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 remis en cause. 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. Consciente de son intérêt pour les forces de sécurité dans le cadre de leurs enquêtes, l'UE reconnaît 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

(32) *Plus précisément, il est demandé à la CJUE :*
- d'interpréter l'article 15, § 1, de la directive 2002/58/CE (e-privacy) comme autorisant les États membres à imposer aux fournisseurs une obligation de conservation généralisée et indifférenciée des données de connexion en vue de leur accès par, respectivement, les services de renseignement et l'autorité judiciaire ;
- de juger si les procédures de recueil des données de connexion peuvent être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours ;
- de juger si une réglementation nationale qui prévoit des mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, préalablement identifiés comme étant susceptibles d'être en lien avec une menace terroriste est autorisée par la directive 2002/58/CE, lue à la lumière de la Charte ;
- de juger si une législation, prévoyant une obligation des fournisseurs d'accès à Internet et hébergeurs de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu des services dont elles sont prestataires, afin de les rendre disponibles pour l'autorité judiciaire, est compatible avec les dispositions de la directive 2000/31/CE (e-commerce), lue à la lumière de la Charte.

conformant aux règles énoncées dans le RGPD visant à la protection des données personnelles. Des discussions ont été initiées entre l'UE et l'organisme en charge de la gestion de cette base de données dénommé *« Internet Corporation for Assigned Names and Numbers »* (ICANN). En juin 2018, l'ICANN a établi un nouvel *« expedited Policy Development Process »* (ePDP), en vertu duquel il devrait travailler sur un modèle d'accès standardisé à la base des noms de domaine, pour toute personne physique ou morale ayant un intérêt légitime.

Ainsi, au niveau européen, la législation se construit progressivement ; elle est loin de répondre efficacement aux enjeux actuels.

1.4 Enjeux technologiques de la lutte contre les cybermenaces

La lutte contre les cybermenaces s'inscrit dans un contexte d'usage de technologies d'anonymisation (par exemple le réseau TOR et les *Darknets*), d'innovations non encore réglementées (telles que les cryptomonnaies) et plus généralement de mutations technologiques profondes de notre société mondiale de l'information (développement du *Cloud* et du chiffrement), associées à un besoin croissant du respect de la vie privée et des données à caractère personnel[33].

Au-delà de l'adaptation nécessaire des techniques de recueil de la preuve pénale à ce nouveau contexte, ces évolutions technologiques obligent à repenser la manière de diligenter des enquêtes.

Le chiffrement par défaut des téléphones et des tablettes se généralise. De plus, ces matériels utilisent également régulièrement des messageries instantanées chiffrées (ex : Télégram, Viber, etc.).

La démocratisation des moyens d'anonymisation et de navigation Internet (privée) sans laisser de trace limite la découverte d'éléments de preuve. Les fournisseurs de VPN *(virtual private network)* mettent à disposition de nouvelles technologies qui permettent aux cybercriminels de masquer le trafic VPN et de rendre quasi-indétectable le transfert d'information sur le réseau.

Il a aussi été observé[34] que les nouveaux types de logiciels malveillants recourent de plus en plus à des nœuds du réseau TOR[35] pour consolider leurs infrastructures. Cette tendance crée de nouveaux obstacles pour la conduite des enquêtes judiciaires, de nombreux moyens d'investigation peuvent ainsi être mis en échec.

L'utilisation de logiciels d'effacement sécurisé de données performants rend également plus difficile le recueil de la preuve.

Parvenir à identifier et localiser les serveurs (souvent en-dehors du territoire national) utilisés par les cybercriminels reste difficile tout comme la récupération en clair de leur contenu. Cette récupération des serveurs proposant des services cybercriminels[36] offre le cas échéant la possibilité de disposer d'éléments d'identification des clients du service cybercriminel et des victimes ou cibles.

Enfin, la démocratisation des supports de type SSD[37], au détriment des disques durs classiques, limite les capacités d'investigations sur les données effacées. De plus en plus fréquemment les supports numériques de type SSD sont directement soudés à la carte mère, nécessitant une copie systématique de ce support aux fins d'analyses. De même, le stockage des données numériques sur des barrettes mémoire pourvues d'une connectique différente pour chaque modèle nécessite une gamme importante d'adaptateurs pour pouvoir effectuer les analyses techniques, les rendant plus coûteuses.

---

(33) Illustré notamment par l'arrêt CJUE Tele2 Sverige du 21 décembre 2016 sur la conservation des données.

(34) Source : division de l'anticipation et de l'analyse (D2A) de la SDLC - CSIRT-PJ

(35) Mettant à disposition différents contenus non indexés présents, le darkweb est accessible par le biais de réseaux d'anonymisation spécifiques. Le ***réseau TOR*** *est le plus connu et le plus utilisé d'entre eux.*

(36) Vente d'identifiant/mot de passe, site de « stresser » pour lancer des attaques Ddos, botnets…

(37) Solid State Drive.

Les réseaux sociaux (Facebook, Snapchat, Instagram) sont devenus de véritables « supermarchés » de la vente de produits frauduleux (voyages, séjours, numéros de carte bancaire, faux papiers…) favorisant l'anonymat. Les investigations y restent ardues.

Au niveau des flux financiers, un certain nombre de difficultés demeure, lié notamment à la facilité d'ouvrir un compte en ligne à l'étranger et à la pratique fréquente d'utilisation de comptes rebonds pour récupérer les fonds provenant d'une activité illicite sur le territoire national. En outre, il est possible d'acheter facilement des terminaux de paiement électroniques (TPE) mobiles (qui peuvent servir à récupérer les données bancaires).

Le traçage en temps réel des flux financiers reste très compliqué, le secret bancaire demeure une réalité. La coopération internationale bancaire et policière est en effet particulièrement réduite avec certains pays.

1.5 Enjeux de coopération européenne et internationale

L'expérience opérationnelle montre que de nombreuses cyberattaques sont planifiées et organisées depuis l'extérieur du territoire français. Il est donc nécessaire de disposer d'une collaboration européenne et internationale renforcée.

Cette coopération prend la forme de contacts bilatéraux, notamment avec les pays sources de cybercriminalité. Elle passe aussi par des échanges entre les services compétents des différents États au sein des instances européennes (le centre européen de lutte contre la cybercriminalité [EC3] d'Europol, et Eurojust) ou internationales (le *« Global Complex for Innovation »* d'Interpol - IGCI). Outre le partage d'informations sur les cyberattaques menées par des organisations criminelles, son objectif est aussi la définition d'approches et de solutions partagées, sinon communes, fixées dans des textes internationaux ou européens.

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

Le Conseil de l'Europe a poursuivi en 2018 ses travaux sur un projet de second protocole additionnel à la convention de Budapest sur la cybercriminalité. Le futur texte ambitionne de répondre au niveau mondial aux mêmes enjeux de l'accès à la preuve numérique dans le contexte de l'informatique en nuage. Il vise aussi à développer de nouveaux outils pour faciliter la coopération judiciaire internationale. Les travaux d'experts, auxquels participe l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), ont déjà permis de définir plusieurs propositions de mesures sur l'entraide pénale d'urgence, l'audition vidéo à distance et la simplification linguistique des demandes. Les travaux se poursuivent sur de futurs outils d'obtention des données auprès des opérateurs internationaux : injonction internationale de produire, modalités de coopération volontaire ou autre alternative. Le Conseil porte aussi un débat sur l'accès direct transfrontière à la preuve, les techniques spéciales d'investigation, les équipes communes d'enquêtes et les compétences de juridiction. L'adoption de ce futur protocole, attendue pour 2020, devra permettre aux acteurs de l'investigation de disposer d'une voie de coopération renforcée avec les 63 pays signataires de la convention de Budapest.

La France soutient activement l'extension de la convention de Budapest, qui garantit un équilibre entre, d'une part, la coopération judiciaire au service de la lutte contre la cybercriminalité et d'autre part, le respect des libertés fondamentales. Au niveau international, l'adoption de cette

convention fait toutefois débat. En 2018, certains pays entrainés par la Russie ont soutenu le projet d'une convention de lutte contre la cybercriminalité qui serait négociée entre l'intégralité des États membres de l'ONU. La conférence CPCJP de l'ONUDC[38] à Vienne, en mars 2019, a confirmé ce clivage sans parvenir à une décision sur l'ouverture de travaux en vue d'un texte onusien.

La mise en œuvre et l'extension de la convention de Budapest se font en complémentarité de l'engagement du G7 en faveur de la lutte contre la cybercriminalité et le terrorisme. Le G7 a réuni en 2018 son groupe dédié, le HTCSG *(High Tech Crime Subgroup)*, qui œuvre au développement de son propre réseau de points de contact 24/7 (complémentaire à celui de la convention de Budapest) et au renforcement de dispositifs (cybersécurité aérienne…). Il soutient les intérêts des services de police dans les grands enjeux internationaux : l'accès à la base WHOIS de l'ICANN, la réflexion sur le chiffrement, le soutien à la convention de Budapest… La dernière réunion du Groupe Lyon-Rome (GLR) des 6, 7 et 8 mars 2019 a poursuivi ces travaux.

1.5.2 Coopération opérationnelle et technique

Pour répondre aux défis posés par la lutte contre les cybermenaces, le ministère de l'Intérieur a défini depuis quelques années une stratégie globale qui, au plan international, vise à mettre en œuvre une coopération multidimensionnelle.

La direction de coopération internationale (DCI), en lien étroit avec les directions opérationnelles du ministère et s'appuyant sur un réseau de 74 services de sécurité intérieure permettant de couvrir 158 pays, développe une coopération technique et structurante. Elle permet de renforcer les liens opérationnels et le développement des moyens de lutte contre la cybercriminalité, notamment avec le continent africain : formation de personnels spécialisés, appui à la création de structures comme l'École Nationale à Vocation Régionale (ENVR) dans le domaine cyber au Sénégal, remontée d'information pour identifier de nouveaux usages et/ou des bonnes pratiques. L'approche structurante dans ce domaine de coopération très technique est aussi recherchée avec le déploiement depuis mars 2017 de postes d'expert technique international (ETI) spécialisé dans la thématique cyber, ayant notamment vocation à participer à la création ou au développement des services de lutte contre la cybercriminalité des pays dans lesquels ils sont implantés.
La DCI héberge aussi la « coordination nationale EMPACT[39] » des services français impliqués dans le cycle politique de l'Union européenne, au niveau de la plateforme multidisciplinaire de lutte contre les menaces criminelles (cf. infra).

Mise en place d'une unité de cyberpatrouille au sein de la division spéciale de cybersécurité de la police judiciaire de Dakar : avec l'aide de l'ETI en cybercriminalité et les formations dispensées, des policiers sénégalais ont pu mener pour la première fois en octobre 2018 des investigations d'initiative sur Internet.

Le critère de retour en sécurité intérieure conditionne en priorité l'implication des services du ministère dans ce type de coopération.

Dans ce contexte, l'OCLCTIC avec l'appui de la DCI a réalisé en 2018 plusieurs actions de formation technique visant à renforcer les capacités de services partenaires localisés dans les pays d'origine de groupes criminels impliqués dans les faits d'escroquerie en ligne : au Burkina

(38) Commission sur la Prévention du Crime et la Justice Pénale de l'Office des Nations unies contre la drogue et le crime.
(39) European multidisciplinary platform against criminal threats.

Faso, au Mali, en Mauritanie ou au Togo. Il a fourni son expertise au Conseil de l'Europe, dans le cadre de ses programmes de renforcement de compétences développés au bénéfice de pays candidats à la convention de Budapest, tout particulièrement l'Algérie, la Tunisie et le Maroc (programme « Cyber Sud » poursuivi en 2019). L'OCLCTIC et la DCI demeurent par ailleurs partenaires du programme GLACY + du Conseil de l'Europe qui porte également sur le renforcement de compétence des pays candidats à la Convention.

Au plan opérationnel, le point de contact 24/7 (issu du G7 et de la convention de Budapest) de l'OCLCTIC a géré :

> 2053 messages transmis par le réseau d'Interpol ;

> 849 messages transmis par le réseau d'Europol ;

> 246 demandes de gel de données (réseau G7/convention de Budapest) au bénéfice d'enquêteurs français ou réciproquement, à la demande de services étrangers.

Au niveau européen, le chef de l'OCLCTIC a assuré, en 2018, la présidence de l'EUCTF *(European cybercrime task force)*, qui réunit les chefs des services cyber des pays de l'UE.

L'unité cyber d'**Europol** (*European Cybercrime Centre* - EC3) constitue un dispositif de soutien aux services d'investigation des pays de l'UE. Au moyen des programmes **EMPACT** qui concernent notamment la lutte contre les cyberattaques, les fraudes aux moyens de paiement non liquides et les atteintes aux mineurs, l'agence promeut, de concert avec les polices européennes, des coopérations transverses, préalables à de nombreuses activités opérationnelles impliquant parfois des partenaires extérieurs à l'Europe. Ce cadre d'action concourt à un partage d'expertise, à la définition de nouveaux moyens, au développement de nouvelles coopérations et de partenariats avec le secteur privé.

Au sein des programmes EMPACT, la France est impliquée :

> dans le groupe de travail « lutte contre les cyberattaques », où la Sous-direction de lutte contre la cybercriminalité (SDLC) pilote une action visant à la mise en place d'un mécanisme de réponse coordonnée à incident en cas d'attaque cyber majeure et une autre visant à l'optimisation de la collaboration avec le secteur privé par le développement du modèle des CERT, et où la DMISC pilote une troisième action portant sur la création d'un réseau d'experts ayant pour objectif de former les enquêteurs aux outils de la gouvernance de l'Internet et d'influer sur les politiques, en représentant les intérêts des enquêteurs européens ;

> dans le groupe « fraude aux moyens de paiement », où l'OCLCTIC, au niveau national, a assuré la coordination de l'opération européenne coordonnée « e-Commerce Action » qui a impliqué 28 pays et permis l'arrestation de 95 suspects début juin 2018.

L'agence européenne se pose aussi comme un acteur précieux dans les réflexions internationales portant sur l'enjeu de l'investigation face aux évolutions de l'espace numérique. En 2018, elle a contribué à l'état des lieux des données utiles dans le débat sur la conservation des données. Elle demeure un contributeur global dans les réflexions sur la preuve numérique, le chiffrement, et toute problématique numérique qui concerne l'investigation. En dépit des limites de son mandat et des obstacles juridiques rencontrés, elle constituerait une option intéressante pour y développer une plateforme d'accès aux données WHOIS au bénéfice des enquêteurs de l'UE.

Focus sur l'action judiciaire transnationale

Créée le 1er septembre 2014, **la section F1 de lutte contre la cybercriminalité du parquet de Paris** est dotée d'une compétence concurrente[40] à celle qui résulte de l'application de l'article 43 du Code de procédure pénale, en matière d'atteintes aux systèmes de traitement automatisé de données (323-1 et suivants du Code pénal) et pour le sabotage informatique (411-9 du Code pénal) pour diriger les enquêtes judiciaires.
De manière très concrète, la section F1 du parquet de Paris est informée des procédures initiées de ces chefs et désigne les services qui diligentent les enquêtes sous son autorité. Lorsque certaines procédures sont initiées par d'autres Parquets, la section F1, en fonction de certains critères (faits déjà suivis ou d'une certaine complexité ou importance…) peut revendiquer et obtenir de l'ensemble des autres Parquets du territoire national qu'ils se dessaisissent à son profit.

À ce titre, la section F1 du parquet de Paris centralise des attaques cyber sérielles, telles que les rançongiciels et dirige des enquêtes portant sur des attaques contre des infrastructures sensibles. Elle dirige aussi les enquêtes relatives aux deux cyber-attaques mondiales ayant émaillé l'année 2017, Wannacry le 12 mai 2017 et NotPetya le 27 juin 2017. Cette dernière enquête est à ce jour la plus vaste enquête internationale jamais conduite, quelle que soit la matière.

Cette internationalisation du contentieux et des enquêtes a été couronnée de nombreux succès en termes de coopération internationale. Dans l'exemple du piratage informatique fin 2018 d'un prestataire privé détenant des plans d'établissement relevant de la sécurité nationale et rendus publics sur Internet, la section F1 a su mobiliser en quelques heures les autorités judiciaires allemandes pour aboutir à la saisie d'un serveur en Allemagne et ainsi obtenir le retrait de ces plans.

(40) Article 706-72-1 du Code de procédure pénale.

Partie II

Usages et phénomènes constatés

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 devient 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 juin 2018, le taux de pénétration de l'Internet(41) est de 55,1 % au niveau mondial, 85,2 % en Europe, 88 % en France. La croissance de l'Internet mobile(42) est la plus forte dans les régions en voie de développement ; fin 2018, le taux de pénétration de ces équipements y atteint 61 %.
Les sites Internet les plus visités en France(43) sont en décembre 2018 : Google, Facebook, Microsoft (même trio qu'en 2017), Groupe Figaro, Amazon, Groupe TF1, Altice (SFR-Numéricable), Webedia, puis Web66, Prisma Media, Wikimedia, Orange, et Vivendi.
L'usage des réseaux sociaux(44) est toujours en hausse, avec environ 3,3 milliards d'utilisateurs au niveau mondial selon les estimations, ainsi qu'un nombre d'utilisateurs réguliers en janvier 2019 de 2,27 milliards pour Facebook (+5 %), 1,9 milliards pour YouTube, 1,5 milliards pour WhatsApp (=), 1 milliard pour Instagram ou encore 326 millions pour Twitter. Le classement est évidemment variable dans les différents pays, avec de nombreux utilisateurs chinois pour Tencent QQ ou russes pour Vkontakte.

Le taux de pénétration des grands réseaux sociaux en France est de 59 % (nombre de comptes par rapport à la population(45)) et la durée moyenne d'utilisation quotidienne de 1,36 heure. En France, les réseaux sociaux les plus importants sont Facebook (40 millions d'utilisateurs par mois), YouTube (37), Twitter (20), Instagram (19), LinkedIn (16), Snapchat (13) et WhatsApp (13).

Les achats en ligne(46) continuent de se développer avec 78 % des habitants ayant réalisé un achat au cours du mois de janvier 2018 au Royaume-Uni, 74 % en Allemagne ou encore 61 % en France.

Depuis quelques années, on constate l'émergence du *smartphone* comme plateforme multi-usages. Le taux d'équipement en *smartphone* des Français a nettement progressé depuis 2011, pour atteindre 78 % en 2018 (en téléphonie mobile le taux s'est stabilisé à 94 %)(47).

Pour la septième année consécutive, les livraisons mondiales de PC reculent, même si les deux dernières années indiquent une certaine stabilisation autour de 259 millions d'unités. Cela montre que le marché du PC est depuis longtemps déjà un marché de renouvellement. Le cabinet Gartner ne prévoit toutefois pas la disparition de l'ordinateur fixe dans les foyers.
Après une décélération, le marché des *smartphones* est en baisse depuis deux ans. Les constructeurs s'efforcent d'accroître leur chiffre d'affaires par *smartphone* vendu, mais les consommateurs ne semblent pas tous prêts à investir de nouveau. Le marché français est proche de la saturation. Les primo-accédants se font plus rares. Le marché d'équipement est devenu un marché de renouvellement avec une utilisation des terminaux plus durable.

(41) **http://www.internetworldstats.com/**
(42) **https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf**
(43) **http://www.statista.com/statistics/473883/sites-internet-les-plus-visites-france/**
(44) **http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/**
(45) **https://www.blogdumoderateur.com/50-chiffres-medias-sociaux-2018/**
(46) *We Are Social Singapour :* **http://fr.slideshare.net/wearesocialsg/**
(47) *CREDOC – « Enquêtes sur les conditions de vie et les aspirations - 2018 » (population de 12 ans et plus).*

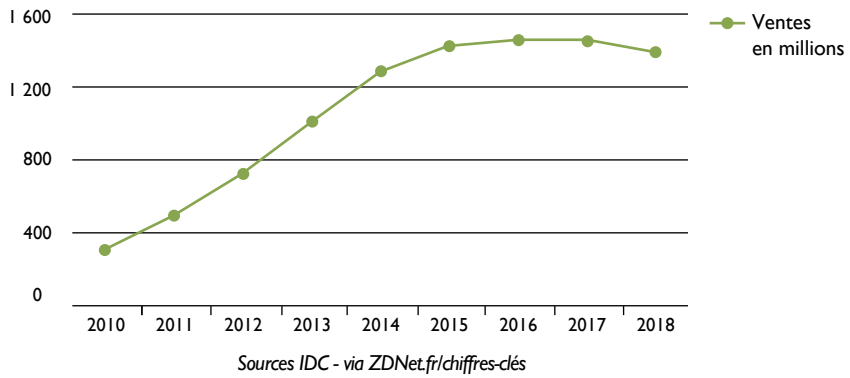


Figure 3 : Livraison mondiale de smartphones 2010-2018 (en millions d'unités)

2.1.2 Le développement des cryptomonnaies

Depuis le début des années 2010, les cryptomonnaies ont connu un développement exponentiel. On dénombre aujourd'hui près de 2 100 cryptomonnaies différentes, dont la principale est le *Bitcoin* (53 % en valeur), et plus de 150 fonds spéculatifs spécialisés dans cette industrie. Fréquent sur le Web, leur usage est prépondérant sur le *darkweb*.

Les cryptomonnaies sont un type de monnaie virtuelle à flux bidirectionnel[48] qui ont la particularité de sécuriser les transactions par le recours à des techniques de chiffrement, ces dernières étant consignées dans une chaine de blocs *(blockchain)*. L'ensemble est entièrement déconnecté des établissements financiers traditionnels, l'identification des porteurs de ces cryptoactifs détenus dans des portefeuilles électroniques est ainsi rendue plus difficile.

La délinquance liée aux cryptoactifs se développe à mesure que le phénomène gagne en popularité à la faveur d'un relatif anonymat et de leur cours qui prend des contours de bulle spéculative. La valeur exorbitante du *Bitcoin* et de ses concurrents a favorisé l'adaptation d'une délinquance traditionnelle, notamment avec l'apparition d'escroqueries pyramidales basées sur les cryptoactifs ainsi que l'essor de nouveaux modes opératoires délictueux.

Le **minage de cryptomonnaie** est le fait de fournir une prestation, généralement une sécurisation des transactions en cryptomonnaie en contribuant à leur vérification, en contrepartie d'une récompense pécuniaire dans cette cryptomonnaie. Cette action est légale sauf si la puissance de calcul du terminal informatique est utilisée de manière **clandestine** et non autorisée à cette fin. Concrètement cela arrive lorsqu'un terminal est infecté par un virus cryptomineur ou que le navigateur du terminal ouvre une page web infectée par ce type de logiciel malveillant. Ce phénomène, dénommé ***cryptojacking,*** est en forte augmentation depuis la fin de l'année 2017.

Depuis quelques années, des cartes bancaires adossées à des comptes en *Bitcoin* ***(Bitcoin to Plastic)*** permettent d'effectuer des achats en *Bitcoin,* de retirer des fonds en devises légales ou encore d'exécuter des transferts de cryptomonnaies en devises. Ces solutions connaissent un développement rapide, notamment en raison de leur flexibilité. En trois ans, le secteur s'est ouvert à une vingtaine d'acteurs, sensibilisés de manière très disparate aux procédures de

(48) Des échanges sont possibles avec des monnaies ayant cours légal.

connaissance client *(Know your customer*[49]*)*. En France, les dispositions du Code monétaire et financier (art. R.561-16-1) n'imposent un contrôle que sur des cartes permettant le stockage de monnaie électronique de plus de 250 euros pour un produit non rechargeable ou de 250 euros par mois pour un produit rechargeable. Il a été constaté que certains milieux criminels utilisent des cartes *Bitcoin to Plastic* en s'appuyant sur la possibilité de contourner ces seuils.

Un cadre réglementaire se met progressivement en place autour de l'écosystème des crypto monnaies et des nouvelles méthodes de levée de fonds utilisant les cryptomonnaies, telles que les ICO *(Initial coin offering)*. Une proposition d'amendement à la loi PACTE (Plan d'Action pour la Croissance et la Transformation des Entreprises) adoptée en seconde lecture à l'Assemblée nationale officialise la réflexion sur la « bancarisation » des acteurs dans le domaine des crypto monnaies. Acteurs et porteurs de projets devraient dès lors pouvoir, via l'Autorité des marchés financiers (AMF), obtenir un visa certifiant le respect des normes anti-blanchiment ainsi que l'origine des fonds en cryptomonnaies qu'ils manipulent.

2.1.3 L'Internet des objets (IoT)

En permettant la connexion d'objets du quotidien aux réseaux informatiques, l'Internet des Objets (IoT – *Internet of Things*) constitue un des symboles de la transformation numérique. L'IoT a notamment investi les secteurs de la domotique, du loisir ou de la santé. Dans ses aspects les plus aboutis, l'IoT a permis l'émergence de systèmes complexes pour fournir de nouveaux services, tels que les systèmes de transports intelligents ou la *smart city*.

2.1.3.1 Typologie des objets connectés

Le vocable IoT recouvre des objets différents : montres, véhicules, réfrigérateurs… Tous ces objets produisent et échangent des données au travers de différents réseaux de communication : le *Wifi* et le *Bluetooth* pour les plus connus, mais aussi Sigfox, Zigbee, LoRa et la 5 G dans un futur proche.

Trois critères permettent de mieux identifier les objets connectés.

En premier lieu, les objets connectés ont **différentes fonctions,** proposant des niveaux de sécurité disparates et offrant des surfaces d'attaque variables. Ils peuvent avoir un rôle de capteur (domotique, montres, lunettes, *pacemaker,* etc.), d'actionneur (serrures, pompe à insuline, *pacemaker,* etc.) ou d'interface de visualisation et d'exploitation des données collectées (*smartphones,* tablettes, etc.). Les capteurs et les actionneurs collectent des données ou déclenchent une action en réponse à des données collectées : ainsi, ils occupent une place moins critique en termes de sécurité dans les architectures IoT, mais représentent toutefois de potentielles failles. À l'inverse, les interfaces occupent une place centrale et les objets qui relèvent de cette catégorie apparaissent comme un point névralgique de l'architecture IoT.

(49) Les processus KYC sont utilisés par les entreprises afin de s'assurer de la conformité des clients face aux législations anti-corruption ainsi que pour prévenir l'usurpation d'identité, la fraude fiscale, et le blanchiment.

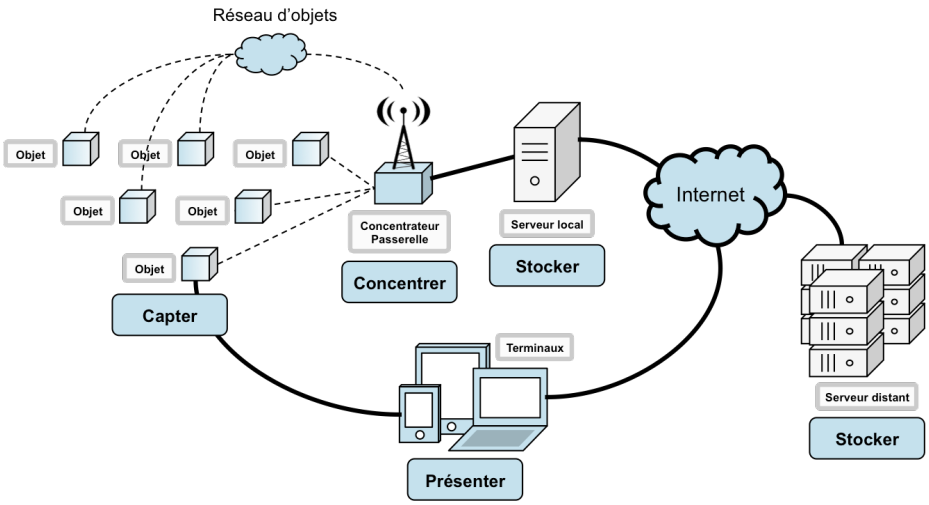


Figure 4 :Architecture IoT
Source **https://blog.octo.com/modeles-architectures-internet-des-objets/**

En second lieu, les objets connectés véhiculent **plusieurs types de données.** Ces données peuvent être à caractère personnel (signes vitaux, géolocalisation, fréquence d'utilisation d'objets pouvant toucher l'intimité de l'utilisateur, etc.), professionnel (données stratégiques) ou public et provenir de sources ouvertes (capteurs d'UV, de luminosité, de température, etc.).

En troisième lieu, les objets connectés ont **différents domaines d'application.** Les objets grand public couvrent la majeure partie des usages actuels et proposent notamment à l'utilisateur un meilleur confort de vie (domotique, montre, chaussure, robots, etc.), ou un meilleur suivi de sa santé (mesures du diabète, de la pression artérielle, du sommeil, de l'activité cérébrale, etc.). Les objets connectés concernent aussi l'industrie, qui les utilise pour améliorer ses process (suivi des stocks, gestion d'équipements) et commercialiser les objets grand public. Enfin, les équipements dits « de relais » (routeurs, passerelles, *gateway*), qui constituent l'infrastructure connectée nécessaire au fonctionnement de cet écosystème numérique, sont des éléments à prendre en considération.

2.1.3.2 Sécurité et traçabilité des objets connectés

La multiplication du nombre d'objets connectés constitue un facteur de vulnérabilité, ainsi qu'une nouvelle ressource pour les réseaux de robots *(botnets)*.

Le renforcement de la législation sur les *IoT* et une connaissance affinée de leurs caractéristiques techniques constituent un enjeu majeur de sécurité. Le Code des communications électroniques européen[50] s'applique aux transmissions entre objets connectés, de même que la directive sur la vie privée et les communications électroniques[51] quand le service est disponible pour le public. Les applications et services IoT sont couverts par le RGPD et la directive sur le commerce électronique[52].

(50) **https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32018L1972&from=FR**
(51) **https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32002L0058&from=FR**
(52) **https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32000L0031&from=FR**

La traçabilité des objets connectés et leur contextualisation constituent également un défi pour les forces de sécurité : elles conditionnent la réussite de leurs investigations. L'identification du support, des interactions dans son environnement et le travail sur la donnée sont trois étapes primordiales, mais complexifiées par la diversité des appareils, leur conception matérielle (composants, etc.) et leurs spécifications (nature des données captées, lieu de stockage, etc.). Pour faire face à ce nouveau défi, le ministère de l'Intérieur peut s'appuyer sur le plateau d'investigation des objets connectés, créé au sein du pôle judiciaire de la gendarmerie nationale (PJGN) : ce plateau est le point d'entrée de ces problématiques pour les enquêteurs. L'évolution du cadre juridique et l'établissement du principe de transparence des données techniques des IoT pourraient contribuer à la facilitation des investigations, à l'instar des dispositions en vigueur aux États-Unis[53].

2.1.3.3 Systèmes de transport intelligents

Véhicule connecté, véhicule autonome, véhicule étendu, véhicule intelligent… : tous ces termes rendent compte de la numérisation croissante du secteur de l'automobile, qui connaît une véritable révolution. Le véhicule « embarque » de plus en plus de composants électroniques et informatiques, tout en offrant de nombreuses portes d'entrée permettant une connexion depuis l'extérieur (prise OBD, USB, *Bluetooth,* GSM, etc.).

Il convient de distinguer les véhicules connectés et les véhicules autonomes. Les premiers, grâce à de multiples interfaces de communication, échangent des données entre eux (V2V), avec l'infrastructure (V2I), le *cloud* (V2C), ou encore avec les appareils numériques de l'utilisateur (V2D). S'agissant des seconds, tout ou partie des fonctions de conduite et de surveillance de l'environnement est automatisé et confié à la machine. Ces deux axes soulevant néanmoins les mêmes problèmes de cybersécurité, on parlera ainsi de véhicule autonome et connecté (VAC).

Les interfaces des VAC constituent autant de nouvelles surfaces d'attaques susceptibles d'être exploitées par la cybercriminalité : aucune cyberattaque réelle n'a pour l'instant été menée contre des véhicules. L'attaque la plus répandue consiste à exploiter les dispositifs électroniques d'un véhicule dans le but de le voler. À moyen terme, il est également envisageable que les attaques touchant les réseaux informatiques traditionnels (virus, rançongiciels, prise de contrôle à distance, attaques distribuées, etc.) concernent les véhicules et leur écosystème (infrastructure, gestion de flotte, distribution de l'énergie…). Quelques scénarios deviennent envisageables, comme le vol de données personnelles contenues dans le système d'info-divertissement, l'immobilisation d'une flotte de véhicules par un logiciel malveillant, assortie d'une demande de rançon au constructeur, la prise de contrôle à distance d'un véhicule autonome et son utilisation comme arme par destination, ou encore le leurrage des systèmes de contrôle en vue de provoquer un accident. Pour autant, la grande variété des modèles de véhicules, et parfois même les différences entre véhicules d'un même modèle fabriqués à des périodes différentes, rendent difficile la généralisation de ces attaques et limitent leur portée en nombre de véhicules affectés. Par contre, l'atteinte à l'image de marque d'un constructeur peut être considérable. Des attaques visant précisément cet objectif sont d'ailleurs plausibles, dans un contexte de concurrence exacerbée.

Ces nouvelles menaces sont aujourd'hui prises en compte par les autorités. Au ministère de l'Intérieur, l'Observatoire central des systèmes de transports intelligents (OCSTI), au sein du PJGN, a vocation à les évaluer. Le sujet a par ailleurs une dimension

(53) Les données des constructeurs et les résultats de tests en laboratoire permettant l'adjonction d'un numéro identifiant les appareils sont rendus publics sur le site internet de la United States Federal Communications Commission (FCC). ***https://www.fcc.gov/oet/ea/fccid***

interministérielle depuis qu'un arrêté de 2018[54], intégrant un volet de cybersécurité, dispose que les demandes d'autorisation d'expérimentation de véhicules autonomes sur la voie publique doivent être adressées conjointement aux ministères de l'Intérieur et de la Transition écologique et solidaire. Les établissements de recherche, à l'instar de l'IRT System X ou Télécom ParisTech (chaire *« Connected Cars and Cybersecurity »*), regroupent également des chercheurs et des acteurs industriels autour de cette thématique à laquelle l'ANSSI est associée. L'industrie automobile dans son ensemble a également pris conscience de l'enjeu que représente la cybersécurité à travers la normalisation[55]. Toutes ces initiatives constituent une première étape dans la prise en compte de la problématique de cybersécurité des véhicules.

2.1.3.4 Les drones

Désormais accessible à faibles coûts au grand public, l'usage des drones civils offre à la fois de nouvelles opportunités, mais aussi de nouvelles menaces. Leur usage peut être malveillant, ou l'usage habituel détourné. Les risques sont réels pour les personnes à l'instar de l'atteinte à la vie privée, mais aussi les installations. On peut citer le survol de complexes militaires ou d'infrastructures critiques, mais aussi des aéroports : en décembre 2018, victime d'un survol délibéré de deux drones empêchant tout trafic aérien, l'aéroport de Gatwick a dû fermer ses portes, perturbant ainsi les voyages de 140 000 passagers à la veille des fêtes de fin d'année et générant des pertes économiques significatives. Cet incident a conduit à l'interdiction, depuis mars 2019, du survol de drone dans une zone de 5 kilomètres autour des aéroports britanniques. Plus globalement, l'Agence européenne de la sécurité aérienne (AESA) a recensé un nombre croissant d'incidents entre des drones de loisir et des avions de ligne. Plusieurs usages hostiles notamment le vol en essaim peuvent également rendre aveugle un système aérien de défense en saturant le nombre de cibles à atteindre.

Face au risque croissant d'un usage malveillant ou détourné de drones, plusieurs réponses sont possibles. L'encadrement de l'usage des drones de loisir passe d'abord par des mesures d'accompagnement des consommateurs : la Direction générale de l'aviation civile (DGAC) a mis à leur disposition une carte interactive[56], ainsi qu'une notice d'avertissement rédigée conjointement avec la Commission nationale Informatique et Libertés - CNIL[57].

Cet encadrement se traduit également par des mesures contraignantes[58], compte tenu des risques que fait peser l'utilisation des drones – notamment ceux équipés de caméras, micros et autres capteurs – sur les droits et libertés fondamentaux, et le droit à la vie privée en particulier. Il existe des règles générales pour tous les drones de loisir, et des règles plus spécifiques pour les drones pilotés à distance grâce à la vidéo, ou pour les drones autonomes qui se pilotent tout seuls grâce à un logiciel d'intelligence artificielle ou un programme de vol préprogrammé. La réflexion menée par le Secrétariat général de la défense et de la sécurité nationale (SGDSN) a débouché sur la loi relative au renforcement de la sécurité de l'usage des drones civils[59], entrée en vigueur le 1er juillet

(54) *Arrêté du 17 avril 2018 relatif à l'expérimentation de véhicules à délégation de conduite sur les voies publiques :* ***https://www.legifrance.gouv.fr/eli/arrete/2018/4/17/TRER1717820A/jo/texte***

(55) *On peut citer la norme ISO/SAE 21434 « Road Vehicles – Cybersecurity Engineering », qui vise, à partir de 2020, la prise en compte de l'aspect cyber tout au long du cycle de vie du véhicule, dès sa phase de conception, ainsi que l'activité d'un groupe de travail dédié au sein du WP.29, organe de l'ONU chargé d'harmoniser les règlementations en matière de véhicules.*

(56) ***https://www.geoportail.gouv.fr/donnees/restrictions-pour drones-de-loisir***

(57) ***https://www.cnil.fr/fr/ou-piloter-son-drone-de-loisir-et-quelles-precautions-en-matiere-de-vie-privee***

(58) *Arrêtés du 17 décembre 2015 relatifs à l'utilisation de l'espace aérien par les aéronefs qui circulent sans personne à bord et à la conception des aéronefs civils qui circulent sans personne à bord, aux conditions de leur emploi et aux capacités requises des personnes qui les utilisent.*

(59) ***https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033293745&categorieLien=id***

2018. Au niveau européen, l'UE travaille depuis 2014 à l'élaboration d'une réglementation qui permettrait d'harmoniser les différentes législations des États sur le sujet. Au niveau international, l'Organisation de l'aviation civile internationale (OACI) a lancé en 2017 une consultation entre les différents États en vue de mettre en place un système de suivi mondial, qui permettra de connaître en temps réel la position et le propriétaire d'un drone, ainsi que son modèle, sa position exacte et son altitude. Les résultats de cette consultation ne sont pas connus à ce jour.

2.1.3.5 *Les smart and safe cities*

Le concept d'IoT est intimement lié à celui de *smart and safe cities:* la sécurisation des territoires intelligents. En effet, l'ensemble des capteurs et objets connectés contribue à la sécurité réelle et perçue des citoyens, ainsi qu'à la protection des personnes et des biens. Ainsi, les caméras, le *Cloud,* les drones, l'intelligence artificielle ou la géolocalisation constituent autant de nouveaux moyens de protéger les populations.

En 2017, plus de 2,3 milliards d'objets connectés étaient déjà déployés dans les *smart cities,* sur un total de 8,4 milliards d'objets connectés dans le monde, soit un marché de 1.700 milliards de dollars et un volume de 10^{22} octets de données. Des projections donnent plus de 50 milliards d'objets connectés en 2020.

Si les objets connectés participent à la sécurisation des territoires, ils sont également exposés aux menaces liées au numérique. Chaque objet connecté compterait entre 10 et 20 failles de sécurité. Or, les fabricants ne souhaitent ni densifier les lignes de codes, ni durcir la connectivité ou les accès au *cloud,* et ce en raison du coût.

Aussi, les objets connectés doivent être protégés, ainsi que les données personnelles et professionnelles qu'ils véhiculent. La *smart and safe city* doit, en premier lieu, faire l'objet d'une évaluation de ses vulnérabilités et de ses risques, en vue de garantir la continuité de ses services, voire la restauration de ses fonctions en cas d'attaque. En second lieu, elle doit recommander et imposer un niveau élevé d'exigence en matière de protection des réseaux et des technologies choisies. Ces dernières doivent préalablement avoir été inspectées et testées, et idéalement être assorties d'un chiffrement des communications utilisées entre les capteurs et les systèmes centraux ou périphériques.

2.2. Phénomènes constatés

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**[60] **ou un partage réseau ;**
- par **installation directe par l'utilisateur** (cas du téléchargement d'une application malveillante, installée volontairement, notamment sur les téléphones mobiles) ;

(60) Selon Kaspersky, les supports amovibles (clés USD, cartes SD…) représentent 30% des infections par des malwares en entreprise (livre blanc 2016 « sensibiliser vos collaborateurs à la sécurité informatique »).

> par **exploitation d'une vulnérabilité sur le système via une plateforme d'exploits** (ou *exploit kit*), vers laquelle 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.

2.2.1.1 Vulnérabilités

L'exploitation d'une vulnérabilité connue ou testée est un mode habituel de compromission des systèmes. L'utilisation de ce mode est facilitée par les plateformes Web qui référencent et répertorient les failles découvertes et les serveurs vulnérables. Ainsi le niveau de technicité requis pour effectuer une attaque apparaissant complexe n'est pas nécessairement élevé.

Sur une période donnée, l'évolution du nombre des vulnérabilités, dans les systèmes d'exploitation ou les logiciels, est toujours délicate à interpréter.

2.2.1.2 Ingénierie sociale

L'ingénierie sociale fait référence à des pratiques de manipulation psychologique à des fins illicites. 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…).

Cette technique est au cœur du procédé utilisé pour les fraudes aux faux ordres de virement internationaux (cf. 2.2.3.2), dites « au président » ou « au changement de coordonnées bancaires », dont sont victimes les entreprises.

La compromission d'un système d'information est fréquemment la conséquence d'attaques préalables ciblées hameçonnage *(spear phishing)* réalisées grâce à l'ingénierie sociale. Les environnements Microsoft professionnel (Microsoft 365) semblent particulièrement recherchés pour permettre l'accès aux messageries et documents grâce aux possibilités de modifier les droits d'accès et d'effectuer des recherches de documents ou mails précis. Ces environnements Microsoft ne sont en effet pas toujours complètement maîtrisés par les clients « entreprise ».
En 2018, il a pu être établi dans plusieurs dossiers que l'origine des compromissions, de l'utilisation d'une messagerie et de l'extraction de données étaient la conséquence d'un *spear phishing* réussi, lequel pouvait être bien antérieur à l'événement.

Typosquatting

Le *typosquatting* consiste à usurper le nom d'une marque ou d'une institution afin de se faire passer pour elle et d'escroquer les victimes, par une modification de manière parfois presque invisible, d'un caractère dans l'adresse du site internet de la marque (ou encore un changement de domaine de premier niveau [TLD] comme. org au lieu de. com). La fausse adresse renvoie vers une page Web qui copie la page d'accueil du site authentique pour tromper les victimes et les amener à communiquer des informations sensibles (mot de passe, coordonnées bancaires, etc.) utilisées ensuite par les escrocs au préjudice des victimes.

À la suite d'une surveillance proactive d'Internet concernant des noms de domaine susceptibles de présenter une ressemblance avec les sites institutionnels, le Centre de lutte contre les criminalités numériques (C3N) a découvert deux noms de domaine : gendarmerie-gouv.fr et gendarmerie-interieur-gouv.fr, qui peuvent être de nature à tromper les visiteurs du site ou les destinataires d'un mail provenant d'une adresse liée à ces noms de domaine.
Indépendamment du caractère non malveillant de la démarche détectée, l'exemple souligne l'**absence de contrôle a priori par les bureaux d'enregistrement et la permissivité de la censure édictée et/ou de son application par l'AFNIC**(61).

2.2.1.3 Les logiciels malveillants

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

- les **rançongiciels** (le virus bloque l'accès au système ou aux données et réclame le paiement d'une rançon) ;
- les **RAT**(62) *(remote administration trojan)* ou Troyen d'administration à distance ;
- les logiciels malveillants de minage de cryptomonnaie (***cryptojacking***) ;
- les ***botnets* de distribution de menaces** (diffusion ou installation d'autres virus) ou **ciblant les systèmes bancaires et de paiement** (ils visent l'utilisation de la banque en ligne, mais aussi les terminaux de points de vente ou encore les distributeurs de billets de banque).

La forte médiatisation en 2017 du **phénomène « rançongiciel »**, qui a suivi les attaques mondiales « Wannacry » et « Notpetya », pourrait avoir incité les malfaiteurs à privilégier d'autres modes opératoires comme le ***spear phishing***(63) et le ***cryptojacking***(64), plus difficiles à détecter et en nette augmentation depuis début 2018. Pour l'ensemble des services d'enquête français, ces menaces restent encore difficiles à traiter. 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*…) notamment grâce à une coopération internationale efficace.

En mai 2018, après 16 mois d'investigations, les enquêteurs de l'OCLCTIC interpellaient en Thaïlande, avec le soutien des forces de police locales, un Français qui avait créé le *malware* utilisé par un groupe organisé spécialisé dans l'attaque de systèmes de traitement automatisé de données à des fins d'extorsion. Le portail Internet d'une entreprise de service britannique avait été compromis pour permettre l'exfiltration de 1 400 comptes bancaires dont la restitution était monnayée par un individu s'exprimant en français. Cette affaire est particulièrement intéressante puisqu'elle a permis de démanteler l'intégralité de la chaîne criminelle, les codeurs de *malwares* n'étant que très rarement identifiés.

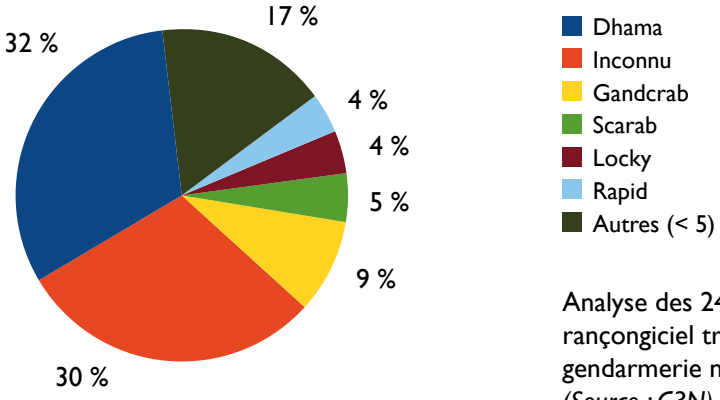
(61) Association française pour le nommage Internet en coopération.
(62) Forme de logiciel malveillant contenant un ensemble de modules permettant de parcourir les données sur le système de la victime ou encore d'y intercepter des frappes au clavier ou ce qui s'affiche à l'écran. C'est l'outil de prédilection des opérations d'attaque en profondeur.
(63) Le phishing (hameçonnage ou filoutage) est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but d'usurper l'identité d'une entreprise, d'un organisme financier ou d'une administration.
(64) Il s'agit d'un script qui s'exécute pendant qu'un utilisateur consulte une page web, tout en se servant du processeur de son ordinateur dans le but de générer de la cryptomonnaie.

Rançongiciels

L'année 2017 a été fortement marquée par des campagnes massives de rançongiciels de type *cryptlocker*[65] à l'échelle mondiale. Si elles n'ont pas poursuivi leur forte croissance, ces attaques persistent en 2018 avec un volume globalement constant de plaintes.

Ainsi 560 plaintes ont été enregistrées en 2018 par les services de police et de gendarmerie. Cependant, ce chiffre reste bien en deçà de la réalité des attaques. La majorité des entreprises victimes ne dépose pas plainte, ni même ne signale les faits aux forces de l'ordre, généralement pour préserver leur image.

Les rançongiciels étant en développement constant, le classement des principales souches évolue mensuellement[66] ; toutefois, pour l'année 2018, la souche « **Dharma** », déjà présente en 2017, demeure la plus identifiée, suivie des différentes versions de « **Gandcrab** ». Dans un bon nombre de cas, la victime a été dans l'incapacité d'identifier la souche l'ayant impactée. 5 % des victimes ayant déposé plainte auraient décidé malgré tout de payer une rançon, en moyenne 5 000 euros[67].



Analyse des 246 plaintes pour rançongiciel traitées par la gendarmerie nationale.
(Source : C3N)

Figure 5 : Occurrence des cryptolockers

Les campagnes impactent en premier lieu les entreprises et les sociétés et dans une moindre mesure les collectivités territoriales. En dépit des nombreuses enquêtes, la typologie des auteurs reste difficile à établir. Ils semblent toutefois disposer de « solutions prêtes à l'emploi », directement téléchargeables sur diverses plateformes de l'Internet, indexées ou provenant du *darknet*. Dans certains cas, l'étude des organisations et serveurs utilisés a permis d'établir des liens entre les équipes cybercriminelles agissant selon les modes opératoires des rançongiciels et des *malwares* bancaires.

(65) Le logiciel malveillant chiffre les données, en vue d'extorquer des sommes d'argent en cryptomonnaie.
(66) L'étude des plaintes sur la période 2016-2018 a abouti à une catégorisation des rançongiciels en plus de 40 familles.
(67) L'extrême fluctuation du cours d'échange du Bitcoin, principale monnaie virtuelle utilisée dans ce type d'attaque, conduit à nuancer ce chiffre en euros. La demande de rançon la plus élevée constatée est de 24 BTC. Cependant, la majorité des demandes de rançon oscille entre 0,5 BTC et 3 BTC.

Il peut également être noté un **changement de stratégie dans l'utilisation des rançongiciels par les cybercriminels.** Aux attaques massives avec des montants de rançon relativement faibles, apparaissent se substituer récemment des attaques par rançongiciel de plus en plus ciblées touchant de grandes entreprises. Celles-ci apparaissent discriminées pour leur chiffre d'affaires significatif et leur possibilité de payer des rançons très élevées (plusieurs centaines de milliers d'euros).

Il convient aussi de souligner que, depuis plusieurs mois, les hôpitaux sont victimes d'attaques par rançongiciels (ou autres virus).

Entre juillet et début septembre 2018, plusieurs vagues d'infection en France ont impacté le ministère de la Justice, des centres pénitentiaires et des établissements bancaires. La compromission des victimes s'est effectuée par un mail comportant un lien de redirection sur un site Internet également compromis sur lequel avait été déposée la charge virale. Le rançongiciel a été identifié comme étant dénommé ***PyLocky.*** Les auteurs des faits sont en cours d'identification par la brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI).

La BEFTI dispose désormais des éléments techniques permettant de créer un outil de déchiffrement pour les versions 1 et 2 de *Pylocky.* Depuis fin 2018, avec l'accord du Parquet de Paris et avec l'appui du dispositif national de lutte contre la Cybermalveillance (ACYMA – cf. infra § 3.4.5), le STSI²[68] a mis au point le déchiffreur. Cet outil est mis à la disposition du public librement et gratuitement, sur la plateforme cybermalveillance.gouv.fr. Sa disponibilité s'effectue au niveau international sur le site Internet « nomoreransom.org » (service édité en partenariat par Europol, la police néerlandaise et des entreprises de cybersécurité).
Il convient de noter qu'un outil de déchiffrement pour les dernières versions du rançongiciel *GandCrab* a été développé par la police roumaine, Europol et *Bitdefender;* il a été mis à disposition en début d'année sur le site « nomoreransom.org ». En mars 2019, la BEFTI, toujours dans le cadre d'Europol, a permis l'identification d'un nouveau serveur utilisé pour le rançongiciel *GandCrab.*

Malwares de type RAT

Le *malware* de type *Remote Access Tool* (RAT) est un programme installé sur l'ordinateur de la victime, soit à son insu suite à une attaque, soit directement par la victime qui est trompée, ce qui permet de prendre le contrôle de l'ordinateur à distance.

Les RAT permettent la plupart du temps d'accéder aux principales fonctionnalités de l'ordinateur infecté, telles que d'allumer la webcam, d'ajouter des contacts sur les messageries instantanées type SKYPE ou MSN, d'effectuer des captures d'écran de l'ordinateur infecté, de récupérer les mots de passe, notamment ceux enregistrés dans les navigateurs web, mais aussi ceux tapés par l'utilisateur, grâce aux fonctionnalités de *keylogger* (enregistreur de frappe clavier) ou de contrôler le système d'exploitation de manière générale…

Leur but est de passer inaperçus aux yeux de l'utilisateur afin de ne pas être détectés par les antivirus, pour voler les informations ou utiliser les ressources de l'ordinateur le plus longtemps possible. Ces *malwares* sont souvent utilisés pour créer des *botnets* (réseau d'ordinateurs infectés).

(68) Service des technologies et des systèmes d'information de la Sécurité intérieure, rattaché organiquement à la DGGN à Issy-les-Moulineaux.

Simples d'utilisation, ils ne nécessitent pas de connaissances pointues en informatique car ils sont mis à la disposition des utilisateurs « clé en main ».

Le C3N a initié en août 2017 une enquête sur un site Internet faisant la promotion d'un logiciel espion qui permettrait de découvrir l'orientation homosexuelle des enfants. Le mis en cause interpellé aurait gagné par la vente de ce logiciel plus de 31 000 euros. 15 000 euros ont été saisis sur son compte bancaire. Environ 400 personnes physiques et morales avaient alors souscrit la prestation illicite. Il a été requis contre l'auteur un an d'emprisonnement avec sursis et 30 000 euros d'amende. Le 4 février 2019, il a été condamné à 8 mois d'emprisonnement avec sursis.

Au cours d'opérations de recherche de compromissions, la division de l'anticipation et de l'analyse (D2A) de la SDLC a observé une difficulté de distinguer un rançongiciel de l'outil de prise en main à distance (RAT) dans les dossiers de cyberattaques prenant la forme d'un chiffrement de fichiers de données. Après analyse, il s'avère régulièrement que le logiciel malveillant pris pour un rançongiciel est en réalité un RAT dont les actions frauduleuses perdurent après le chiffrement de la machine infectée.

Phénomène de *cryptojacking*

La sécurisation des transactions en cryptomonnaie passe par des calculs mathématiques complexes qui nécessitent une puissance importante, et donc des ressources matérielles et énergétiques ; elle est récompensée par la génération de cryptomonnaies nouvelles. Depuis quelques temps, ce minage de cryptomonnaie n'est plus une activité rentable pour les particuliers et la concurrence est rude entre les « mineurs » ou coopératives de cryptomineurs, dont les revenus sont logiquement proportionnels à la puissance de calcul déployée.

Dans ce contexte, la nouvelle tendance en matière de logiciel malveillant est l'installation d'outils de minage de cryptomonnaies, à l'insu des propriétaires des ordinateurs. Ces *malware*s travaillent en tâche de fond, mettant à profit la puissance de calcul de tout un réseau de machines infectées pour générer du profit, le coût étant supporté par la victime. Ce phénomène est **en forte augmentation depuis la fin de l'année 2017.** Selon un rapport de *Cyber Threat Alliance* de septembre 2018, le nombre de sites Internet compromis par des cryptomineurs malveillants aurait augmenté de 450 % en 2018, l'essentiel des attaques se concentrant sur le minage de cryptomonnaie Monero (85 %).

Le C3N a été saisi suite à deux attaques informatiques sur un serveur permettant d'installer un logiciel de minage de cryptomonnaie Monero. Ce minage a été décelé par l'hébergeur technique, qui a constaté une charge anormale du processeur (CPU) de 100 % et a alerté l'administration d'État utilisatrice du serveur. L'enquête initiée fin 2017 a permis de confirmer que deux ***botnets*** (réseaux de PC contaminés) ont infecté plusieurs serveurs implantés sur le territoire national sans que les responsables de la sécurité des systèmes d'information (SSI) de ces entités ne les détectent. Les portefeuilles correspondant aux recettes des deux *botnets* et s'élevant à 58 moneros ont été saisis en mars 2018. Ils seront attribués au service enquêteur au titre de biens non réclamés.

L'INRIA[69] a déposé plainte auprès de la direction générale de la sécurité intérieure (DGSI) pour des faits constitutifs des infractions d'accès, maintien et introduction de données dans un système de traitement automatisé de données (STAD). Courant janvier 2018, l'INRIA a constaté une utilisation frauduleuse d'une plateforme technique permettant d'exploiter la puissance de calcul de plusieurs milliers d'ordinateurs, en donnant l'illusion d'un seul ordinateur virtuel puissant. Cette infrastructure permet de résoudre d'importants problèmes de calcul nécessitant des temps d'exécution très longs. Les ingénieurs de l'INRIA se sont aperçus qu'un processus inhabituel, nommé *« minergate-cli »*[70], tournait sur un des nœuds de la plateforme. L'enquête judiciaire a démontré qu'une personne avait usurpé des identités de chercheurs de la communauté scientifique pour obtenir des accès à cette plateforme. Cette personne utilisait alors la puissance de calcul de l'infrastructure pour miner une crypto monnaie nommée « XMR »[71].

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.).

Les attaques ciblant les systèmes bancaires et de paiement

Les virus ciblant les systèmes de paiement des points de vente se sont massivement développés il y a 5 ans, ciblant les pays où les pistes magnétiques sont encore utilisées, notamment les États-Unis. La France, où l'usage de la puce sur la carte bancaire est en place, a toutefois été touchée par ce phénomène ces dernières années.

Les malwares bancaires

Ciblant les comptes en ligne, le *malware* bancaire permet de voler les identifiants de connexion et d'injecter du contenu directement sur les sites web des banques ouverts sur des machines infectées. Après avoir ciblé les micro-ordinateurs, **les *malwares* bancaires sont en plein essor sur les mobiles.** L'étude publiée par Kaspersky[72] dresse un tableau inquiétant sur le nombre d'attaques de chevaux de Troie mobiles, redirigeant les utilisateurs vers des pages de *phishing* (hameçonnage). L'éditeur de logiciels de sécurité a enregistré 61 000 infections de ce type durant le second trimestre 2018, soit une augmentation d'environ 40 % par rapport au précédent record fin 2016. Les pirates

(69) L'Institut National de Recherche en Informatique et en Automatique est un institut national de recherche dédié au numérique employant 2400 collaborateurs issus des meilleures universités mondiales qui relèvent les défis des sciences informatiques et mathématiques. Il s'agit d'un établissement public à caractère scientifique et technologique placé sous la tutelle des ministères de la Recherche et de l'industrie.

(70) Minergate est un programme utilisé pour « miner » de la cryptomonnaie (Bitcoin, Ethereum, Monero…) et la particularité de ce logiciel réside dans sa simplicité, aucun paramètre n'est à définir.

(71) XMR correspond à la cryptomonnaie Monero.

*(72) **https://securelist.com/it-threat-evolution-q2-2018/87172/***

ciblent davantage les banques américaines, russes et polonaises. Seulement 0,1 % des attaques détectées au deuxième trimestre ont visé la France.

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

Le *jackpotting* 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 en 2015 en Europe, la France ayant été touchée en décembre 2016.

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 pour y connecter un ordinateur muni d'un logiciel adapté et déclencher le retrait de numéraires ;

> 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.

Cybercrime as a Service

Les ***malwares* clefs en main** ont toujours attiré les « pseudo-pirates » informatiques. Désormais, le modèle CaaS *(Cybercrime as a Service)* est un modèle de diffusion des outils malveillants qui se démocratise. Il suffit désormais de payer un « prestataire » pour qu'il active son réseau de machines infectées à votre profit.

En mars 2018, les enquêteurs de la DIPJ de Marseille interpellaient un primo-délinquant pour des faits d'accès frauduleux dans un système de traitement automatisé de données, d'escroquerie et de blanchiment, faisant suite au piratage d'un site Internet de vente de dissertations. L'intrusion, par l'utilisation d'une faille logicielle, permettait au malfaiteur de modifier les coordonnées bancaires de certains prestataires/rédacteurs dont les règlements étaient redirigés vers des comptes de complices. L'enquête démontrait la très forte implication de l'individu dans le piratage informatique, la récupération de milliers de numéros de cartes bancaires et de centaines de milliers de couples e-mail/mot de passe et l'espionnage de nombreuses personnes via leur webcam suite à la compromission de leur ordinateur au moyen du *malware « Darkomet ».*

2.2.2 Les attaques visant les systèmes d'information

Les attaques contre les systèmes d'information sont de plus en plus nombreuses et de même les fuites de données qui en sont parfois la conséquence.

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. Elles sont furtives pour pouvoir demeurer dans le système d'information de la victime le plus longtemps possible. Faisant l'objet de modes opératoires nécessitant des compétences diverses, elles sont constituées 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.

Le 20 février 2014, un groupe français spécialisé dans l'aéronautique déposait plainte après la découverte de compromissions informatiques détectées sur son infrastructure réseau. L'enquête judiciaire menée par la DGSI a permis de démontrer que des pirates informatiques avaient réussi à compromettre les identifiants et mots de passe du gestionnaire légitime des noms de domaine de ce groupe. Ces individus avaient ensuite créé plusieurs sous-domaines frauduleux leur permettant d'exfiltrer furtivement des données. Progressivement, l'enquête française, en étroite coopération avec le FBI, a mis en évidence plusieurs sources de compromission au sein de l'infrastructure informatique de ce groupe :

> l'infection d'un ordinateur portable par une clef USB lors d'un voyage en Chine ;
> des compromissions d'ordinateurs fixes utilisés par des employés de filiales de ce groupe ;
> l'utilisation d'un site Internet créé frauduleusement à partir d'un nom de domaine généré illégitimement comme point d'infection.

Les investigations menées par la DGSI ont mis en évidence que les pirates cherchaient à obtenir des informations sur la conception de la nouvelle génération de moteur développé par cette société ciblée.

Le 24 avril 2018, le parquet de Paris a enjoint la DGSI de lui transmettre l'ensemble des actes procéduraux et scellés réalisés et a procédé à une « dénonciation officielle » aux autorités américaines, correspondant à un transfert d'autorité judiciaire permettant d'engager des poursuites au bénéfice des intérêts français.

Le 23 janvier 2019, le groupe de conseil en technologie Altran était victime d'une attaque informatique de grande ampleur, obligeant la direction à procéder à la déconnexion de l'ensemble des serveurs hébergeant leurs applications ainsi que les réseaux internes (téléphonie, courriels…). Le groupe était la cible d'un rançongiciel chiffrant, *LockerGoga,* variante du *malware Ryuk,* auquel ses services informatiques et l'ANSSI tentaient de faire face. La remédiation s'avérait complexe. La section F1 du parquet de Paris a saisi conjointement l'OCLCTIC et la DGSI pour mener les investigations judiciaires.

Comme mode de compromission des systèmes, l'usage de couples d'identifiant/mot de passe récupérés ou achetés sur Internet (libre ou *darknet*) est fréquent. Ces *« credentials »* permettent au cybercriminel d'accéder directement à un serveur, une messagerie ou d'établir une connexion de bureau à distance (RDP), lequel pourra alors augmenter ses droits, déposer des *backdoors,* récupérer d'autres identifiants / mots de passe, se déplacer latéralement dans le système d'information ou effectuer des suppressions ou modifications sur les systèmes. Ce mode de compromission permet aux cybercriminels de mettre en échec les protections *anti-phishing* adoptées par les entreprises ou la vigilance des utilisateurs.

Courant 2016, l'éditeur d'un service de cartes de paiement sans ouverture de compte bancaire découvrait que plusieurs achats de *Bitcoins* avaient été réalisés aux moyens de comptes clients artificiellement crédités suite à une attaque de leur infrastructure informatique par injection SQL. L'entreprise victime déplorait 61 transactions frauduleuses, pour un préjudice de plus de 35 000 €. L'analyse des flux de *Bitcoins* a permis d'identifier le bénéficiaire de l'ensemble des transactions effectuées, utilisées pour partie aux fins d'acquisition de lingots d'or auprès d'une société située aux Pays-Bas et pour une autre partie pour se faire délivrer des cartes de paiement fonctionnant avec des comptes en *Bitcoins (BTC to plastic)* par une société sise à Gibraltar.

Les attaques contre les serveurs DNS[73] sont réputées en croissance, ce que confirme l'ICANN[74], dans son alerte de février 2019. L'ICANN met en garde contre des attaques de grande ampleur, ciblant les infrastructures des systèmes de noms de domaine (DNS). En effet, il a été observé un nombre croissant de rapports d'incidents concernant des changements non autorisés sur des adresses Internet ou des remplacements d'adresses serveurs légitimes par des adresses de machines contrôlées par des cyberattaquants. En France, très peu d'attaques de ce type font l'objet de plaintes auprès des services judiciaires.

Retour sur NotPetya

Le 27 juin 2017, la crise NotPetya touchait 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. Ces évènements, d'une ampleur majeure, ont provoqué la paralysie de nombreuses entreprises situées principalement en Ukraine et au sein de l'UE par effet de bord, occasionnant ainsi un préjudice financier colossal.

À cette occasion, la coopération internationale a pleinement joué et les canaux Europol et Interpol ont été des outils de communication et des facteurs d'efficacité majeurs. Saisi du dossier en France, le parquet de Paris (section F1) a rapidement sollicité le bureau français d'Eurojust. En charge de l'enquête, l'OCLCTIC a établi ainsi des échanges avec les enquêteurs des pays européens concernés. Cette affaire en cours est à ce jour la plus vaste enquête judiciaire internationale jamais conduite.

(73) Le DNS (Domain Name System) est un service permettant d'établir une correspondance entre un nom de domaine et une adresse IP.
(74) Société pour l'attribution des noms de domaine et des numéros sur Internet - autorité de régulation de droit californien.

2.2.2.2 Détournement et « vol » de données

L'année 2018 a été une année record de fuites de données. Le graphique ci-dessous présente les principales fuites de données ayant été révélées.

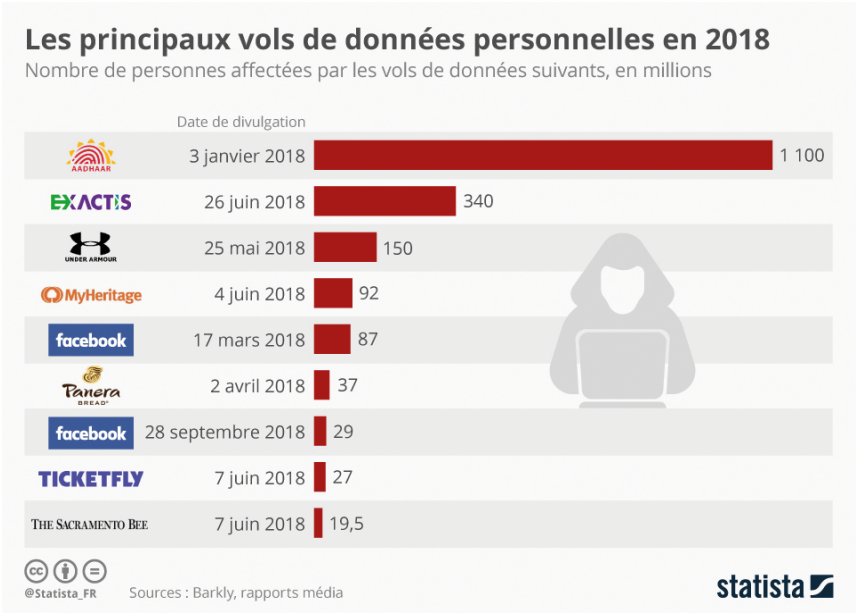


Figure 6

En janvier, des journalistes de *« The Tribune »* ont pu accéder à la base de données biométriques indiennes *Aadhaar,* mettant ainsi en évidence la compromission des données des 1,1 milliard de citoyens enregistrés dans le pays. Cela constitue à ce jour la plus grosse faille de données personnelles révélée de l'année 2018. Facebook apparaît deux fois : d'abord avec le scandale *Cambridge Analytica* en mars où 87 millions d'utilisateurs avaient été affectés par la fuite de leurs données ; puis fin septembre avec la compromission des données de 29 millions d'utilisateurs. Plus récemment en novembre, à la veille du *Black Friday,* Amazon a été victime d'une fuite de données liée à une erreur technique. De très nombreux clients de la plateforme d'achat en ligne ont reçu un mail leur indiquant que leur nom et adresse électronique avaient été divulgués par erreur.

Le vol de données personnelles dans les fichiers clients d'entreprise ou au sein d'administrations publiques (tel que le piratage du service Ariane pour les Français à l'étranger du MEAE[75] en 2018), continue d'être l'objectif régulier des intrusions dans les systèmes de traitement automatisé de données. Les données obtenues sont réutilisées pour des opérations d'escroquerie à la vente à distance, pour des *phishing* visant les clients identifiés ou encore pour l'exercice d'un chantage aux dépens de l'entreprise. Elles peuvent aussi être tout simplement revendues en vue d'être utilisées par d'autres délinquants dans le cadre du montage d'escroqueries financières plus classiques (crédit à la consommation…).

(75) Ministère de l'Europe et des Affaires étrangères.

En septembre 2018, la BEFTI a diligenté une enquête d'initiative sur la publication d'une annonce sur le site exploit.in, proposant à la vente un accès administrateur illégitime à un site web de presse français. L'entreprise éditant le site interne de cette société de presse était en situation de crise depuis deux jours ayant constaté la redirection de ses utilisateurs mobiles vers un nom de domaine quasi similaire, à une lettre près, et forgé selon la méthode du *typosquatting*.
Une fois sur ce site frauduleux l'internaute se voyait proposer une application Android correspondant à un *malware* bancaire de type *Anubis*.
L'échange d'information a permis aux équipes de sécurité d'identifier sur leur système d'information la présence d'un logiciel *webshell* d'accès avec privilège (programme qui, une fois installé, donne à celui qui l'utilise un accès direct aux données présentes sur le serveur) et ce depuis 2016.
L'exploitation des journaux d'activité a permis d'identifier l'extraction d'une base de données de 2 millions d'utilisateurs comportant nom, prénom, adresse électronique et parfois numéros de téléphone.

Arnaque sur WhatsApp
Vol de données personnelles

Début janvier 2019, des messages ont circulé sur l'application WhatsApp proposant des offres promotionnelles alléchantes concernant de nombreux parcs d'attractions : Futuroscope, Disneyland Paris, ou encore le Puy du Fou. L'usager devait partager le message avec 20 amis sur WhatsApp et pouvait ensuite accéder à une page où il devait rentrer ses coordonnées pour récupérer les fameuses places gratuites. Cette opération n'était qu'une arnaque destinée à récupérer des données personnelles.

Figure 7 : Tweet d'alerte plateforme cybermalveillance.gouv.fr en date du 13 février sur son compte twitter @cybervictimes

2.2.2.3 Les dénis de services

Le nombre de plaintes pour des faits de déni de service est en diminution, en partie en raison de la souscription par les entreprises de protection anti-DDoS en interne ou par le biais de prestataires.

Par ailleurs, un rapport de la firme de sécurité *Kaspersky* publié début février 2019 indique que les attaques par déni de service au quatrième trimestre 2018 sont en baisse de 13% par rapport à la même période de l'année précédente. Il précise également que les origines géographiques des attaques DDoS sont principalement sur la Chine, les États-Unis, et l'Australie.

Office des postes et Télécommunications de Polynésie française
Le 6 juin 2018, le parquet de Paris saisissait la DGSI d'une enquête relative à des attaques informatiques par déni de service affectant depuis le début de l'année le principal FAI polynésien, l'Office des Postes et Télécommunication (OPT) de Papeete[76].
Il s'agissait d'attaques par « réflection »[77] qui utilisait le réseau Internet fourni par une filiale de l'OPT, l'opérateur VINI. La fréquence de ces attaques ne cessait de croître et perturbait de plus en plus les accès Internet de toute la Polynésie française.
Un internaute, utilisant le pseudonyme « DK », revendiquait sur Internet et dans la presse locale être l'auteur des attaques. Il justifiait ces actes par les tarifs prohibitifs pratiqués par l'opérateur VINI. Pour cesser ces attaques, il demandait le versement d'une somme de 300 dollars en *Bitcoins*.
Les investigations menées par la DGSI sur les éléments techniques remis par l'OPT et à partir des constatations en sources ouvertes ont permis d'identifier « DK ».
Il a été interpellé le 3 juillet 2018 et a reconnu les faits, confirmant sa volonté de lutter contre le coût trop élevé des services Internet proposés par l'opérateur VINI et une qualité qu'il estimait ne pas être à la hauteur. Pour réaliser ses attaques, il expliquait avoir conçu un outil dédié aux attaques en déni de service accessible par un site à l'adresse www.hardstresser.com qu'il hébergeait chez l'opérateur OVH. Il faisait évoluer son outil pour améliorer constamment l'efficacité de ses attaques. Afin de payer l'hébergement de ce site, il proposait de louer du temps d'attaque au tarif de 60 $ pour 7 200 secondes.
Interpellé, le mis en cause a vu tout son matériel informatique saisi et placé sous scellé. Mineur, il a été déféré au parquet de Papeete et a été présenté devant un juge des enfants.

Déni de service téléphonique

Moins répandues, les attaques en déni de service TDos *(Telephonic Denial of Service)*[78] saturent les plateformes 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.

Les enquêtes ouvertes et clôturées par la BEFTI en 2017 et 2018 n'ont pas fait apparaître d'organisation structurée mais plutôt des adolescents se livrant de façon habituelle à des actions visant les services d'urgence pour réaliser des canulars ou des actions de *swatting* (cf. §2.2.2.5) sans volonté de blocage des lignes téléphoniques. Cependant par leur action répétée, les auteurs ne peuvent ignorer que monopoliser les postes téléphoniques constitue une entrave au système d'information, pénalement réprimée.

Les investigations numériques et téléphoniques ont permis d'identifier et d'interpeller deux individus auteurs qui sont à l'origine de plus de 8 000 appels à des services d'urgence en 2018. Ces auteurs mineurs sont en attente de jugement devant le Tribunal Correctionnel de Paris.

(76) Ces attaques informatiques ont eu un fort retentissement en Polynésie française. Le service Internet ayant été très perturbé par ces attaques, un climat anxiogène était en train de naître sur cet archipel peu habitué à ce type d'action.
(77) L'attaque par « réflection » est une technique consistant à usurper une adresse IP, puis interroger des serveurs de diffusion répartis dans le monde, sur lesquels existent des failles de sécurité. De fait, les serveurs répondent légitimement à cette IP, qui se trouve en l'espèce être une IP de l'OPT, occasionnant une saturation des connexions.
(78) Équivalent des attaques en déni de service distribué sur les serveurs informatiques (DDoS).

2.2.2.4 Les défigurations

Après avoir connu un pic en janvier 2015 après les attentats ciblant la France avec 140 procédures engagées, le nombre de plaintes pour des faits de défiguration[79] est en forte diminution.
Très peu de plaintes ont été déposées en 2018 auprès des services de police ; après six procédures en 2017, 4 ont été enregistrées auprès de la BEFTI à Paris ou auprès des services de gendarmerie.
Ces plaintes ne rendent pas compte de la totalité du phénomène.

En effet, en 2018, 412 cas de défigurations ont été recensés par l'ANSSI à partir de 276 tickets d'incidents enregistrés dans une base de son centre opérationnel SSI (contre 603 défigurations en 2017, soit -32 %). 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 : 84 (ministères, préfectures, académies, universités, lycées, hôpitaux, services d'urgence, établissements publics…) – *baisse de 31 % par rapport à 2017 ;*
- collectivités locales : 150 (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) – *baisse de 48 % par rapport à 2017 ;*
- opérateurs d'importance vitale (OIV) : 7 ;
- entreprises : 4 ;
- autres / Non catégorisés : 31 (associations d'intérêt public, pompiers, écoles non publiques, unions professionnelles).

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

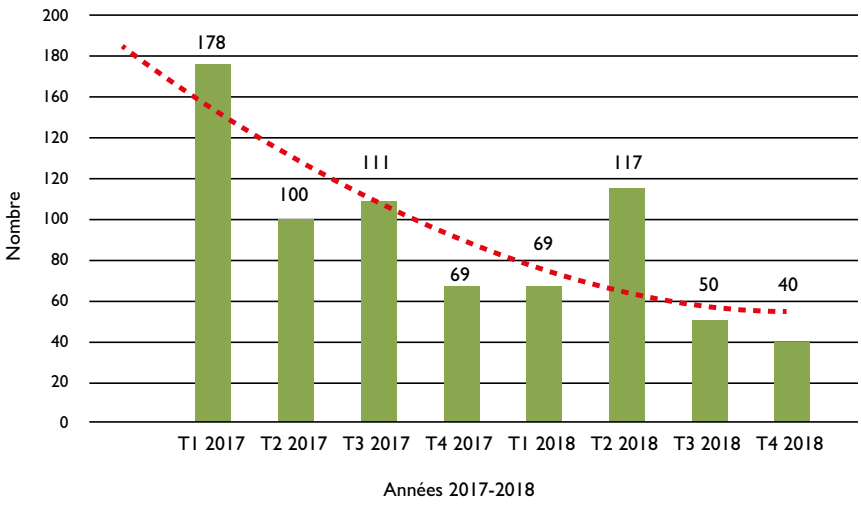


Figure 8 : Défigurations recensées en 2017 et 2018 par l'ANSSI
NB : Le pic de défigurations du 1er trimestre 2017 est dû à une vulnérabilité WordPress / Joomla et celui de 2e trimestre 2018 à une même attaque sur 42 sites de mairies hébergés sur une même IP.

(79) *La défiguration (ou défaçage) est l'altération visuelle de l'apparence d'un site Internet non voulue par son éditeur. Elle est le signe visible qu'un site web a été attaqué et que le ou les attaquants en ont obtenu les droits, leur permettant ainsi d'en modifier le contenu.*

Globalement, la tendance sur plusieurs années est clairement à la baisse.

Le 10 avril 2018, le clip musical « Despacito » de Luis Fonsi, qui avait dépassé plus de 5 milliards de vues sur la chaîne Youtube, a été défiguré sur le site de la société américaine Vévo, partenaire de Youtube. Dans un premier temps, le titre du clip et de la vignette de présentation ont été modifiés, puis le clip supprimé. Une centaine d'autres titres de cette même chaîne Youtube ont été défigurés. Les faits ont été revendiqués sous des pseudonymes de *hackers* connus. L'enquête diligentée par la BEFTI a permis d'identifier les auteurs et d'établir que ces faits ont été consécutifs à l'achat sur Internet par ces derniers d'un couple d'identifiant/mot de passe correspondant à celui d'un administrateur système qui leur a permis de récupérer le code source du site internet de la société victime. Ayant reconnu les faits, les auteurs ont été déférés au Parquet. L'un a été jugé irresponsable et le second condamné à une peine de travaux d'intérêt général. L'action civile suit son cours.

2.2.2.5 Les attaques téléphoniques

En matière de fraude à la téléphonie, les malfaiteurs ont adopté 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.

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.

Les faits signalés aux forces de police et de gendarmerie ont très largement concerné deux procédés : le ***phreaking***[80] 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[81] 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 2018 de 8 plaintes visant des fraudes aux autocommutateurs téléphoniques (contre 14 en 2017) ; le préjudice total reste important, environ 552 700 euros (également légèrement en baisse par rapport à 2017 avec 570 000 euros). Cette fraude qui, au plan macroéconomique est énorme, perdure car les factures téléphoniques dans les grandes entreprises ne sont pas particulièrement analysées. Elle n'est donc repérée que tardivement et souvent révélée par l'opérateur. Il n'en reste pas moins que des mesures simples en amont peuvent réduire la fraude, comme l'utilisation de télégestion à distance avec un code personnalisé et non par défaut, ou le paramétrage strict des serveurs permettant les communications des postes et assistants téléphoniques aux fonctionnalités coûteuses telles les lignes internationales.

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

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

La participation de la BEFTI à un groupe de travail au sein d'Europol EC3 sur la fraude aux numéros internationaux surtaxés a permis d'identifier de nouveaux axes d'investigation qui ont été mis à profit en 2018.

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 le numéro de la ligne téléphonique du professionnel. Ce dernier obtient ainsi des informations confidentielles ou demande que lui soient effectués des virements pour alimenter un compte ouvert à son nom.

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.

Le C3N a enquêté sur des actions téléphoniques malveillantes à l'encontre de plusieurs Centres d'Opérations et de Renseignement de la Gendarmerie sur le territoire national. Plus de 1 000 appels dissimulés ont ainsi été émis sur un même week-end, du 1er au 3 juillet 2017, visant à provoquer des interventions urgentes des forces de l'ordre et à ouvrir des conférences téléphoniques mettant en relation divers services d'urgences (SAMU, SOS médecin, pompiers, gendarmerie et police) entre eux de manière non désirée. Le mis en cause a été interpellé en août 2018.

2.2.3 L'utilisation d'Internet à des fins criminelles

2.2.3.1 L'utilisation d'Internet à des fins terroristes

Au cours de l'année 2018, la plateforme de signalement des contenus illicites de l'Internet (PHAROS) a recueilli 4 550 signalements relatifs à des contenus terroristes ou apologiques (2,8 % du total des signalements), contre 6 750 en 2017 et 11 400 en 2016 (respectivement 4,4 % et 6,7 % des signalements).

La volumétrie globale des productions de propagande diffusées par les organes « officiels » de **l'organisation EI** (Nashir News et Amaq) est ainsi en baisse, bien qu'une reprise des diffusions ait été constatée en fin d'année. La publication du magazine officiel « Rumiyah » a été stoppée en 2017. Les seules parutions régulières de l'organisation terroriste restent le bulletin hebdomadaire « Al Naba » (en PDF), ainsi que les bulletins audios quotidiens de la radio « Al-Bayan ». Néanmoins, les sympathisants de l'organisation terroriste EI (tel que Fursan Upload) continuent de diffuser et de multiplier les nouveaux contenus sur plusieurs canaux Telegram et sur différents services d'hébergement *(cloud).* De la même manière, ils font perdurer les anciennes productions en les republiant continuellement. Ils utilisent quotidiennement les services de copie de contenus pour diffuser et sauvegarder la propagande. Telegram demeure le primo vecteur de publicité et de stockage des nouvelles parutions. Toutefois, le changement de politique de ce réseau, répondant depuis le mois d'avril 2018 aux demandes de retrait des contenus à caractère terroriste et procédant à la suppression de nombreux comptes de sympathisants, pourrait expliquer l'utilisation depuis décembre 2018 de nouveaux vecteurs de diffusion.

Un appel en ligne aux dons en cryptomonnaie a été détecté, le 27 juin 2018, sur un site sympathisant de l'organisation EI mettant à disposition une grande quantité de contenus numériques de l'organisation. Toutefois, ce procédé ne semble pas s'être développé.

La mouvance Al-Qaïda dispose toujours de nombreux organes de diffusions officiels qui représentent les différentes entités de l'organisation (AQMI (JNIM), AQPA, AQSI et Al-Shebbaab notamment). Cette diversité se traduit par l'activité d'organes multiples, tels que le G.I.M.F, Sahab Média, Al Malahem et Al Fustaat, ainsi que via des organes concentrés sur les missions de traduction. Ces entités utilisent Telegram comme vecteur de publicité et de stockage des parutions.
En 2018, AQMI a notamment diffusé plusieurs communiqués relatifs à la situation d'otages, parmi lesquels Sophie Petronin, humanitaire enlevée au Mali en 2016 et dernier otage français retenu dans le monde.
La production d'infographies de menaces, émanant de sympathisants du groupe terroriste, en rapport avec les fêtes religieuses, les évènements de société (gilets jaunes) et sportifs (coupe du monde), demeure par ailleurs régulière. Le ralentissement de la propagande de l'organisation terroriste est lié à la réactivité croissante des grands réseaux sociaux (notamment Twitter), utilisés pour faire la publicité des contenus, qui neutralisent les comptes signalés.

En 2018, la plateforme PHAROS a transmis 12 100 demandes de retrait pour des contenus à caractère terroriste (contre 30 634 en 2017), 4 877 demandes de déréférencement et 51 demandes de blocage.

Par ailleurs, depuis le 28 février 2018, la plateforme PHAROS dispose d'un nouveau relais au niveau européen, via une connexion avec l'application IRMa[82] d'Europol. Les échanges de données reposent sur la transmission d'une liste d'adresses URL de contenus terroristes éligibles à une mesure de retrait. Au 31 décembre 2018, la plateforme PHAROS a intégré 69 937 contenus à caractère terroriste dans l'application européenne.

2.2.3.2 Les escroqueries

Les modes opératoires, parfaitement maîtrisés par les malfaiteurs, sont adaptés aux évolutions de la société et aux faits d'actualité. Les cybercriminels utilisent désormais systématiquement les outils d'anonymisation (VPN, Proxy, réseau Tor, téléphones équipés d'application de cryptage, applications de type WhatsApp, utilisation de numéros virtuels de type ONOFF…) et, de plus en plus, des systèmes de blanchiment d'argent recourant à des cryptomonnaies ou des plateformes de paiement dématérialisées.
En 2018, trois principaux types d'escroqueries massives ont impacté le territoire national portant le préjudice à plus d'un milliard d'euros. Les escroqueries aux faux ordres de virements internationaux sont une nouvelle fois en baisse. Les escroqueries aux faux investissements sur le FOREX *(foreign exchange)* se poursuivent. Alors que l'année précédente avait été marquée par une recrudescence des propositions frauduleuses d'investissements dans le diamant, en 2018 se sont développées des escroqueries liées à des placements indexés sur les cryptomonnaies. De nombreuses victimes restent en effet sensibles à une promesse de gain rapide, au rythme de l'évolution des cours des taux de change des monnaies virtuelles.
Enfin, l'année 2018 a aussi vu l'essor des escroqueries aux faux supports techniques et a également été marquée par la permanence des formes classiques d'escroqueries en ligne : escroqueries au préjudice des e-commerçants, escroqueries à la romance, chantages à la webcam, fausses annonces…

(82) Internet Referral Management application de l'unité de référencement Internet d'Europol (EU IRU).

Escroqueries aux faux ordres de virements internationaux (FOVI)

Depuis 2010, avec une accentuation entre la fin 2013 et fin 2014, la France est confrontée à un phénomène d'escroqueries d'envergure au préjudice d'entreprises françaises, de filiales françaises d'entreprises étrangères, de collectivités ou établissements publics et de fortunes françaises.

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 (cf. rapport état de la menace lié au numérique en 2018).

Les faits de FOVI sont, encore cette année, en net recul en France tant au niveau du nombre qu'en termes de montants, comme le montrent les histogrammes ci-dessous.

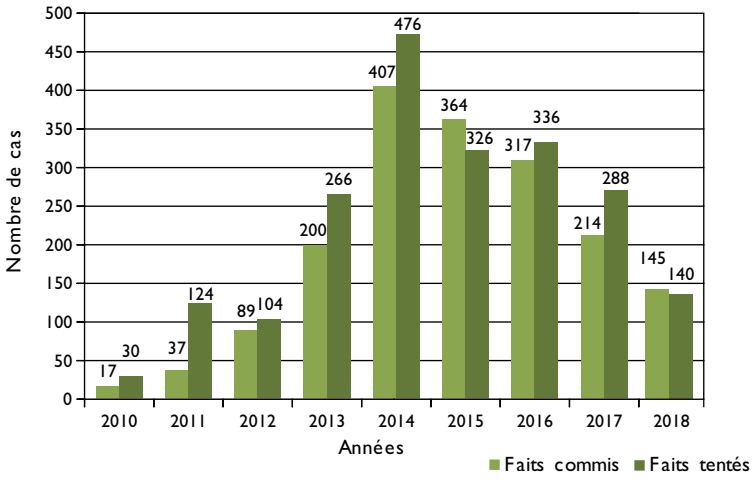


Figure 9 : - FOVI – Nombre de faits -Source OCRGDF

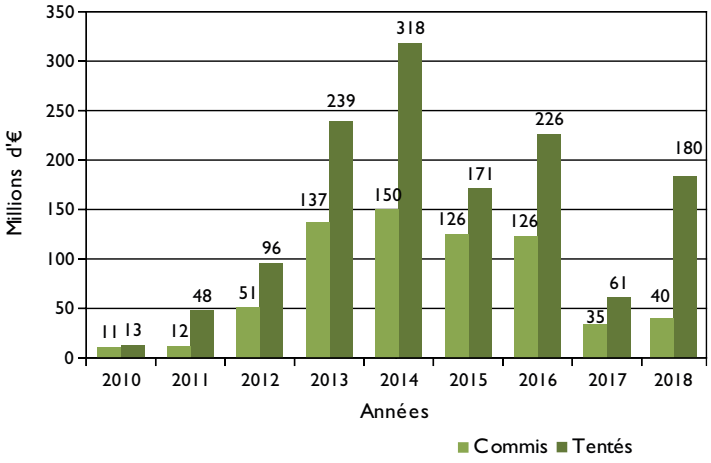


Figure 10 : - FOVI – Montants en jeu -Source OCRGDF

L'office central pour la répression de la grande délinquance financière (OCRGDF) de la direction centrale de la police judiciaire (DCPJ) a recensé, pour la France depuis le début du phénomène en 2010, plus de 2 600 sociétés victimes d'escroqueries avec un préjudice estimé à près de 700 millions d'euros pour les faits commis et 1,4 milliard d'euros pour les tentatives. Le phénomène est toujours prégnant sur le territoire.

En mars 2018, un groupe d'escrocs se faisant passer pour les dirigeants d'une entreprise cinématographique a délesté cette entité de la somme de 19 millions d'euros en persuadant sa filiale néerlandaise de transférer en plusieurs fois ce montant sur un compte extérieur, pour une prétendue acquisition à Dubaï.

Une série de démarches a permis d'inverser la courbe du préjudice. 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 en mars 2015 (MEDEF), le Club des directeurs de la sécurité et de la sûreté des entreprises (CDSE) en janvier 2016 et la Fédération bancaire française (FBF)[83].

Escroqueries aux faux investissements sur le FOREX *(foreign exchange)*

Après avoir connu une forte progression entre 2010 et 2015, ce phénomène s'est atténué, puis est réapparu à la fin de l'année 2017 jusqu'à l'été 2018.

Dans un premier temps, de nombreux sites internet d'investissement au FOREX *(Foreign Exchange)* ont été rachetés par des groupes criminels franco-israéliens et détournés de leur objet initial. Puis, ont été recrutés des ingénieurs informatiques afin de créer des services en ligne fictifs et des *call-centers*. Par un démarchage téléphonique intensif et/ou de la publicité sur le web, les particuliers sont invités à s'inscrire sur le site 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 (*« coach »*, 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, néanmoins il apparaît dépasser plusieurs centaines de millions d'euros en France. Des actions de prévention face aux escroqueries au FOREX ont été mises en place. L'Autorité des Marchés Financiers (AMF) réalise d'importantes campagnes d'information et de sensibilisation du public. Elle publie également une liste noire des sites proposant illégalement des services financiers en matière de FOREX. Les sites frauduleux ne sont identifiés qu'après le dépôt de plainte des victimes et sont très souvent remplacés par de nouveaux sites. Il est donc extrêmement difficile d'agir dès leur création en obtenant le blocage du site ou de procéder au gel des comptes bancaires, les fonds ayant été dissipés antérieurement.
Une deuxième action préventive consiste à prohiber ce type d'investissement. Par exemple, l'autorité des valeurs mobilières d'Israël a interdit à toutes leurs sociétés nationales d'options binaires[84] de cibler leurs citoyens. Les États-Unis ont fait de

(83) Création de modules de ***e-learning*** *sur le FOVI au faux président et sur les escroqueries au changement de coordonnées bancaires, en diffusion gratuite pour un objectif de prévention – DCPJ, DMISC, CDSE, FBF.*

(84) Une option binaire se différencie des autres options par le fait que le gain possible est connu à l'avance. Le principe est de prévoir le cours à la hausse (Call) ou à la baisse (Put) d'un produit sous-jacent à une date ou dans une durée de temps prédéfinie. Si le contrat est respecté, le trader empoche le gain prédéfini à l'émission de l'option. Si le contrat n'est pas respecté (la prévision est donc fausse), alors le total de l'investissement est perdu.

même. En août 2016, la Belgique est devenue le premier pays européen à prohiber ces placements financiers. Enfin, depuis le 2 juillet 2018 pour les options binaires et le 1er août 2018 pour les contrats sur la différence, l'autorité européenne des marchés financiers a interdit, par périodes de trois mois renouvelables, leur commercialisation et distribution aux particuliers. Les groupes criminels, surfant toujours sur l'actualité, ont diversifié leurs supports frauduleux à l'automne 2017. Ils ont ainsi recyclé les plateformes créées pour le FOREX et procédé à un démarchage agressif en matière d'investissement dans le diamant et dans les crypto-actifs.

Escroqueries aux placements indexés sur les cryptomonnaies

Le mode opératoire apparaît identique à celui de l'escroquerie à l'investissement dans le diamant, phénomène ayant perduré en France entre 2015 et 2017, au préjudice de milliers de victimes, pour un montant total de plus de 35 millions d'euros (cf. rapport 2018 - état de la menace pour l'année 2017).

Dans le cas de la fraude à l'investissement dans la cryptomonnaie, développée par des groupes criminels organisés franco-israéliens, les futures victimes sont approchées par des publicités sur Internet ou des campagnes d'*e-mailing,* les amenant sur des sites présentant des achats de cryptomonnaie comme un investissement "sûr", "très rentable", avec un accompagnement par des analystes marchés et stratégiques.

Le battage médiatique qui a accompagné les valeurs records du *Bitcoin* fin 2017 et début 2018 a créé un attrait autour de cette monnaie, que les escrocs ont largement su exploiter. Face à la chute progressive du *Bitcoin,* les victimes ont réagi en voulant récupérer leur investissement. L'étude des plaintes recueillies par la gendarmerie pour les escroqueries aux faux investissements en cryptomonnaie montre en effet une corrélation avec cette forte hausse du *Bitcoin :*

Figure 11 : Évolution du cours du *Bitcoin* de 2013 à 2019. Source : https://www.coingecko.com/fr/graphiques_cours/bitcoin/eur

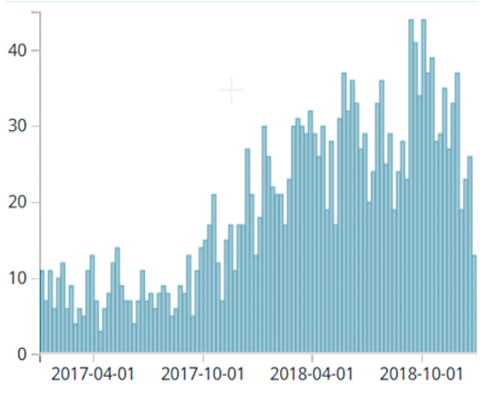


Figure 12 : Évolution du nombre de plaintes recueillies en gendarmerie pour des escroqueries aux faux investissements en cryptomonnaies.

Toutes les sociétés d'investissement dans la cryptomonnaie, visées par les enquêtes, sont domiciliées dans des pays d'Europe de l'Est, avec généralement un siège social secondaire fictif en région parisienne. L'activité de la société, son site Internet et les *call-centers* sont gérés depuis Israël.

En France, l'activité d'intermédiation consistant à recevoir des fonds de l'acheteur de cryptomonnaie pour les transférer au vendeur de cryptomonnaie relève d'un agrément de prestataire de paiement délivré par l'Autorité de contrôle prudentiel de résolution (APCR). Bien évidemment, toutes les plateformes visées par les enquêtes judiciaires ne disposent pas de cette qualité afin d'exercer leur activité sur le territoire national.

Fin 2017, des faits d'escroqueries en bande organisée portant sur de faux investissements en cryptomonnaie, au préjudice de plus de 57 victimes en France et dans l'UE, ont été rapprochés (préjudice de 5 millions d'euros).
Les investigations conduites par les sections de recherche de Strasbourg et Metz révèlent l'ampleur du phénomène et la complexité de l'organisation criminelle transnationale. Plus d'une trentaine de comptes bancaires liés à 20 entreprises ont été identifiés ainsi que le circuit de blanchiment.
Interpellés en janvier 2019, les quatre escrocs ont été mis en examen : trois écroués et un placé sous contrôle judiciaire. 1 025 000 € ont été saisis au titre des avoirs criminels.

Depuis un an, pour les faits dont l'OCRGDF a connaissance, le préjudice global s'élève à ce jour à plus de 35 millions d'euros, représentant plusieurs centaines de plaintes enregistrées sur l'ensemble du territoire.

La prévention apparaît encore comme le meilleur rempart face à ce type d'escroqueries opérées depuis l'étranger. L'AMF réalise d'importantes campagnes d'information et de sensibilisation du public et a également publié une liste noire des sites proposant ce type d'investissement.

Escroqueries aux faux supports techniques

L'escroquerie aux faux supports techniques consiste à perturber la victime par l'affichage intempestif de fenêtres indiquant la présence d'un virus sur l'ordinateur ou faisant état d'un problème grave touchant le système d'exploitation, 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 ce dépannage fictif. Une fois l'intervention terminée, la victime est invitée à régler le prétendu dépannage par virement ou par carte bancaire. En cas de refus, le technicien peut la menacer de rendre son système inutilisable. Connu initialement sous la dénomination *Compufly,* ce phénomène s'est démultiplié sous d'autres appellations *Easy support, Eureka,* « meilleurordinateur.com » tout au long de l'année 2017 avec une campagne d'escroquerie particulièrement active en novembre 2017.

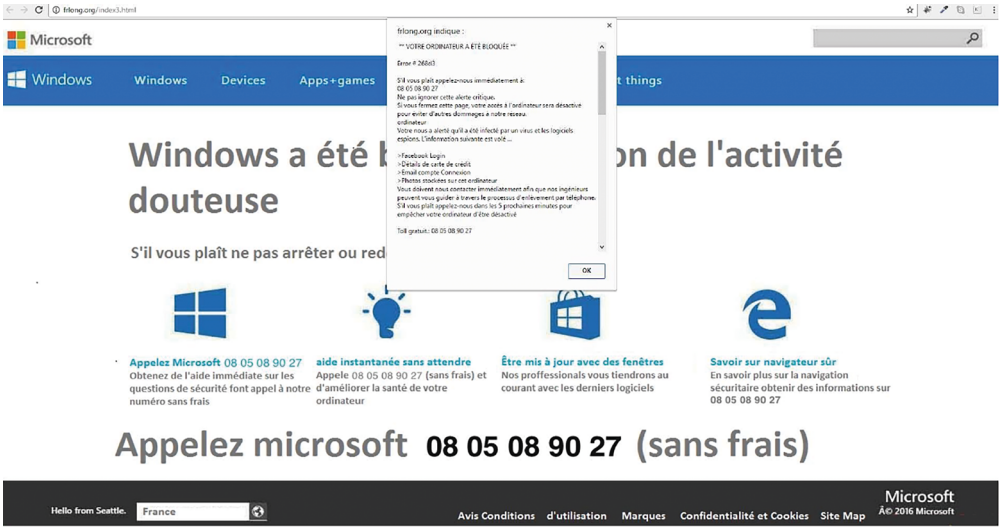


Figure 13 : Écran d'un ordinateur ciblé par une escroquerie aux faux supports techniques

Les rapprochements menés par le C3N ont permis de répertorier sur l'année 2017, 211 faits déclarés en gendarmerie. Sur la région parisienne, la BEFTI a enregistré 36 plaintes. Les échanges avec le GIP ACYMA ont permis de faire le lien entre plusieurs appellations de sociétés utilisant le même mode opératoire. Au regard de la multiplication des faits et des préjudices individuels minimes, la section F1 « cybercriminalité » du parquet de Paris a centralisé les procédures.

La BEFTI a été chargée de la première enquête selon ce mode opératoire visant les supports *Compufly* et *Easy support.* L'enquête se poursuit sur commission rogatoire et des demandes d'entraide pénale ont été lancées.

Saisi par la section cyber du parquet F1 de Paris, le C3N a recensé, en mars 2018, près de 8 000 internautes victimes d'escroqueries aux « faux supports techniques » pour un préjudice total évalué à près de deux millions d'euros. Les investigations ont permis d'identifier la manière d'opérer de cette organisation criminelle, laquelle utilisait des *call-centers* implantés en Tunisie. Le 29 janvier 2019, l'auteur principal et ses deux complices, dirigeants d'une société d'assurance de la région lyonnaise, ont été interpellés et placés en garde à vue. Au titre des avoirs criminels, 1,9 million d'euros ont été saisis. Les escrocs ont été mis en examen pour escroquerie en bande organisée, entrave au fonctionnement d'un système de traitement automatisé de données et blanchiment d'argent, et placés sous contrôle judiciaire strict, assorti de cautions de 100 000 €.

Dans un autre dossier sur commission rogatoire internationale émanant des autorités allemandes, la BEFTI a procédé en novembre 2018, à l'interpellation d'un couple d'Indiens, gérants d'une société de dépannage informatique, destinataire de plus de 400 000 € provenant de victimes allemandes selon ce mode opératoire des faux supports techniques et transférant l'essentiel des fonds en Inde. L'enquête a établi leur responsabilité et déterminé qu'ils agissaient pour le compte de centres d'appels situés en Inde apparaissant comme les organisateurs de la fraude.

Escroqueries à la fausse amitié (Scam Romance)

En avril 2018, agissant en exécution d'une commission rogatoire délivrée par un juge d'instruction parisien, les enquêteurs de l'OCLCTIC ont interpellé six individus appartenant à une équipe de malfaiteurs africains spécialisée dans les escroqueries sur internet. Ayant noué une liaison amoureuse via le site « e.darling » avec un prétendu marchand d'art italien, la victime était conduite, sous divers prétextes, à verser à celui-ci près de 9 000 euros par différents moyens (mandats internationaux, recharges de cartes prépayées et de téléphone), en échange de trois chèques qui s'avéraient être volés. Les premières investigations mettaient en évidence une escroquerie à la romance orchestrée depuis la Côte d'Ivoire. Pour le transfert des fonds en Côte d'Ivoire, les auteurs avaient recours aux services de banquiers occultes et diversifiaient les moyens de monétisation. Ainsi, il apparaissait que des commerçants complaisants, voire complices, facilitaient l'utilisation des cartes prépayées ou de cryptomonnaies achetées avec l'argent récupéré. Au terme de deux ans d'investigations, le volume considérable des escroqueries était mis en lumière : 700 cartes prépayées rechargées par les victimes et représentant près de 3 millions d'euros, étaient découvertes par l'étude des flux financiers. 27 victimes directes d'escroqueries via Internet étaient identifiées, ainsi qu'une centaine d'autres ayant subi l'usurpation de leur identité pour l'achat de cartes prépayées. Les investigations confirmaient une quasi-industrialisation des fraudes et révélaient qu'à l'autre bout de la chaîne, en Côte d'Ivoire, existe une bourse aux coupons de rechargement permettant aux escrocs de monétiser leur fraude auprès d'intermédiaires qui, en échange d'une commission, se substituent à eux.

Escroqueries au RGPD

Une vague d'escroqueries au RGPD est apparue après son entrée en vigueur le 25 mai 2018. Le mode opératoire est le suivant : l'auteur prend contact avec la victime et l'informe de la non-conformité de son entreprise au RGPD. L'escroc persuade la victime d'investir dans un faux service de mise en conformité via une plateforme Internet ou téléphonique qui se chargera de récupérer ses données bancaires. Les préjudices constatés varient entre 500 € et 1 500 € par escroquerie.

En juin 2018, la CNIL a diffusé sur son site Internet une alerte sur cette escroquerie qu'elle a réitérée en novembre avec des exemples de courrier « fausse mise en conformité RGPD ». La gendarmerie a également réalisé un certain nombre d'actions de communication sur cette escroquerie par l'entremise des référents sûretés.

Figure 14: Notice de vigilance de la CNIL

Escroqueries aux numéros de « Service à Valeur Ajoutée » (SVA)

Les escroqueries à la téléphonie se caractérisent par de lourds préjudices. L'année 2018 a vu de nouveaux cas de compromission des commutateurs téléphoniques des entreprises à des fins d'escroquerie aux numéros de Service à Valeur Ajoutée (SVA), dits « numéros surtaxés », opérés par des groupes organisés ultra-spécialisés. Techniquement complexes, ces infractions reposent sur une superposition aux interconnexions de services et d'opérateurs téléphoniques nationaux et internationaux. Elles nécessitent des canaux importants de blanchiment. Cette criminalité demeure une spécialité de certains ressortissants israéliens. Elle s'appuie notamment sur une multitude de prestataires de services, souvent complaisants contre lesquels l'OCLCTIC oriente désormais ses investigations.

Le 29 mai 2018, les enquêteurs de l'OCLCTIC interpellaient, pour escroqueries et blanchiment d'escroqueries en bande organisée, les dirigeants et employés d'une société spécialisée dans l'agrégation de numéros de type « service à valeur ajoutée », suite à la plainte d'un grand groupe de communication dont les marques étaient usurpées. Les escrocs promettaient, via l'appel vers des numéros surtaxés spécialement créés, de gagner des cadeaux qui s'avéraient inexistants. Le mode opératoire impliquait la création d'une société fictive afin d'obtenir des numéros SVA auprès d'un agrégateur. Une fois les numéros attribués, une autre personne était chargée de mettre en place un dispositif incitant les victimes à appeler : page web et profils Facebook/Instagram ou mise en place d'un système d'appel ou d'envoi de SMS automatisé. Enfin, une ou plusieurs personnes, voire des structures de type *« call center »*, étaient chargées de réceptionner les appels des victimes et de les maintenir en ligne le plus longtemps possible. L'ensemble de ces acteurs participait à un système organisé, dans lequel les fraudeurs et les agrégateurs percevaient les gains des appels émis par les consommateurs, lesquels pouvaient aller jusqu'à 3 euros au décrochage et 0,80 euro par minute. Le préjudice global a été évalué à près de 30 millions d'euros. Sans la complaisance de certains agrégateurs, cette arnaque très lucrative peut difficilement être mise en place. Dans le cadre d'un important travail de recoupement d'affaires sur plusieurs années, un agrégateur était ciblé. Les interpellations et investigations subséquentes confirmaient le rôle de fournisseur de moyens de sociétés dédiées exclusivement à la fraude aux numéros surtaxés durant la période 2015-2018. 6 millions d'euros étaient saisis.

Autres escroqueries

En janvier 2018, les enquêteurs de la DIPJ de Versailles démantelaient un groupe criminel dirigé par un individu, effectuant des escroqueries au préjudice de personnes vulnérables. Une quarantaine de victimes a été recensée, pour un préjudice supérieur à 300 000 euros. Parmi divers modes opératoires, le principal stratagème consistait à joindre des abonnés de lignes de téléphone fixe identifiés par un prénom « ancien » en se présentant comme policier ou magistrat de pôle financier et à faire croire à un piratage de carte bancaire. Après avoir mis en confiance les victimes, le malfaiteur parvenait à obtenir leurs références bancaires complètes qu'il utilisait pour réaliser des achats en ligne. Un autre mode opératoire consistait à faire croire aux correspondants qu'ils avaient été victimes du vol de certaines données personnelles et à obtenir par mail à une adresse « police-nationale-gouv.com » des fiches de paie, avis d'imposition et relevés de comptes. En cas de réticence, le principal malfaiteur leur transmettait une fausse réquisition de police ou copie de carte professionnelle. Les documents ainsi obtenus servaient ensuite de support à leurs agissements auprès de nouvelles victimes.

Dans le cadre de la surveillance du réseau Internet, les enquêteurs de la section de recherches de Grenoble identifiaient une méthode de blanchiment d'infractions par le biais de cartes bancaires spécialement liées à des comptes en monnaie virtuelle de type *Bitcoin*. Un couple a ainsi été mis en cause pour près de 630 000 € d'escroqueries commises depuis 2015 en ouvrant des comptes ou souscrivant des crédits avec de faux documents provenant du *Darkweb*. L'argent escroqué était ensuite blanchi par le biais des comptes virtuels et des cartes ADV CASH. Le couple a été interpellé le 7 février 2019 ; de nombreux documents et matériels servant aux escroqueries ainsi que des produits de luxe ont été saisis. L'homme a été mis en examen et écroué.

2.2.3.3 Extorsions de fonds

Extorsion de fonds avec menace

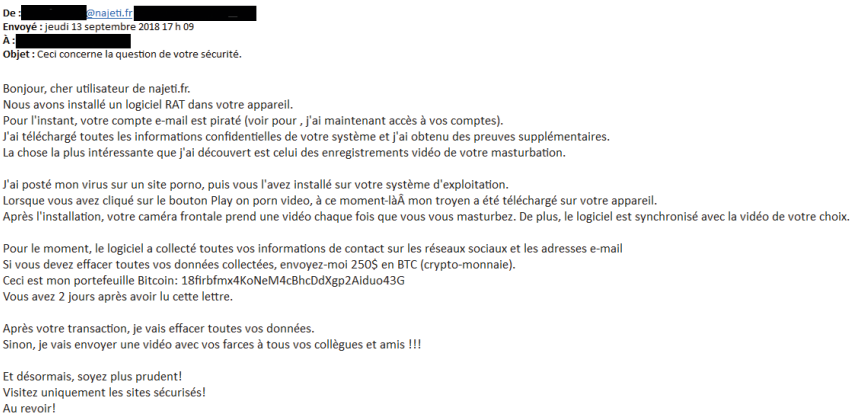
En matière d'extorsions, les tendances 2018 s'inscrivent sur plusieurs points dans la continuité de l'année 2017. Dans leur grande majorité, les victimes demeurent des hommes, souvent jeunes (31 % de mineurs en 2018, contre seulement 20 % en 2017). Leur hameçonnage s'est opéré en premier lieu via les sites de rencontre puis via l'usage des réseaux sociaux dont notamment Facebook. Les sites de rencontre servent de passerelles vers Facebook, qui fournit à l'auteur la liste des contacts parfois très proches de la victime. La présence d'Instagram dans près de 10 % des cas est une nouveauté en 2018. Comme en 2017, 1 victime sur 3 cède au chantage et paie une somme d'argent allant jusqu'à plusieurs dizaines de milliers d'euros, avec une somme moyenne de 1 100 euros, contre 600 euros en 2017. Cette hausse peut s'expliquer en partie par une évolution du mode opératoire qui consiste à davantage cibler les victimes les plus faibles pour maximiser les profits.

L'origine des auteurs reste complexe à établir en raison du faible taux d'élucidation de ces affaires. Toutefois, la Côte d'Ivoire semble toujours abriter une communauté significative d'auteurs. En effet, dans un quart des dossiers analysés par l'OCLCTIC (53 sur 200), les investigations remontent directement vers ce pays d'Afrique de l'Ouest, via les adresses IP ou les instructions de paiement. Comme les années précédentes, des signalements Interpol contenant les renseignements utiles de la procédure (pseudonyme, IP, téléphone…) ont été systématiquement émis vers les États de résidence des auteurs.

L'OCLCTIC entretient une coopération avec la Plateforme de Lutte Contre la Cybercriminalité de la police ivoirienne qui peut fournir des informations intéressantes concernant les profils des criminels. Ces derniers ne semblent pas évoluer dans des réseaux organisés, mais se transmettent plutôt leur « savoir-faire » de manière informelle. Les individus commettent leurs délits sur des *smartphones*, à domicile ou sur la voie publique, durant leur période d'inactivité professionnelle. Les gains illicites sont immédiatement dépensés. Les enquêtes se heurtent aux difficultés locales d'investigation, notamment en termes de possibilités d'identification de numéro de téléphone ou d'adresse IP. Pour autant, tous les signalements transmis par la France sont systématiquement exploités par les policiers ivoiriens et a minima intégrés dans leur base de données, afin d'initier des enquêtes judiciaires.

« Sextorsion » – chantage à la webcam prétendument piratée

En septembre 2018, la gendarmerie s'est intéressée à la diffusion massive d'un e-mail indiquant la récupération de vidéos intimes suite au piratage de l'ordinateur de la victime (Web Cam) et sa navigation sur des sites pornographiques. L'auteur exigeait un paiement en *Bitcoin* sous peine de diffuser les vidéos qu'il disait avoir récupérées par un logiciel de prise de contrôle à distance (RAT). Les données personnelles éventuellement alléguées avaient en réalité été obtenues sur Internet et non par l'utilisation d'un RAT.



De : [redacted]@najeti.fr [redacted]
Envoyé : jeudi 13 septembre 2018 17 h 09
À : [redacted]
Objet : Ceci concerne la question de votre sécurité.

Bonjour, cher utilisateur de najeti.fr.
Nous avons installé un logiciel RAT dans votre appareil.
Pour l'instant, votre compte e-mail est piraté (voir pour , j'ai maintenant accès à vos comptes).
J'ai téléchargé toutes les informations confidentielles de votre système et j'ai obtenu des preuves supplémentaires.
La chose la plus intéressante que j'ai découvert est celui des enregistrements vidéo de votre masturbation.

J'ai posté mon virus sur un site porno, puis vous l'avez installé sur votre système d'exploitation.
Lorsque vous avez cliqué sur le bouton Play on porn video, à ce moment-làÃ mon troyen a été téléchargé sur votre appareil.
Après l'installation, votre caméra frontale prend une vidéo chaque fois que vous vous masturbez. De plus, le logiciel est synchronisé avec la vidéo de votre choix.

Pour le moment, le logiciel a collecté toutes vos informations de contact sur les réseaux sociaux et les adresses e-mail
Si vous devez effacer toutes vos données collectées, envoyez-moi 250$ en BTC (crypto-monnaie).
Ceci est mon portefeuille Bitcoin: 18firbfmx4KoNeM4cBhcDdXgp2Aiduo43G
Vous avez 2 jours après avoir lu cette lettre.

Après votre transaction, je vais effacer toutes vos données.
Sinon, je vais envoyer une vidéo avec vos farces à tous vos collègues et amis !!!

Et désormais, soyez plus prudent!
Visitez uniquement les sites sécurisés!
Au revoir!

Figure 15 : Exemple de mail de chantage - source C3N

Le but recherché est ici d'extorquer de l'argent aux victimes en échange de leur silence. Il s'agit d'une escroquerie de type ingénierie sociale, destinée à exploiter les faiblesses psychologiques, sociales et organisationnelles. En réalité, l'auteur ne détient aucune vidéo de la victime. Il agit sur le ressort psychologique en faisant mention de données personnelles, ce qui donne de la crédibilité à son mail et à son chantage.

Depuis janvier 2019, le site cybermalveillance.gouv.fr a constaté une forte recrudescence de ces campagnes d'arnaques. Pour sensibiliser le public, une fiche d'information et de conseil a été diffusée sur le site[85].

Le mode opératoire a évolué au fil du temps, avec en particulier des menaces sur l'intégrité physique de la victime. Les escrocs comptent sur le volume de pourriels envoyés et la crédulité de leurs destinataires, pour rentabiliser leur campagne.

(85) **https://www.cybermalveillance.gouv.fr/nos-articles/chantage-a-la-webcam-pretendue-piratee/**

Extorsion de fonds avec violence

Internet reste utilisé pour faciliter le délit traditionnel d'extorsion accompagné de violences physiques.

Un couple était interpellé en août 2018 par la sûreté départementale de la DDSP du Rhône (69). La femme donnait rendez-vous à son domicile à des clients pour des prestations sexuelles sur le site de chat gratuit coco.fr. Sur place, les victimes faisaient l'objet d'extorsion avec arme et remettaient sous la contrainte tous leurs effets personnels (téléphones, titres de transports…), ainsi que leurs cartes bancaires et les codes afférents. Trois victimes étaient répertoriées. Les deux auteurs ont été interpellés puis écroués.

2.2.3.4 La lutte contre la fraude à la carte bancaire

Les données statistiques

Le montant total de la fraude sur les transactions de paiement et de retrait effectuées en France et à l'étranger avec des cartes françaises a de nouveau reculé en 2017 (de 9,6 % par rapport à 2016)[86]. Il s'établit à 360,7 millions d'euros, et cela alors même que le montant total des transactions augmente sensiblement (5,8 %) à 664,6 milliards d'euros. En conséquence, le taux de fraude sur les cartes de paiement françaises s'établit désormais à 0,054 %, contre 0,064 % en 2016, soit son plus bas niveau sur la période 2009-2017.

Ce taux moyen recouvre toutefois des situations contrastées, avec notamment une fraude très réduite sur les paiements au point de vente (0,008 %), mais plus significative sur les paiements à distance (0,161 %), en dépit d'une nouvelle baisse remarquable de la fraude sur ce canal. La fraude sur les paiements sans contact présente un taux de 0,02 % et résulte seulement du vol ou de la perte de la carte.

L'usurpation de numéros de cartes pour réaliser des paiements frauduleux reste toujours la principale origine de la fraude (66 % en montant), la seconde étant le vol (32 %).

Enfin, le nombre de cartes françaises pour lesquelles au moins une transaction frauduleuse a été enregistrée au cours de l'année 2017 s'élève à 1 213 000, en progression de 6,5 % par rapport à 2016, mais avec une baisse significative du montant unitaire des cas de fraude à 84 euros en 2017, contre 95 euros en 2016.

Ces résultats sont essentiellement dus au déploiement de dispositifs avancés de prévention de la fraude par l'ensemble des acteurs, tant des émetteurs de moyens de paiement que des commerçants et des entreprises, notamment :

> le recours croissant à des dispositifs d'authentification du payeur, notamment au moyen du protocole **3D-Secure,** pour mieux protéger les transactions de paiement sur Internet ;

> le développement de dispositifs de ***scoring,*** c'est-à-dire de systèmes experts capables d'évaluer le niveau de risque d'une transaction donnée sur la base de certaines de ses caractéristiques.

(86) Données issues du rapport 2018 de l'Observatoire sur la sécurité des moyens de paiement (OSMP).

Ces outils de prévention de la fraude font aujourd'hui partie des exigences en matière de sécurité inscrites dans la 2e directive européenne sur les services de paiement (DSP2), en application depuis janvier 2018 dans l'ensemble de l'UE.

Pour l'année 2018, 53 703 plaintes pour fraude à la carte bancaire[87] ont été traitées par les services de police ; ce chiffre est relativement stable par rapport à 2017 (53 840 faits recensés). Paris demeure le premier département où ces faits sont portés à la connaissance des forces de sécurité (25 %), suivi du Rhône (5 %) et des Bouches-du-Rhône (4 %). Le taux d'élucidation reste faible (5 %).

Les modes opératoires

Considérée comme l'une des priorités européennes de la lutte contre la cybercriminalité, la captation des données bancaires demeure un fait criminel fortement présent sur le territoire national. Les modes opératoires concernent désormais tous les types de distributeurs automatiques (distributeurs de billets, bornes de distribution d'essence, automates d'autoroute, dispositifs de règlement de parking…), sur lesquels ***skimmers***[88] et ***shimmers***[89] continuent d'être installés. Les terminaux de paiement portatifs peuvent être également compromis ou complètement détournés de leurs finalités. Ces captations de données sont notamment le fait de nombreux groupes criminels d'Europe centrale ou balkanique, lesquels sévissent lors de raids traversant les régions françaises. Les données sont ensuite revendues sur des sites Internet classiques, sur le *darknet* ou au travers d'applications téléphoniques. Leur ré-encodage sur des cartes à piste magnétique permet notamment des fraudes dans des pays d'Amérique ou d'Asie du Sud-Est ne possédant pas les mêmes standards de sécurité que la France.

En 2018, les attaques de distributeurs bancaires par la **technique dite du *« jackpotting »***[90] se sont diversifiées et intensifiées. Si le mode opératoire consistant à percer les façades des automates afin d'y connecter un ordinateur semble avoir disparu, deux variantes s'imposent désormais : une première, non destructrice, consiste en la désolidarisation de la façade du distributeur de billets de son socle afin de permettre un accès direct aux connectiques ; une seconde s'effectue par le retrait pur et simple de l'écran de l'automate pour accéder aux branchements du serveur gérant les caissettes d'argent. Pour l'année 2018, les attaques ont principalement eu lieu en région parisienne, dans l'Est de la France ainsi qu'en région lyonnaise pour un préjudice global de 420 000 euros (le préjudice de chaque attaque peut varier entre 12 000 et 150 000 euros selon le dispositif attaqué). Il ressort des différentes interpellations que les auteurs sont principalement issus d'Europe de l'Est.

---

(87) Ces chiffres sont extraits du fichier TAJ (traitement des antécédents judiciaires) et regroupent les qualifications d'utilisation frauduleuse de carte bancaire, d'utilisation frauduleuse d'un moyen de paiement en France et captation des données en France ou à l'étranger ou en un lieu indéterminé, d'utilisation frauduleuse d'un moyen de paiement à l'étranger et captation des données en France, d'utilisation frauduleuse du numéro de carte bancaire, utilisation frauduleuse numéro carte bancaire (compte français et captation de données en France ou en lieu indéterminé) et falsification contrefaçon de carte de paiement ou de retrait.

(88) Matériel se glissant dans la bouche/fente d'un automate, tout en laissant de l'espace pour qu'une carte bancaire puisse y être glissée naturellement. Une copie des données de la piste magnétique sera alors réalisée par le matériel sans que cela n'ait une quelconque implication sur le bon fonctionnement de la carte bancaire.

(89) Le shimmer est un matériel similaire au skimmer dans son intégration dans un automate mais qui intercepte les données de la puce de la carte bancaire, dont son code confidentiel.

(90) Connexion d'un ordinateur portable soit pour accéder aux données du calculateur du DAB, soit pour injecter un malware visant à vider totalement ce dernier, à l'instar des célèbres machines à sous des casinos.

En réponse, un dispositif de coordination de la lutte contre le *jackpotting* a été mis en place par l'OCLCTIC en 2018 ; il repose sur le suivi de tout fait survenant sur le territoire national.
Globalement le nombre de piratages de distributeurs automatiques et de terminaux, toutes techniques confondues, est en très forte baisse en 2017.

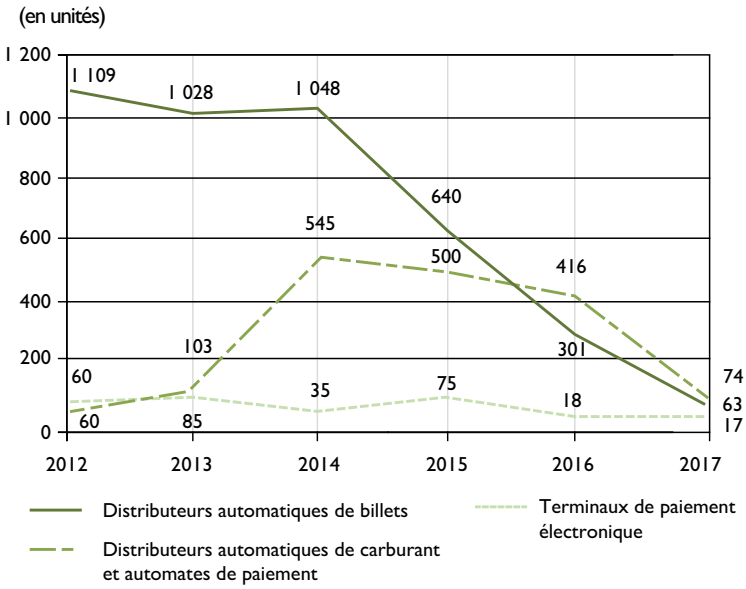


Figure 16 : Nombre d'infractions constatées sur les distributeurs et terminaux
Source : Observatoire de la sécurité des moyens de paiement.

L'action des services de police

Dans la nuit du 3 au 4 juillet 2018, les effectifs de la Brigade Anti-Criminalité du Commissariat du Havre procédaient à l'interpellation de deux ressortissants roumains, lesquels venaient de tenter de mettre en place un *skimmer* en centre-ville. Saisis des faits, les enquêteurs du SRPJ de Rouen établissaient les habitudes des deux individus et découvraient dans leur chambre d'hôtel un matériel complet de captation de données de cartes de paiement pour distributeurs automatiques.

En mai 2018, les enquêteurs de la DIPJ de Lille mettaient au jour les activités d'un groupe organisé originaire de Côte d'Ivoire et du Maroc, spécialisé dans l'usurpation de numéros de cartes bancaires aux fins d'escroquerie dans la vente à distance. Le mode opératoire consistait en la récupération de numéros de cartes bancaires (par hameçonnage des victimes ou suite à des achats sur le *darknet*), ainsi que des identifiants de connexion aux box Internet des victimes, afin de programmer un renvoi vers les escrocs des appels des banques en vue de confirmation des achats. Les produits technologiques achetés frauduleusement étaient ensuite récupérés en France ou en Italie. Les produits immatériels (mandats Western Union et cartes TransCash) étaient saisis au Maroc.

En mai 2018, les enquêteurs de la DIPJ de Lyon interpellaient un individu de nationalité djiboutienne pour des faits d'escroquerie par manipulation de terminal de paiement électronique. L'individu, dirigeant d'une entreprise de sécurité informatique en France, surfacturait ses prestations et utilisait également des numéros de cartes bancaires étrangères, illégalement obtenus, pour un préjudice total de 162 000 euros (sur un montant de 414 000 euros de tentatives). Les fonds étaient ensuite blanchis au travers d'autres entreprises complices et de comptes bancaires personnels notamment situés à l'étranger.

Europol coordonne un certain nombre d'actions ciblées permettant de lutter contre les usages frauduleux de numéros de cartes bancaires volées ou piratées.

Opération « Global Airport Action Day »
Depuis 2013, l'agence européenne programme des journées d'action, les *Global Airport Action Day* (GAAD), en liaison avec les compagnies aériennes, les sociétés de cartes bancaires (CB) et les services d'enquête des États à travers le monde, en collaboration avec Interpol notamment. La fraude CB est à l'origine d'environ 13 % des pertes financières observées par les compagnies aériennes. Chaque année en Europe, 300 000 transactions illégales, soit 820 par jour, affectent ces sociétés, les compagnies *« low cost »* étant plus particulièrement touchées. Depuis avril 2014, la gendarmerie des transports aériens (GTA) participe au nom de la France à ces *Action Days*. Lors de l'opération 2018, 141 personnes ont été arrêtées dans 226 aéroports répartis dans les 61 pays participants. En France, la GTA a ainsi intercepté, les 20 et 21 juin, 5 passagers qui tentaient de voyager grâce à un billet payé en ligne avec une carte bancaire usurpée.

Opération « e-commerce Action Week 2018 »
Durant la période du 6 au 16 juin 2017, EC3 *(Europol Cyber Crime Center, Focal Point « Terminal »)* impulsait une dynamique à 28 pays européens et partenaires pour lutter contre les escroqueries commises sur Internet au moyen de cartes bancaires usurpées. Sur coordination de l'OCLCTIC et avec la participation de services d'enquête de la DCPJ, de la DCSP, de la Préfecture de Police de Paris et de la Gendarmerie nationale, 17 individus étaient interpellés en flagrant délit. Au total, 95 interpellations ont été réalisées sur l'ensemble de l'action par les 28 pays participants.

L'action des organismes bancaires

Du point de vue de la brigade des fraudes aux moyens de paiement (BFMP) de la Préfecture de Police, la lutte contre la fraude aux cartes bancaires repose aujourd'hui essentiellement sur l'amélioration de la sécurité des cryptogrammes (suite de 3 chiffres au recto de la CB). Ainsi plusieurs banques (la Société Générale étant la première) proposent des cartes bancaires à cryptogramme dynamique : leur changement est automatique et régulier. Ainsi, les sites de vente à distance, qui demandent au porteur de renseigner le cryptogramme, ne peuvent pas réutiliser ces données bancaires après un certain laps de temps, puisque celles-ci auront été modifiées. Les risques de fraude avec de telles CB pour des achats à distance sont ainsi très limités.

Les banques testent aussi une nouvelle carte équipée, comme certains *smartphones,* d'un lecteur d'empreintes digitales pour sécuriser les paiements sans contact. Il doit être noté qu'en 2017, le nombre de paiements sans contact a doublé : avec les 51,2 millions de cartes sans contact en circulation en France, un peu plus de 1,2 milliard de règlements sans frappe de code ont été enregistrés (628 millions en 2016), pour un montant total de 12,9 milliards d'euros (6,5 milliards d'euros en 2016)[91]. Il est donc important de sécuriser ce moyen de paiement même s'il est limité à un montant de 30 euros.

2.2.3.5 Les marchés criminels en ligne

Le *Darkweb* continue de fournir une assistance aux cybercriminels à la recherche d'un réseau de contacts et des outils nécessaires à la commission des infractions. Il demeure une plateforme essentielle dans l'organisation de nombreux trafics et constitue l'interface de revente des données personnelles acquises frauduleusement à l'occasion des diverses formes de cyberattaques.

En juin 2018, un forum francophone majeur du *darknet,* la « **Main Noire** », qui opérait depuis plusieurs années, a été démantelé. Quatre de ses gérants domiciliés sur Lille, Marseille et Montpellier ont été arrêtés simultanément. Alimentant des trafics de toutes natures, ce site était adossé à une place de marché permettant la mise en relation de vendeurs et d'acheteurs de produits ou services illicites, tels que des stupéfiants, des faux documents d'identité et des données bancaires frauduleusement captées. L'enquête diligentée par Cyberdouanes (DGDDI) et l'OCLCTIC, sous la direction du parquet de la J.I.R.S. de Lille, a démontré un haut niveau d'organisation et de structuration du site, à l'instar des plateformes commerciales classiques. La base de données du forum a pu être saisie par les enquêteurs ; plus de 3 000 coordonnées d'utilisateurs ainsi que 250 000 messages échangés depuis 2015 ont pu être récupérés.
Déférés le 15 juin 2018 au parquet de la J.I.R.S. de Lille, les 4 administrateurs du site ont été mis en examen par le juge d'instruction désigné. Trois d'entre eux ont été placés sous mandat de dépôt et écroués tandis que le quatrième était placé sous contrôle judiciaire.

(91) Selon l'Observatoire de la sécurité des moyens de paiement (OSMP) de la Banque de France.

En juillet 2018, le C3N a interpellé dans les Hauts-de-France l'administrateur du site ***Wolfshop*** sur le *darkweb,* proposant à la vente plus de 550 000 identifiants (adresse mail, pseudo, mot de passe) de comptes de messagerie, de comptes clients sur les plateformes de grande distribution en ligne ou encore de cartes bancaires. D'autres services étaient également proposés sur le site comme du mail *bombing* ou encore une liste de vulnérabilités informatiques de grands sites commerçants. Ce *« black market »* qui comptait 2 800 utilisateurs est aujourd'hui fermé.

2.2.3.6 Les atteintes aux personnes

Les discours de haine et les discriminations

En 2018, la plateforme de signalement des contenus illicites de l'Internet (PHAROS) a traité au total 14 332 signalements de discriminations, contre 13 277 en 2017. Près de la moitié des contenus signalés relève de la provocation publique à la haine et la discrimination raciale, ethnique ou religieuse (discours antisémites, anti-musulmans, anti-arabes, anti-chrétiens, anti-blancs, etc.)

Les données de l'année 2018 confirment la tendance observée en 2017 :

> un retour à la volumétrie antérieure aux années 2015 et 2016, qui avaient été marquées par un nombre important de signalements en lien avec le terrorisme ;

> une baisse des signalements pour provocation à la haine et à la discrimination raciale, ethnique ou religieuse qui pourrait s'expliquer par les efforts consentis par la plupart des grands réseaux sociaux américains pour modérer les propos les plus virulents (5 093 en 2018 contre 7 246 en 2017 soit -30 %) ;

> une augmentation des signalements d'injures et diffamations (7 798 en 2018 contre 4 555 en 2017 soit +71 %)

Les réseaux sociaux, dont le principal objectif est l'échange et le partage de contenus, constituent les principaux supports de messages de haine. La majorité des signalements se rapporte à des contenus présents sur les réseaux sociaux américains.

Au niveau européen, PHAROS participe aux campagnes de tests organisées par la Commission en application du code de conduite signé avec un certain nombre d'opérateurs de l'Internet le 31 mai 2016 ; il s'agit d'évaluer le délai de prise en compte des messages de haine et de discrimination qui sont notifiés aux opérateurs Youtube, Facebook et Twitter. Ces tests ont été effectués par 31 associations de 24 pays et 3 administrations publiques, parmi lesquelles PHAROS. Un test a été réalisé en 2016, deux en 2017 et un en 2018, de cinq semaines chacun. La volumétrie oscille entre 2 500 et 3 500 notifications par test, tous pays confondus. Les résultats du premier test ont montré l'insuffisance de la réaction des sociétés sondées. Les deux exercices suivants ont révélé en revanche une amélioration de la prise en compte des notifications et la réduction des délais de traitement. L'évaluation des notifications sous 24 heures a progressé à chaque test, passant de 40 % à 51 %, puis à 72 % fin 2018.

Les atteintes aux mineurs

L'influence des médias sociaux

L'année 2018 a aussi été marquée par de nouvelles formes de cyberviolences. Au cours du deuxième semestre, le phénomène dit du « ***Momo Challenge*** » a soulevé des inquiétudes en France. Il est décrit comme un jeu dangereux constitué d'une suite de défis lancée via l'application pour *smartphone* WhatsApp. Des comptes Facebook mettraient au défi les utilisateurs de communiquer avec un numéro de téléphone inconnu. Une fois le premier contact établi via WhatsApp, le compte de « Momo »[92] s'afficherait avec comme premier message « Salut, je suis Momo et je sais tout de toi » et donnerait divers détails relatifs à la vie privée du destinataire. « Momo » enverrait ensuite un certain nombre de défis incitant les utilisateurs adolescents à s'engager dans une série d'actes de plus en plus morbides et violents, en créant un climat anxiogène.

Ce « challenge » vient des pays d'Amérique latine, où dans une affaire de suicide d'une fillette de 12 ans en Argentine, la police aurait initialement fait le lien entre une conversation WhatsApp de la victime et son passage à l'acte. Cette affaire a été relayée par la presse locale puis la presse internationale qui l'a rapprochée du « ***Blue Whale challenge*** »[93]. En France, dans les quelques affaires où ce « challenge » pouvait apparaitre, les forces de sécurité ont constaté qu'il s'agissait avant tout d'adolescents qui ont eu des comportements malveillants envers d'autres. Plusieurs comptes de réseaux sociaux ont été désactivés. Les unités territoriales ont été avisées du phénomène et des contacts ont été engagés avec des associations de protection de l'enfance (e-enfance…).

Deux mineurs de 15 et 16 ans, auteurs d'agressions commises sur d'autres lycéens, ont été interpellés fin 2017 par la sûreté départementale de la DDSP de Moselle (57). Le « **Marave challenge** » est une sorte de jeu né sur les réseaux sociaux et consiste à lancer un défi visant à rouer de coups un inconnu dans la rue et filmer contre une récompense de quelques dizaines d'euros. Les auteurs ont été identifiés suite à l'exploitation des caméras de surveillance de la ville et du réseau de transport, par des investigations sur les réseaux sociaux et l'analyse de leurs téléphones portables. Un mineur a été placé en centre éducatif fermé et le second sous contrôle judiciaire.

(92) « Momo » est le pseudonyme d'un individu qui se cache derrière la photographie d'une « femme oiseau » sculptée par un artiste japonais (La « Mother Bird » de Midori HAYASHI, exposée à la Vanilla Gallery de TOKYO depuis 2016), connu pour ses créations chimériques et horrifiques. Apparue sur Instagram en août 2016 sur le compte d'HAYASHI, la photographie servait d'avatar au profil WhatsApp de « Momo ».

(93) Le « Blue Whale Challenge » avait causé en 2016 plusieurs dizaines de suicides en Russie. Il était apparu en France fin 2016.

Le cyberharcèlement

S'il touche aussi les adultes (ex.: ligue du LOL), le cyberharcèlement est particulièrement le fait des mineurs entre eux, participant à l'ensemble des violences dans le cadre du milieu scolaire. Un certain nombre de structures sont dédiées à cette problématique, notamment Net Ecoute (0800 200 000) et le ministère de l'Éducation nationale a ouvert un site « Agir Contre le Harcèlement ».

Dans un contexte d'utilisation quotidienne des réseaux sociaux, le cyber-harcèlement et ses variantes peuvent avoir des conséquences irrémédiables.

Le 28 février 2018 en Nouvelle-Aquitaine, la gendarmerie est intervenue sur le suicide d'un mineur victime de *« sextorsion »*. Un jeune homme âgé de 17 ans s'est suicidé après avoir discuté avec un profil « féminin » sur Facebook. Le mineur, qui s'était dénudé devant la webcam, a été victime d'extorsion et de menaces concernant la diffusion de cette vidéo. N'ayant pas les moyens de répondre financièrement et ne supportant pas l'idée de voir la vidéo diffusée, il a mis fin à ses jours. Les investigations ont permis d'orienter l'enquête vers la Côte d'Ivoire. Plusieurs autres mineurs ont été approchés selon des scénarios similaires. L'enquête est toujours en cours.

La gendarmerie sensibilise les jeunes sur ces risques via des interventions dans les collèges et le C3N innove par la réalisation d'une vidéo Youtube[94] réalisée et diffusée par un YouTuber populaire.

Les services sont particulièrement attentifs à l'utilisation des réseaux sociaux par les mineurs et réagissent au plus vite sur des signalements laissant suggérer un risque d'atteinte à l'intégrité physique d'un mineur.

Le 8 janvier 2018, une personne signalait à la gendarmerie une vidéo sur **Periscope** mettant en scène une adolescente annonçant vouloir se suicider le jour même du toit de son lycée. Rapidement, le C3N a identifié le lycée et l'identité du mineur. Les forces de l'ordre ont pu se rendre au domicile, découvrir la mineure saine et sauve et informer sa famille.

Lutte contre la pédopornographie et l'exploitation sexuelle des enfants en ligne

Le phénomène de l'exploitation sexuelle des mineurs en ligne continue de croître. 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 (y compris des nourrissons) et des actes de plus en plus graves et violents. Les producteurs s'attachent de plus en plus à « anonymiser » ces matériels en occultant tout élément d'identification.

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

(94) Tibo InShape - public ciblé 13-16 ans.- ***https://www.youtube.com/watch?v=jrsbX_FOVHM***

La brigade de protection de la famille de la sûreté départementale de la DDSP du Rhône (69) a interpellé en septembre 2018 un prédateur sexuel qui piégeait les mineurs sur les réseaux sociaux. Se dissimulant sous de faux profils, l'individu mettait les jeunes en confiance, avant de leur demander des photographies. Les menaçant ensuite de les diffuser sur les réseaux sociaux, il exigeait d'autres clichés et vidéos de nature pornographique. Quatre mineurs signalaient avoir été piégés sur Snapchat. Les enquêteurs mettaient à jour lors des perquisitions 500 fichiers pédopornographiques échangés sur Skype avec une dizaine d'autres personnes sur le site Cocoland. L'individu a été écroué.

Il convient également de mentionner la progression des faits d'abus sexuels d'enfants commis à distance - phénomène dit du « ***live streaming*** » -, apparu 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 un ou plusieurs mineurs pré-pubères, sur ordre de l'acheteur. Initialement réalisée exclusivement aux Philippines, la production de ce type de vidéos s'étend à des pays d'Europe, en particulier la Roumanie. Plusieurs enquêtes initiées par l'OCRVP[95] ont concerné de jeunes victimes roumaines.

En 2018, suite à un signalement TRACFIN en raison de mouvements de fonds émis par des particuliers en France et à destination principalement d'agences Western Union situées aux Philippines (île de CEBU), l'OCRVP a été saisi de plusieurs enquêtes préliminaires pour des faits de *live streaming* impliquant des ressortissants français. L'OCRVP[95] s'emploie, non seulement à identifier les auteurs de ce type d'infractions mais également à tenter d'identifier les victimes, avec l'appui d'Europol et d'Interpol.

L'augmentation significative du nombre et des types de support utilisés 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.

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 TOR, permettant d'anonymiser l'origine des connexions. Une part importante d'individus à profils élevés, producteurs et/ou abuseurs sexuels s'y retrouve.

Par ailleurs, il est constaté la diffusion, via ces forums, d'images et de vidéos mettant en scène des mineurs victimes d'agissements de plus en plus violents, notamment d'actes sexuels accompagnés d'actes de torture pouvant aller jusqu'à la mort de l'enfant. Nombre de pédophiles migrent vers ces sites dits *« hurtcore »*.

En octobre 2018, l'OCRVP identifiait et interpellait l'un des membres de l'équipe d'administration du plus important et du plus ancien forum pédopornographique du *darknet,* comptant plus d'un million d'utilisateurs. Ce Français, en charge de la communauté francophone des membres de ce site, était mis en examen et écroué.

(95) Office central pour la répression des violences aux personnes.

Malgré l'action des services répressifs et l'utilisation de techniques spécifiques telles 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 toujours constaté que d'autres sites sont recréés rapidement.

Les outils d'anonymisation (VPN, proxys.) et les logiciels de cryptage sont par ailleurs toujours très utilisés. De même, les applications de communication mobiles (WhatsApp, Snapchat, Viber, Instagram) sont aussi un moyen pour ces délinquants d'échanger de manière sécurisée et chiffrée 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 servent également de supports aux prédateurs sexuels pour entrer en contact avec des victimes potentielles. Ce phénomène dit du *« grooming »* est toujours très prégnant.

En octobre 2017, un enquêteur de la région de gendarmerie de Toulouse initiait une enquête sous pseudonyme empruntant l'identité d'une fillette de 12 ans sur un forum de discussion du Web. Rapidement, il était abordé par un homme qui tenait des propos à caractère sexuel. Pendant neuf mois, l'homme a incité « l'enfant » à le rencontrer pour avoir une relation sexuelle et lui a envoyé des vidéos et des photos pornographiques. Le 19 juin 2018, le suspect a été interpellé alors qu'il devait rencontrer sa victime à Rodez. La perquisition de son véhicule a permis la saisie d'une boite de préservatifs neuve et de divers éléments corroborants. À son domicile, les enquêteurs ont saisi du matériel informatique renfermant des fichiers pédopornographiques. Après avoir reconnu la totalité des faits, l'homme a été condamné à 4 ans de prison ferme et écroué.

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). Tout matériel à caractère pédopornographique découvert au cours d'une enquête doit être transmis au CNAIP pour intégration.

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 utilisées dans le cadre d'échanges sous pseudonyme avec des prédateurs sexuels.

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 2018
Images	11 740 173	1 350 684 soit 11,5 %
Vidéos	81 440	5 182

À titre d'illustration en 2018, le CNAIP a pu identifier une victime grâce à l'exploitation des alertes de la base ICSE d'Interpol. Lors de l'exploitation du matériel informatique d'un prédateur sexuel, les autorités belges ont découvert du contenu pornographique mettant en scène des mineurs, dont un paraissait résider en France. La victime était identifiée par la gendarmerie française dans la région Grand-Est.

Le CNAIP participe, pour la France, à la « ***Victim Identification Task Force*** », une force d'intervention qui a été mise en place depuis 2014 sous l'égide d'Europol et Interpol. Regroupant 27 experts internationaux pendant deux semaines à Europol, elle procède à l'identification de victimes et d'auteurs à partir de données transmises à Europol par tous les pays impliqués dans cette lutte (volume de 32 millions d'images et vidéos). À ce jour, cette « ***Task Force*** » a permis d'identifier 241 victimes et 94 agresseurs dans 28 pays. Au cours de la cinquième session annuelle, une victime française résidant les Hauts-de-France a été identifiée en octobre 2018 par un expert du CNAIP.

Depuis 2017, le CNAIP a participé à une opération coordonnée par Interpol et Europol aux fins d'identifier et d'interpeller l'utilisateur d'un forum du *Darknet*. Celui-ci mettait régulièrement en ligne de nouvelles photos et vidéos de viols d'enfants de moins de 5 ans. Le violeur d'enfants a été formellement identifié et localisé au Portugal. Lors de son interpellation en juin 2017 par les autorités portugaises, le violeur multi-réitérant était en possession de divers objets mis en évidence parmi les publications postées sur le forum du *Darknet*. De manière incidente dans ce dossier, un Français a été identifié pour détention et diffusion d'images pédopornographiques. Il a été interpellé à la suite de l'enquête conjointe du C3N et de la section de recherche de Cayenne, en janvier 2018.

2.2.3.7 « Cyberinfluence » et atteintes à la démocratie

Les manipulations de l'information, ingérences étrangères

Les manipulations de l'information ne sont pas un phénomène nouveau. Leur actualité récente est liée à la combinaison de deux facteurs : d'une part, les capacités inédites de diffusion rapide et de viralité offertes par Internet et les réseaux sociaux ; couplées, d'autre part, à la crise de confiance que vivent les démocraties et qui dévalue la parole publique allant jusqu'à relativiser la notion même de vérité[96].

Les élections présidentielles américaine de 2016 et française de 2017, et l'organisation des élections européennes, ont convaincu les pouvoirs publics et les instances européennes qu'il fallait s'impliquer davantage sur ce phénomène. En réaction aussi, les plateformes Internet ont consenti des efforts de mobilisation.

Il y a manipulation de l'information lorsque trois critères cumulatifs sont réunis : une campagne orchestrée, une diffusion massive de nouvelles fausses ou biaisées, et un objectif politique préétabli et hostile.

Au plan européen, le 21 septembre 2018, la Commission a présenté une communication intitulée « Garantir des élections européennes libres et équitables », promouvant un environnement en ligne plus transparent, fiable et responsable, notamment par la publication d'un code de bonnes pratiques contre la désinformation en ligne. Ce code prévoit des mesures concrètes qui seront mises en œuvre par les plateformes signataires

(96) « Les manipulations de l'information, un défi pour nos démocraties », rapport du Centre d'analyse, de prévision et de stratégie (CAPS, ministère de l'Europe et des Affaires étrangères) et de l'Institut de recherche stratégique de l'École militaire (IRSEM, ministère des Armées).

(Google, Facebook, Twitter) pour lutter contre la désinformation. Par exemple, les plateformes en ligne doivent augmenter la transparence de la publicité à caractère politique, proposer des formations aux groupes politiques et aux autorités électorales et intensifier leur coopération avec les vérificateurs de faits *(fact-checker)*. La Commission a par ailleurs présenté le 5 décembre 2018 un plan d'action contre la désinformation.

La méthode *« astroturfing »*

L'*astroturfing* est une méthode de manipulation des tendances sur les réseaux sociaux à travers plusieurs vecteurs visant à créer artificiellement un sentiment de mobilisation populaire.

Cette technique repose principalement sur la manipulation du comportement de relais d'opinions. Pour ce faire, plusieurs faux comptes (qu'il s'agisse d'un réseau de *bots,* de multiples faux comptes, ou de militants) interpellent sur les réseaux sociaux des journalistes ou leaders d'opinion afin, en s'appuyant sur des biais cognitifs (il s'agit, ici, de faire croire à une personne qu'une information est validée car largement partagée par son environnement), de les pousser à relayer leur message. Une fois le mouvement amorcé par les premiers partages de la fausse information, des influenceurs donnent un « verni de réalité » aux publications. La fausse information/opinion est ensuite relayée par ses abonnés, afin de faire accroire un mouvement populaire spontané. L'information sera reprise par les médias (soit pour démentir ou pour retransmettre), une fois qu'une certaine résonance aura été atteinte, marquant la réussite de la campagne d'*astroturfing* (l'objectif étant de diffuser le plus largement une opinion ou fausse information).

Incitations à l'émeute et appels à la violence

Sur les réseaux sociaux, des incitations à l'émeute et des appels à la violence contre les personnes et les biens ont été lancés en octobre 2018 dans le cadre du **mouvement de « la purge ».** Un individu a été interpellé par la sûreté départementale du Rhône (69) pour avoir relayé, après l'avoir modifiée, la vidéo Snapchat #LaPurge en l'adaptant au contexte lyonnais. Il a été écroué à l'issue de sa garde à vue.
L'auteur d'un post sur le réseau social Twitter et revendiquant d'être à l'origine de la vidéo Snapchat a également été interpellé par la sûreté départementale de la DDSP de l'Isère (38).

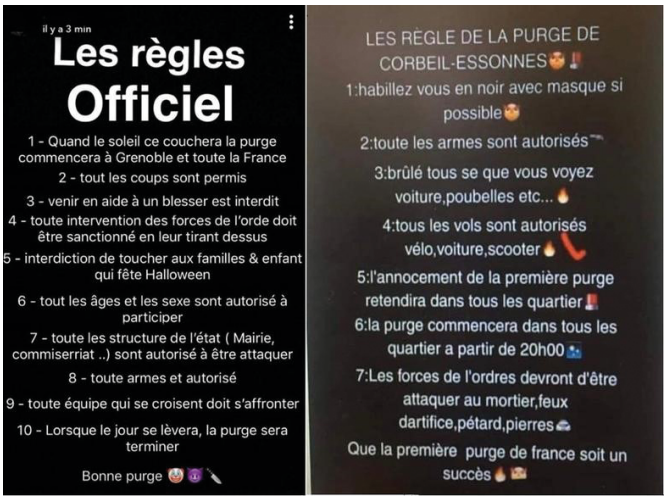


Figure 17 : Les règles de « la purge »
http://www.lefigaro.fr/actualite-france/2018/10/31/01016-20181031ARTFIG00144-purge-contre-les-policiers-l-auteur-presume-juge-le-28-novembre.php

2.3. Perception de la menace

Réalisée par les éditeurs de solutions de sécurité, la mesure de la menace cyber peut être discutée et parfois manquer d'objectivité. En effet, ceux-ci pourraient avoir tendance, dans un contexte concurrentiel, à souligner de façon exagérée les risques encourus par leurs clients ou des prospects. Mais surtout, leur mesure peut être faussée par la répartition de leur clientèle dans les différentes régions du monde.

Par ailleurs, le fait que les victimes d'actes de cybercriminalité déposent peu de plaintes auprès des forces de l'ordre induit des statistiques ministérielles inférieures à la réalité ; cela 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

Faute de définition juridique de la cybercriminalité[97], il n'est pas possible de recenser de manière précise et exhaustive les infractions relevant de cette notion, qui relève avant tout du mode opératoire. Ainsi le périmètre de la cybercriminalité comprend nécessairement les atteintes aux systèmes de traitement automatisé de données (S.T.A.D.) des articles 323-1 et suivants du Code pénal. Il peut recouvrir aussi :

> un certain nombre d'infractions de droit commun spécifiquement aggravées par la circonstance de commission via un réseau de communications électroniques ;

> plusieurs atteintes aux droits de la personne résultant des fichiers ou traitements informatiques ;

(97) Cf. Rapport sur la cybercriminalité, du groupe de travail interministériel présidé par le Procureur général Marc Robert, février 2014 - pages 10 à 19.

> de très nombreuses infractions de droit commun commises avec une dimension de cybercriminalité dans le mode opératoire ou le moyen ayant permis d'approcher la victime : recel, fraude, escroqueries…

Les fonctionnaires de police et les militaires de la Gendarmerie nationale reçoivent les plaintes des victimes d'infractions cyber en application de l'article 15-3 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 conçu pour mesurer 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 (SCRIBE).

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.

Diminution du nombre d'atteintes aux systèmes de traitement automatisé de données (STAD) déclarées en 2018 (SSMSI)

Le suivi des infractions d'atteintes aux systèmes de traitement automatisé de données a été amélioré en 2018[98], il permet d'en identifier davantage. Les tendances constatées restent inchangées.

Au cours de l'année 2018, la police et la gendarmerie ont enregistré 9970 infractions d'atteintes aux S.T.A.D., soit une moyenne de 830 infractions par mois. Ce niveau se situe en baisse par rapport à 2017 (-6,6 %) et à 2016 (-9,8 %). Il convient de mentionner que cette tendance statistique est difficilement interprétable en raison d'un faible taux de plaintes pour ce phénomène.

(98) Suite à des travaux exploratoires, il est apparu que de nombreuses infractions échappaient au traitement, notamment en GN. Les données corrigées 2016/2017/2018 sont différentes en niveau, mais pas en tendance.

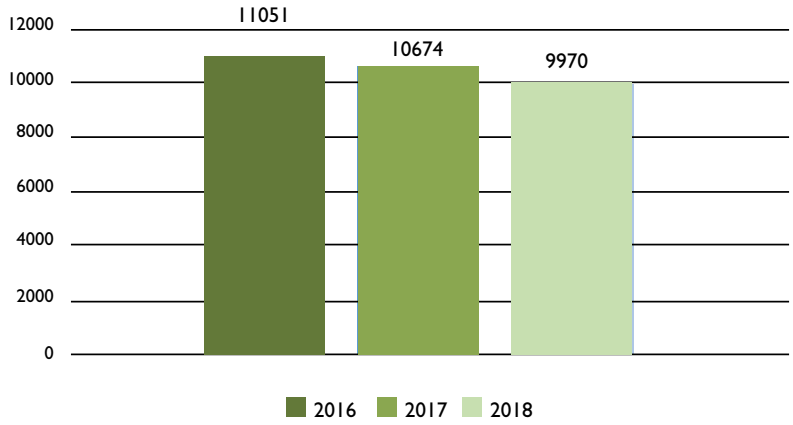


Figure 18 : Atteintes aux STAD – Évolution du nombre d'infraction déclarées
Sources : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie
Agrégat 101 - Dates de regroupement : date PN : date d'ouverture -- date GN : date de première validation BDRIJ
NB : Suite à des travaux exploratoires, il est apparu que de nombreuses infractions échappaient au traitement, notamment en GN. Les données corrigées 2016/2017/2018 sont différentes en niveau, mais pas en tendance.

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

Les accès frauduleux représentent en 2018 toujours la grande majorité des atteintes aux S.T.A.D. (71 %) ; ils sont toutefois en baisse (-14 %). Viennent ensuite les atteintes aux données (22 % du contentieux) qui sont en hausse de 21 % par rapport à 2017. Les altérations et entraves au fonctionnement (6 % du contentieux) sont en hausse (+12 %) après une baisse significative l'année passée. Les infractions de détention de moyens d'atteinte aux S.T.A.D. sont stables (1 % du contentieux). Très peu de détentions non autorisées de dispositif technique de captation de données informatiques ont été constatées en 2018 par les forces de police et gendarmerie (29), à un niveau quasi-identique à celui de 2016 et 2017.

Catégorie d'infractions	Année 2016	Part en 2016	Année 2017	Variation 2017/2016	Part en 2017	Année 2018	Variation 2018/2017	Part en 2018
1 - Accès ou extractions frauduleuses	8 125	*74 %*	8 194	1 %	77 %	**7 068**	- 14 %	**71 %**
2 - Altération ou entrave au bon fonctionnement	718	*6 %*	494	- 31 %	5 %	**555**	12 %	**6 %**
3 - Atteintes aux données	2 031	*18 %*	1 839	- 9 %	17 %	**2 223**	21 %	**22 %**
4 - Détention de moyens	177	*2 %*	147	- 17 %	1 %	**124**	- 16 %	**1 %**
Total général	11 051	*100 %*	10 674	- 3 %	100 %	**9 970**	- 7 %	**100 %**

Figure 19 : Atteintes aux S.T.A.D. – Nombre et part d'infractions par catégorie
Source : SSMSI- Base des crimes et délits enregistrés par la police et la gendarmerie.
Champ : France – PN : dates d'ouverture GN : date de première validation BDRIJ
NB : Suite à des travaux exploratoires, il est apparu que de nombreuses infractions échappaient au traitement, notamment en GN. Les données corrigées 2016/2017/2018 sont différentes en niveau mais pas en tendance.

Pour en savoir plus :

INSEE –INHESJ/ONDRP – SSMSI Rapport d'enquête cadre de vie et sécurité Décembre 2018, https://www.interieur.gouv.fr/Interstats/Actualites/Rapport-d-enquete-cadre-de-vie-et-securite-2018

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

Autres infractions déclarées en 2018 (SSMSI)[99]

Les **atteintes au secret des correspondances émises par voie électronique** constatées en 2018 s'établissent à 390, en légère baisse de 2,5 % par rapport à 2017.

Selon l'art. 434-15-2 du Code pénal, est puni de trois ans d'emprisonnement et de 270 000 euros d'amende le fait, pour quiconque ayant connaissance de la convention secrète de **déchiffrement d'un moyen de cryptologie** susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de la remettre aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités.

L'obligation de remettre aux autorités judiciaires une convention secrète de déchiffrement cryptologique a été jugée conforme à la Constitution. En effet, dans une décision rendue sur question prioritaire de constitutionnalité, le Conseil constitutionnel a précisé que l'obligation de fournir une convention secrète de déchiffrement ne contrevient pas au droit de garder le silence (décision n° 2018-696 du 30 mars 2018).

En 2018, les forces de police et gendarmerie ont relevé plus de 430 infractions de refus de remettre aux autorités judiciaires ou de mettre en œuvre la convention secrète de déchiffrement d'un moyen de cryptologie, chiffre qui a été multiplié par cinq par rapport à 2017.

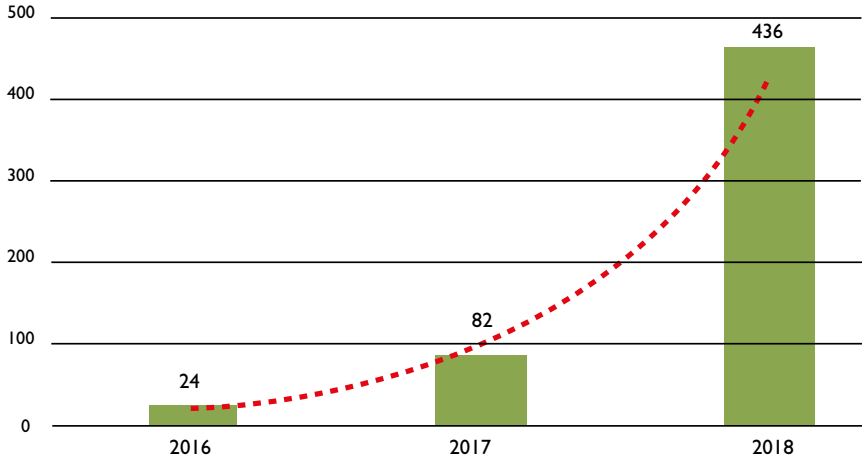


Figure 20 : Clés de chiffrement. – Nombre de refus relevé
Sources : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie

(99) *Ces statistiques correspondent aux infractions enregistrées par les forces de l'ordre. Les évolutions constatées doivent être interprétées avec précaution. En effet, elles peuvent ne pas correspondre à l'évolution de la cyberdélinquance réelle mais à une modification du processus déclaratif des victimes (variation du taux de plainte) ou encore à un changement des pratiques de classement des infractions par les forces de l'ordre.*

Le nombre de **harcèlements au moyen d'un service de communication en ligne**[100] **a doublé** entre 2016 et 2018. Les mineurs représentent 19,6 % des victimes en 2018.

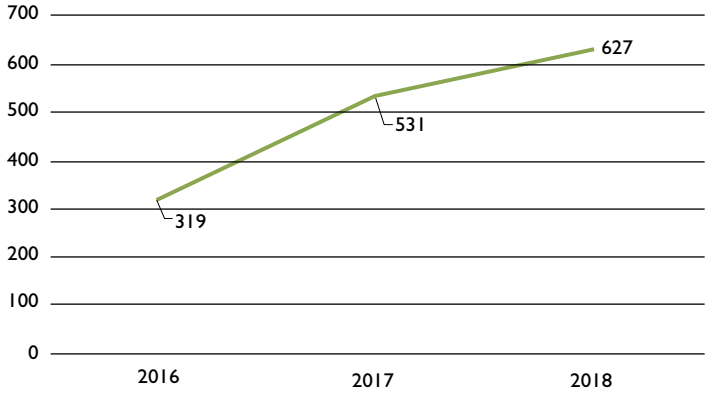


Figure 21 : Harcèlements au moyen d'un service de communication en ligne
Sources : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie

Au niveau des **mises en péril des mineurs,** 4 catégories d'infractions sont spécifiquement de nature cyber, le fait que l'infraction soit commise par l'utilisation d'un service de communication au public en ligne constituant une circonstance aggravante. Il s'agit des propositions sexuelles faites à un mineur de moins de 15 ans par un majeur utilisant un réseau de communication électronique, suivies ou non d'une rencontre ; des atteintes sexuelles sur un mineur de moins de 15 ans par un majeur mis en contact avec la victime par un réseau de communication électronique et enfin de corruption de mineur par une personne mise en contact avec la victime par un réseau de communication électronique.

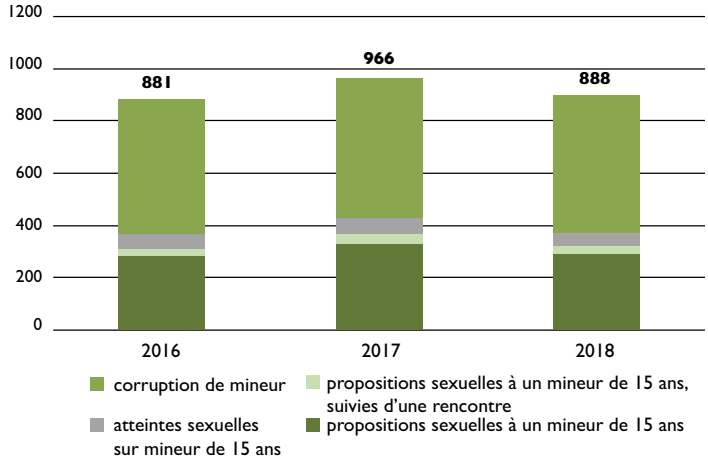


Figure 22 : Mises en péril des mineurs spécifiques cyber. – Nombre d'infractions
Sources : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie.

(100) par des propos ou comportements répétés ayant pour objet ou effet une dégradation des conditions de vie altérant la santé d'une personne.

Même si ces infractions baissent en 2018, elles restent d'un niveau élevé. Elles sont matérialisées pour la plupart, par l'action des services opérationnels, qui mettent en œuvre des techniques d'enquêtes sous pseudonyme sur les réseaux (cf. § 1.3).

Infractions à la loi « Informatique et Libertés » : Évolution sur 3 ans (2016-2018)

Ces infractions présentent un caractère générique ; si elles ne peuvent pas toutes être considérées comme relevant de la cybercriminalité, elles sont avant tout relatives à des traitements de données numériques.

Le nombre d'infractions à la loi Informatique et Libertés, stable en 2016 et 2017, est en hausse en 2018 (+14 %), année de l'entrée en vigueur du RGPD.

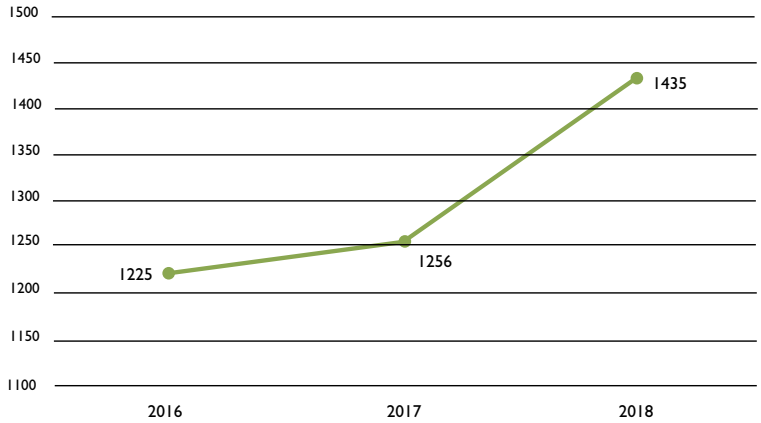


Figure 23 : Infractions à la loi informatique et libertés. – Nombre d'infractions
Sources : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie

Quatre catégories représentent la quasi-totalité de ces infractions en 2018 :

> la **divulgation illégale** volontaire et nuisible **de données à caractère personnel :** 408 infractions, soit 28,4 % ;

> l'**absence de sécurisation de l'accès** aux services de communication au public en ligne (Internet) et négligence caractérisée : 359 infractions, soit 25 % ;

> la **collecte de données** à caractère personnel **par un moyen frauduleux,** déloyal ou illicite : 268 infractions, soit 18,7 % ;

> le **détournement de la finalité d'un traitement** de données à caractère personnel : 230 infractions, soit 16%.

Vision statistique des infractions constatées par la 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. Cette remontée s'effectue 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

En 2018, le nombre de plaintes traitées par la Gendarmerie pour des infractions relevant du champ[101] cyber a augmenté **de plus de 7 % pour atteindre près de 67 890 faits.** Ainsi il est relevé une augmentation plus modérée qu'en 2017 (hausse de 32 % par rapport à 2016).

La part des escroqueries dans les infractions cyber demeure largement majoritaire et représente 73 % du phénomène cyber en gendarmerie. Deux phénomènes saisonniers et récurrents à la matière sont observés :

> les escroqueries à la location de courte durée pour les vacances scolaires, (notamment estivale et d'hiver) ;

> la période de Noël propice aux escroqueries en tout genre : petites annonces, faux sites, ventes de produits contrefaits, *phishing* « Remboursement des Impôts »

Par ailleurs, malgré l'apparition de nouveaux vecteurs, les modes opératoires demeurent globalement inchangés. Ils reposent encore massivement sur des campagnes de *phishing,* le recours à des techniques d'ingénierie sociale et d'usurpation d'identité.

Répartition des infractions cyber les plus représentées

Une analyse des dix natures d'infraction les plus utilisées dans les comptes rendus permet d'élaborer une clé de répartition des infractions Cyber en gendarmerie.

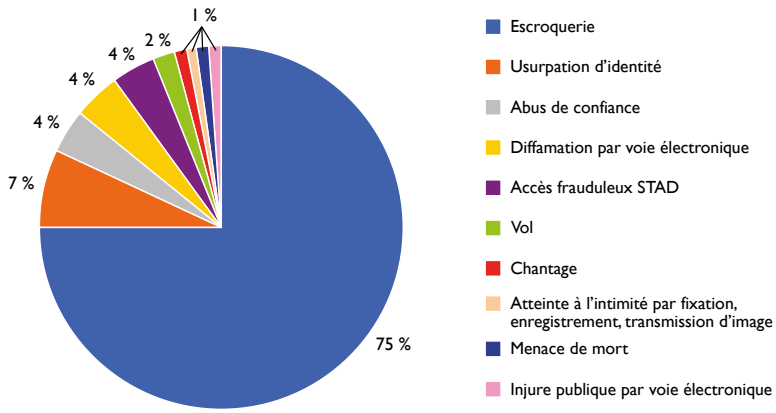


Figure 24 : Répartition CRPJ Cyber en 2018 – Source : GN – C3N

(101) *Sont ici considérées comme hors champ cyber, les infractions de corruption ou d'agression de mineurs après mise en contact par un réseau de communications électroniques, ainsi que celles liées à la pédopornographie (consultation, enregistrement, détention ou diffusion d'images).*

Vision statistique des infractions constatées par la Préfecture de Police

L'infocentre Orus de la Préfecture de Police de Paris fournit les données statistiques sur les plaintes liées à la cybercriminalité, pour les deux directions concernées, la direction de la sécurité de proximité de l'agglomération parisienne (DSPAP) et la direction régionale de la police judiciaire [102] (DRPJ).

Ventilation des infractions traitées en 2018	DSPAP	DRPJ	Total
Atteintes aux STAD	1 390	331	1 721
Escroqueries en ligne (dont CB)	289	380	669
Autres infractions en ligne (hors STAD & Escroqueries)	690	180	870
	2 369	891	3 260

Figure 25 : Ventilation des infractions traitées par la Préfecture de Police de Paris en 2018

Les atteintes aux STAD représentent 52 % des infractions catégorisées cyber à la Préfecture de Police et les escroqueries 20%. Parmi les 870 autres infractions en lignes relevées, 388 plaintes (12% du total) sont en lien avec des mineurs victimes[103] (12% au total) et 236 autres plaintes portent sur des faits de cyber-harcèlement ou d'appels malveillants (7% du total). Enfin, sont avérés :

> 38 cas d'atteintes aux secrets de correspondances émis par voie électronique ;
> 39 cas de collectes de données personnelles par un moyen frauduleux, déloyal ou illicite ;
> 33 cas de détournements de données personnelles ;
> 23 cas d'apologie du terrorisme en ligne.

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

La plateforme PHAROS de l'OCLCTIC exploite les signalements émis sur le site www.internet.signalement.gouv.fr par des internautes et des professionnels du numérique, qui constatent des comportements ou des contenus publics de l'Internet qu'ils estiment illégaux. En 2018, les policiers et gendarmes de PHAROS ont reçu et traité 163 723 signalements (contre 153 583 en 2017, soit +6,6 %).

(102) La DRPJ traite la cybercriminalité avec principalement ses brigades spécialisées : BEFTI, BRDA (délinquance astucieuse), BFMP (moyens de paiement), BRDP (délinquance sur la personne) et BPM (mineurs).

(103) 29 cas de corruption et 7 d'agressions de mineurs après mise en contact par un réseau de communications électroniques, le restant portant sur des faits de consultation, d'enregistrement, de détention ou de diffusion d'images pédopornographiques.

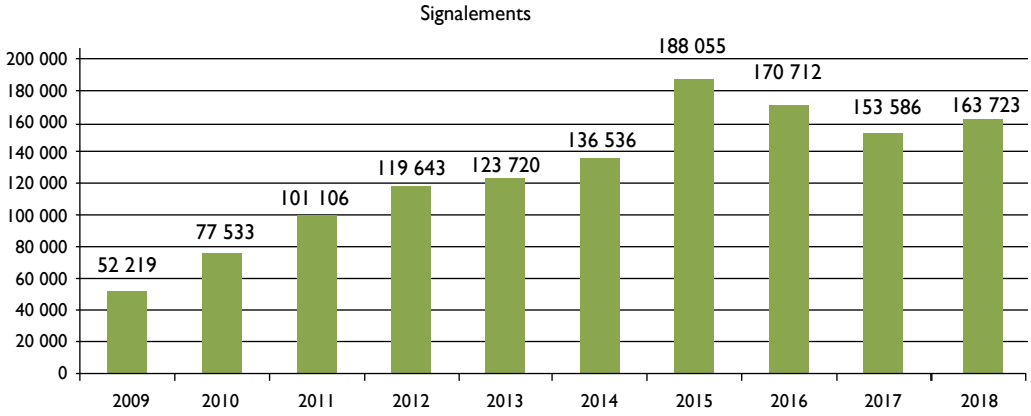


Figure 26 : Évolution du nombre de signalements à la plateforme Pharos

En 2018, la typologie des signalements est la suivante :

> 90 190 signalements dans le domaine des escroqueries et extorsions, soit 55,1 % des signalements (51,2 % en 2017) ;
> 20 547 dans le domaine des atteintes aux mineurs (pédopornographie, prédation sexuelle…), soit 12,6 % des signalements (13,1 % en 2017). 5 926 contenus ont été envoyés aux partenaires étrangers via Interpol, du fait d'éléments situés hors de France (serveurs d'hébergement d'images pédopornographiques ou adresses IP des internautes) ;
> 14 332 signalements dans le domaine des discriminations, soit 8,8 % des signalements (8,6 % en 2016) ;
> et 4 567 signalements dans le domaine de l'apologie et de la provocation à des actes terroristes, soit 2,8 % des signalements (4,1 % en 2017).

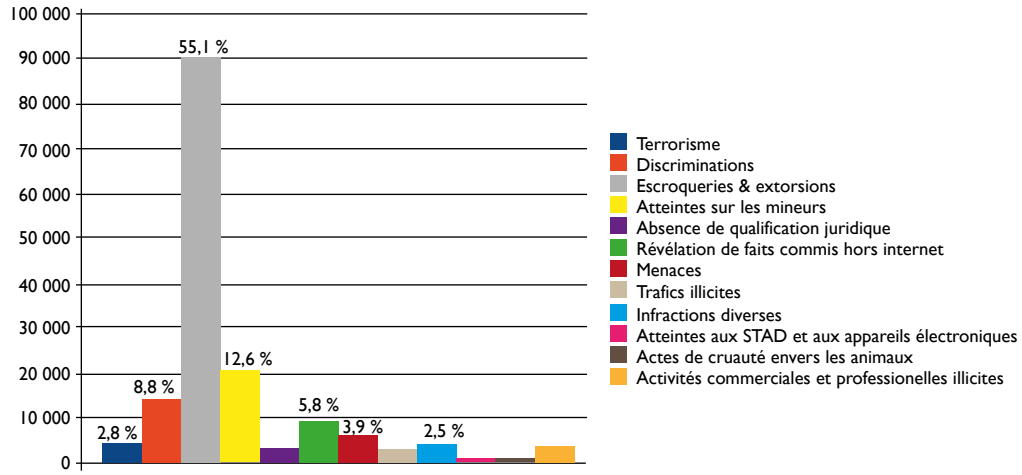


Figure 27 : Répartition des signalements PHAROS par catégorie.

18741 demandes de retrait (-41 % par rapport à 2017), 1644 demandes de blocage (+120 %) et 8528 demandes de déréférencement (+220 %) ont été adressées aux professionnels de l'Internet au cours de l'année[104], en application de l'article 6-1 de la LCEN. Pour les mesures de blocage, ce sont 2811000 connexions à des pages pédopornographiques et 23280 connexions à de la propagande terroriste qui ont été empêchées.

L'approche partenariale développée avec le secteur privé et les associations (en particulier l'association « Point de Contact » et « Signal Spam ») a permis de renforcer les signalements, pour constituer près de 4 % de la totalité des signalements reçus.

2.3.1.3 Activité de la plateforme Perceval

Le lancement de PERCEVAL a été annoncé publiquement le 6 juin 2018 par le ministre de l'Intérieur. Cette plateforme accessible au grand public en ligne, via service-public.fr, vise à recueillir et analyser le contentieux massif des **usages frauduleux de carte bancaire.**

État des signalements enregistrés (10 mois)

PERCEVAL a recueilli plus de 100000 signalements, représentant plus de 400000 usages frauduleux[105] depuis l'ouverture du téléservice ; soit une moyenne de 310 signalements par jour depuis la création de la plateforme. Depuis novembre 2018 plus de 450 signalements par jour sont effectués sur la plateforme, confirmant une progression en constante augmentation.

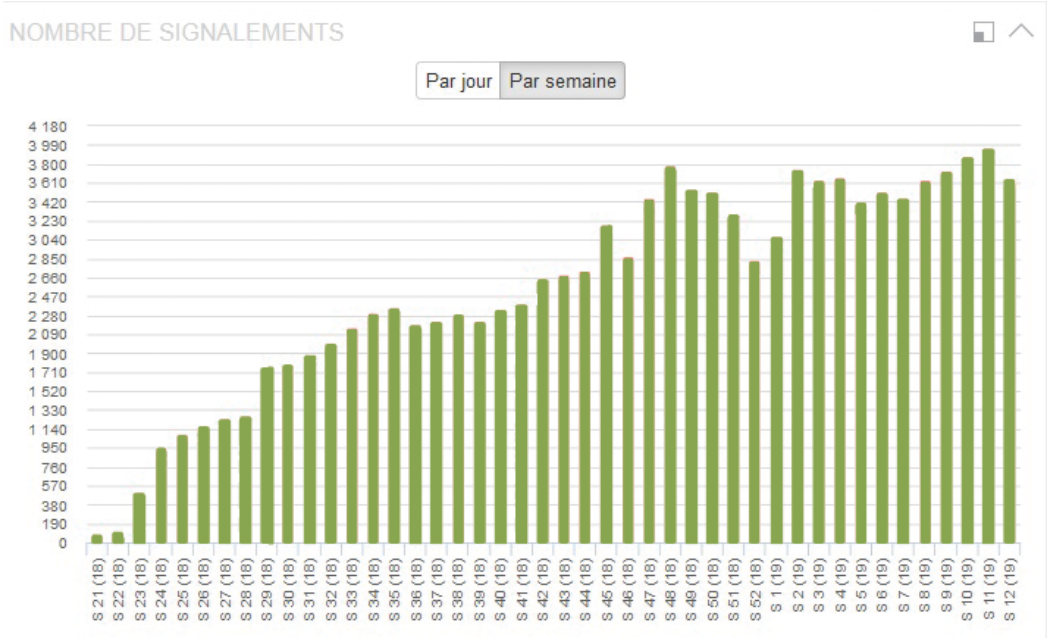


Figure 28 : Évolution des signalements Perceval entre juin 2018 et mars 2019

(104) En ce qui concerne les images pédopornographiques, PHAROS a adressé en 2018 : 7.717 demandes de retrait, 3.699 demandes de déréférencement et 393 demandes de blocage.

(105) Un internaute signale près de 4 usages frauduleux en moyenne par signalement effectué sur Perceval.

Le préjudice moyen par signalement est de 480 €. Plus de 4 500 signalements portent sur un préjudice supérieur à 1 500 €. Le préjudice total rapporté dans PERCEVAL est évalué à plus de 55 millions d'euros.

Selon l'Observatoire sur la sécurité des moyens de paiement (OSMP), 3,48 millions de paiements à distance frauduleux étaient recensés pour l'année 2017, avec un préjudice total de 234,2 millions d'euros. Ainsi en comparaison avec ces données et rapporté à la durée de fonctionnement du téléservice, PERCEVAL parvient à collecter près d'un sixième des signalements d'usagers et près d'un tiers du préjudice identifié par les acteurs économiques. En ce sens, cela atteste d'une bonne identification de l'outil par le public.

Activité judiciaire issue de la plateforme PERCEVAL au 31/12/2018

Les données collectées par la plateforme PERCEVAL sont analysées par les enquêteurs du service central de renseignement criminel (SCRC) de la Gendarmerie à Pontoise. De nombreux recoupements et rapprochements ont conduit à l'ouverture de 55 enquêtes auprès du parquet de Pontoise (95) et l'envoi de 285 réquisitions.

Sur ces 55 enquêtes judiciaires :

> 27 ont déjà été ventilées aux parquets compétents au regard du lieu de livraison de la marchandise achetée frauduleusement et/ou de l'identification des mis en cause ;

> 28 dossiers sont encore en cours d'exploitation au sein du département délinquance économique et financière du SCRC.

L'enquête la plus significative a permis l'identification de plusieurs auteurs pour un préjudice cumulé supérieur à 100 000 €. Plus de 15 victimes ont signalé les faits de détournement de carte bancaire dans PERCEVAL, dans cette affaire.

2.3.1.4 Activité de la plateforme d'assistance aux victimes de cybermalveillance

Porté par une démarche interministérielle, le dispositif national d'assistance est accessible depuis octobre 2017 au travers de la plateforme *cybermailveillance.gouv.fr.* Il est animé par le groupement d'intérêt public (GIP) Action contre la cybermalveillance (ACYMA), dans lequel le ministère de l'Intérieur est fortement impliqué au côté de l'ANSSI (voir § 3.4.5 pour une description complète).

En 2018, la plateforme a assisté près de 29 000 victimes (85 % de particuliers, 12,6 % d'entreprises et 2,4 % de collectivités).

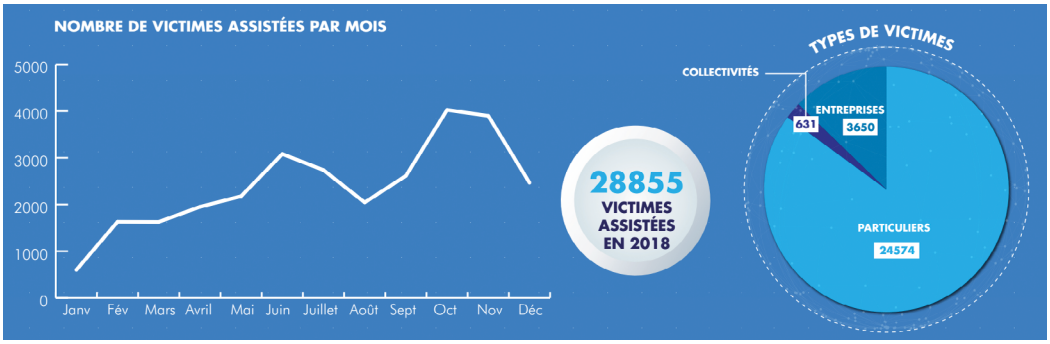


Figure 29 : Victimes recensées par le dispositif ACYMA

Au travers des informations recueillies, l'hameçonnage, les virus (dont les rançongiciels) et les pourriels *(spam)* sont les trois menaces figurant parmi les quatre les plus importantes. Ce tableau est complété par le piratage de compte s'agissant des particuliers, les intrusions sur les serveurs s'agissant des entreprises et les défigurations de sites s'agissant des collectivités.

Le dispositif permet de détecter rapidement des phénomènes émergents. Début février 2019, le dispositif a constaté une forte recrudescence des campagnes d'arnaques au chantage à la webcam (prétendue piratée - cf. § 2.2.3.2) avec des pics hebdomadaires de plus de 7 000 victimes assistées sur ce sujet (semaines 6 et 7). Un message de prévention a été immédiatement diffusé et le site a été modifié afin de prendre en compte cette nouvelle menace.
Durant le premier trimestre 2019, la plateforme a accompagné plus de 38 000 victimes (contre près de 29 000 pour toute l'année 2018). Le dispositif a ainsi assisté plus de 70 000 victimes depuis son lancement.

2.3.2 Vision des cybermenaces par les services du ministère de la Justice

Le travail des forces de police et de gendarmerie alimente l'activité des juridictions.
Le système statistique du ministère de la Justice ne permet pas de déterminer des variables de mode opératoire, et donc d'isoler au sein du vaste ensemble des infractions de droit commun, celles qui peuvent relever de la cybercriminalité.
Il est en revanche possible de repérer les infractions spécifiques, soit les infractions d'atteintes aux STAD ou en lien avec le traitement de fichiers dans les condamnations, soit en raison d'une circonstance aggravante spéciale.
Dès lors, les données chiffrées afférentes à la cybercriminalité apparaissent nécessairement très en deçà de la réalité que cette notion recouvre, en particulier dans la mesure où elles ne rendent pas compte des infractions financières commises en ligne.
Deux sources produites par la sous-direction des statistiques et des études (SDSE) du secrétariat général du ministère de la Justice permettent de décrire l'activité judiciaire :

> le système d'information décisionnelle (SID) construit à partir des données présentes dans le logiciel Cassiopée[106] expose les flux d'affaires enregistrées puis orientées par les parquets ;

> les tables construites à partir du casier judiciaire national permettent de détailler précisément les décisions (condamnations et compositions pénales) définitives prononcées par les juridictions pénales, à l'exception des relaxes et des acquittements.

Chacune de ces sources permet de décrire des phases différentes de l'activité judiciaires et livrent des informations complémentaires ; les données du ministère de l'Intérieur portent par ailleurs sur la phase de constatation des infractions et d'élucidation, en amont de la saisine de l'autorité judiciaire.

(106) Logiciel d'enregistrement et de traitement des affaires pénales.

Les données :

> Affaires nouvelles et orientées par les parquets pour des infractions d'atteintes aux STAD

Entre 2013 et 2017, les affaires nouvelles ont plus que doublé (x2,4).

Entrée ou maintien irrégulier dans un système informatique et dégradation, destruction ou vol de données ou de fichiers informatiques	2013	2014	2015	2016	2017
Affaires nouvelles	3246	4260	6572	8194	7925

Source : Ministère de la Justice/SG/SEM/SDSE/ SID-Cassiopée – Traitement DACG-PEPP

> Affaires nouvelles et orientées par les parquets pour des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques

Entre 2013 et 2017, les affaires nouvelles portant sur les atteintes à la protection des données à caractère personnel sont orientées à la baisse, après avoir connu un pic en 2014.

Atteinte à la protection des données à caractère personnel	2013	2014	2015	2016	2017
Affaires nouvelles	2050	2830	2437	2274	1785

Source : Ministère de la Justice/SG/SEM/SDSE/ SID-Cassiopée – Traitement DACG-PEPP

> Condamnations prononcées pour des infractions spécifiques à la cybercriminalité

Entre 2013 et 2017, les condamnations pour des infractions d'atteintes aux STAD ont augmenté de 56 %. Les premières condamnations pour atteinte à la vie privée apparaissent en 2017, de même que celles pour harcèlement moral à partir de 2014. Plus de 550 condamnations par an ont été prononcées ces dernières années pour des faits de propositions sexuelles à mineur de 15 ans ou pédopornographie avec l'utilisation d'un réseau de communication électronique.

Infractions	Textes principaux	Infractions ayant donné lieu à condamnations				
		2013	2014	2015	2016	2017*
Atteintes aux STAD	Articles 323-1 à 323-8 du Code pénal	141	191	275	220	221
Atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques	Articles 226-16 à 226-24 du Code pénal	45	50	63	68	72
Atteinte au secret des correspondances électroniques	Article 226-15 alinéa 2 du Code pénal	15	21	30	27	15
Envois réitérés de messages malveillants par réseau de communications électroniques	Article 222-16 du c Code pénal		2	39	151	240
Atteinte à la vie privée (diffusion d'images ou paroles à caractère sexuel sans le consentement de la personne)	Article 226-2-1 alinéa 2 du Code pénal					20
Viol avec mise en contact par réseau de communications électroniques	Article 222-24 8° du Code pénal	3	3	5	5	3
Agression sexuelle avec mise en contact par réseau de communications électroniques	Article 222-28 6° du Code pénal	4	5	8	5	7
Atteinte sexuelle avec mise en contact par réseau de communications électroniques	Article 227-26 4° du Code pénal	27	25	18	23	20
Harcèlement moral au moyen d'un réseau de communications électroniques	Article 227-26 4° du Code pénal		1	5	7	8
Diffusion d'images de violences	Article 222-33-3 alinéa 2 du Code pénal	60	41	54	42	66
Corruption de mineur avec mise en contact par réseau de communications électroniques	Article 227-22 du Code pénal	99	84	107	115	135
Proposition sexuelle faite à un mineur de 15 ans au moyen d'un réseau de communications électroniques	Article 227-22-1 du Code pénal	87	109	132	119	115
Pédopornographie avec utilisation d'un réseau de communications électroniques	Article 227-23 alinéas 3 et 4 du Code pénal	499	375	370	439	444
Proxénétisme avec mise en contact par réseau de communications électroniques	Article 225-7 10° du Code pénal	43	62	73	43	43
Recours à la prostitution de mineur ou personne vulnérable avec mise en contact par réseau de communications électroniques	Article 225-12-2 2° du Code pénal	1		2	3	4
Diffusion de procédés destinés à la fabrication d'engins explosifs par réseau de communications électroniques	Article 322-6-1 alinéa 2 du Code pénal	2	1		2	1
Provocation ou apologie du terrorisme au moyen d'un service de communication en ligne	Article 421-2-5 alinéa 2 du Code pénal			40	78	79
Contrefaçon d'œuvres de l'esprit au moyen d'un service de communication au public en ligne	Articles L.335-2 à L.335-4 du Code de la propriété intellectuelle	1	5	7	9	7
	TOTAL	**1 027**	**975**	**1 228**	**1 356**	**1 500**

Source : Ministère de la Justice/SG/SEM/SDSE fichier statistique du Casier judiciaire national – Traitement DACG-PEPP
*données provisoires

2.3.3 Perception de la menace par les entreprises françaises

Comme l'année passée, le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) a produit en janvier 2019 une enquête intitulée « baromètre de la cyber-sécurité des entreprises »[107]. 174 entreprises[108] membres y ont participé.

La majorité des entreprises ont été touchées par des cyber-attaques : 80 % en ont constaté au moins une en 2018 (plus de 10 pour 32 %), respectivement + 1 point et + 4 points par rapport à 2017. Le nombre de cyber-attaques constatées tend toutefois à se stabiliser pour près d'une entreprise sur deux, par rapport à 2017.

Le *phishing* est le mode d'attaque le plus fréquent (73 %), étonnamment la fraude au président (FOVI) touche encore une entreprise sur deux en 2018. Le rançongiciel est cette année au troisième rang avec 44 % d'entreprises touchées, suivi par le *social engineering* (40 %).

Le *Shadow IT*[109] et les vulnérabilités résiduelles sont les cyber-risques auxquels les entreprises sont les plus exposées (plus de 60 % des entreprises répondantes).
98 % des entreprises estiment que la transformation numérique a une incidence sur la sécurité des systèmes d'information des données. En tête des enjeux : le recours massif au *Cloud,* utilisé par 87 % des entreprises, un mode de stockage qui pose des problèmes de non-maîtrise qui nécessite pour les responsables interrogés (RSSI) le recours à des outils de sécurisation supplémentaires à ceux proposés par le prestataire. De nombreux cas de piratage témoignent d'une progression de la cybercriminalité via les objets connectés. Pour l'IoT, la caractéristique la plus marquante reste les failles de sécurité présentes dans ces équipements.

Face à ces risques, de nombreuses solutions techniques sont implantées. Au-delà des antivirus, VPN, filtrage web et AntiSPAM, on note aussi l'adoption de solutions de protection fondées sur l'IA (56 % des répondants) et la souscription de plus en plus courante aux cyber-assurances. 50 % ont souscrit un contrat, soit +10 points / 2017.
Avec la prégnance des cyber-attaques, des investissements commencent à se sentir dans la part du budget IT consacrée à la sécurité, même si celle-ci reste faible (supérieure à 5 % pour 41 % des entreprises consultées).

*(107) **https://www.cesin.fr/fonds-documentaire-4eme-edition-du-barometre-annuel-du-cesin.html***
(108) Répartition : 11 % de moins de 250 salariés, 37 % entre 250 et 5 000, 35 % entre 5 000 et 50 000, 17 % de plus de 50 000 salariés.
(109) Mise en place et utilisation d'applications non approuvées par l'entreprise.

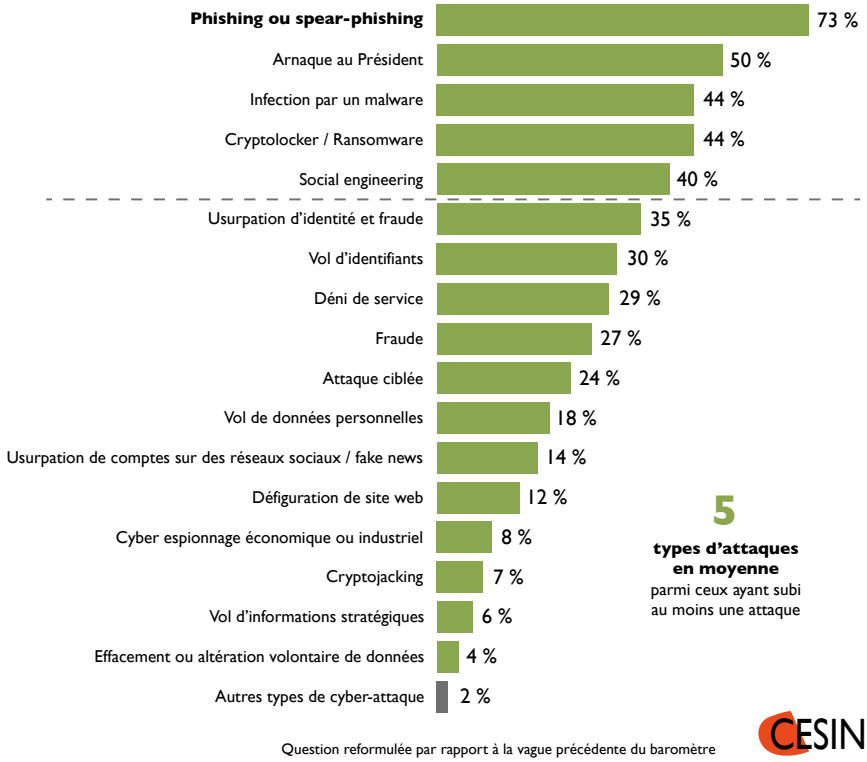


Figure 30 : Type d'attaques subies par les entreprises

Le constat du Club de sécurité de l'Information Français (CLUSIF) dans l'enquête « Menaces informatiques et pratiques de sécurité 2018 »[110] menée auprès de 350 entreprises de plus de 100 salariés, se distingue et relève quant à lui les taux suivants :

> 30 % ont subi une infection virale, provenant d'attaques non ciblées ;

> 29% ont été ciblées par des tentatives d'hameçonnage *(phishing)* ;

> 24% des entreprises consultées ont été victimes de tentatives d'extorsion ou de fraude au président (FOVI) ;

> 4% indiquent avoir été confrontées à du cyber-espionnage.

Le nombre d'entreprises ayant formalisé leur politique de sécurité de l'Information (PSSI) reste globalement stable, à 69 % ; ce pourcentage augmente avec la taille des entreprises. Une meilleure connaissance des actifs de l'entreprise induit une meilleure protection. Sur ce point, l'enquête révèle une croissance de plus de 10 points en deux ans de l'inventaire des actifs, passant à 85 % pour les inventaires au moins partiels et à 56 % pour les inventaires complets.

(110) ***https://clusif.fr/publications/menaces-informatiques-pratiques-de-securite-france-edition-2018-rapport/***

Selon l'étude du CESIN, les enjeux pour demain restent plus humains que techniques. Pour les responsables de la sécurité des systèmes d'information (RSSI), l'enjeu principal pour l'avenir de la cybersécurité est celui de la formation et de la sensibilisation des utilisateurs. La gouvernance de la cybersécurité doit également être placée au bon niveau. Malgré un impact positif de la mise en conformité RGPD sur la gouvernance des entreprises (59 %), la confiance en la capacité des COMEX à prendre en compte les enjeux de la cybersécurité est très inégale en fonction des secteurs d'activité. Enfin, la pénurie de ressources humaines en cybersécurité est un défi majeur pour les organisations.

2.3.4 Vision européenne proposée par Europol

Europol, dans son rapport sur l'évaluation de la cybercriminalité, paru en septembre 2018 (*Internet Organised Crime Threat Assessment* dit « *iOCTA* »), dégage les grandes tendances de la cybercriminalité dans l'Union européenne :

> la persistance des attaques par rançongiciels ou par déni de service distribué, qui peuvent être le fait d'États et non plus seulement d'individus ou de groupes relevant de la criminalité organisée. L'objectif poursuivi n'est plus exclusivement financier mais aussi de déstabilisation ;

> l'ingénierie sociale qui reste l'une des techniques cybercriminelles les plus utilisées ;

> Le développement des cryptomonnaies pour financer ou blanchir les revenus d'une activité criminelle et leur minage. Les logiciels malveillants de minage de cryptomonnaie ont été largement distribués par les cybercriminels en 2018 (cf. *cryptojacking*) ;

> un volume toujours plus important de contenus illicites sur Internet, notamment pédopornographiques (partagés de manière confidentielle et sur les *darknets,* qui demeurent des places de marchés cybercriminels malgré la fermeture des plus importants d'entre eux tels que Alphabay, Hansa et RAMP) et terroristes (diffusés à des fins de propagande notamment) ;

> des fraudes sans présence de la carte (*Card-No-Present* ou CNP) aujourd'hui courantes et un usage continu de la technique du *skimming*.

Une synthèse du rapport IOCTA 2018 figure en annexe.

2.3.5 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 :

> L'impact financier des incidents informatiques est encore mal connu et son évaluation est réalisée par moins de la moitié des entreprises (43 %) selon l'étude « Menaces informatiques et pratiques de sécurité » du CLUSIF 2018. Cette démarche est plus répandue dans les secteurs de la Banque-Assurance (63 %). Selon l'étude du CESIN (cf. infra), les cyber-attaques ont des impacts concrets dans 59 % des cas (+10 points / 2017) sur le *business* des entreprises touchées : ralentissement voire arrêt de la production, indisponibilité du site Internet, retard de livraison, perte de chiffre d'affaires (CA),...

> Pour les entreprises[111], 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, sachant que ce coût est plus élevé pour les industries fortement réglementées ;

(111) Étude Ponemon Institute pour IBM 2017 - ***https://www.ibm.com/security/infographics/data-breach//***

> Selon un sondage effectué auprès de 1 000 entreprises [112], 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 million d'euros pour une entreprise de plus de 5 000 salariés. Il existe également une disparité entre les différents secteurs d'activités ; les entreprises de services informatiques et les acteurs de la grande distribution, de la logistique et des transports doivent anticiper des pertes plus importantes en cas d'intrusion ;

> En novembre 2018, une étude sur la cybersécurité des PME françaises réalisée par l'IFOP [113] menée auprès de dirigeants de ce type d'entreprises, met en avant que près d'un quart des PME interrogées ont subi une attaque informatique dans l'année écoulée. Pour 64 % d'entre elles, cette attaque a entraîné un coût inférieur à 10 000 euros, mais pour 14 % d'entre elles ce coût était supérieur à 50 000 euros ;

> L'OSMP publie chaque année le volume précis des montants frauduleux, les préjudices étant portés selon les cas par les banques, les commerçants ou parfois les 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 467 millions d'euros en 2017 (dont 290,5 millions d'euros réalisés sur des transactions sur Internet), en baisse de 9,7 % par rapport à 2016 (après déjà une baisse d'1 % en 2016).

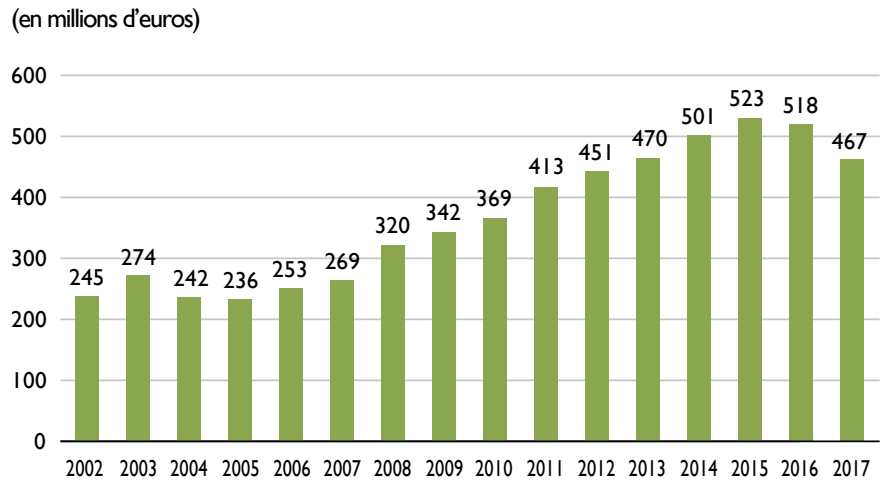


Figure 31 : Montant de la fraude sur les transactions traitées dans les systèmes français, cartes françaises et étrangères. Source : Observatoire de la sécurité des moyens de paiement.

(112) NTT Com Security, « Brèches de sécurité - quel est le coût réel pour votre business? », octobre 2016.

(113) Les PME face aux enjeux de sécurité informatique, Étude IFOP du 5 au 9 novembre 2018 de nature quantitative auprès de 702 décideurs, réalisée pour Kaspersky et Euler Hermes.

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[114] instituant un délégué ministériel aux industries de sécurité et à la lutte contre les cybermenaces (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. 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 Gouvernance

À l'occasion de son intervention au 10e Forum international de la cybersécurité (FIC) en janvier 2018[115], le ministre de l'Intérieur a confié à la DMISC le soin d'élaborer une « feuille de route cyber » en lien avec les directions opérationnelles et les services concernés du ministère. Il s'agissait de définir leur ambition partagée, visant à prévenir les cybermenaces, gérer les cybercrises et lutter contre la cybercriminalité.

Son élaboration s'inscrit dans un contexte de continuité. En effet, le ministère s'est engagé il y a déjà plusieurs années dans la lutte contre les cybermenaces, comme en témoignent la création d'une mission dédiée, intégrée dans la DMISC en 2017, et la réalisation de travaux préparatoires en 2014 et 2017[116]. Par ailleurs, le ministère de l'Intérieur a contribué à la rédaction de la Revue stratégique de cyberdéfense[117], confiée par le Premier ministre au secrétariat général de la défense et de la sécurité nationale (SGDSN) et publiée en février 2018.

Tout au long de l'année 2018, la feuille de route cyber a mobilisé l'ensemble des services du ministère : services opérationnels, secrétariat général, attachés de sécurité intérieure, etc., mais aussi des partenaires externes, institutionnels et privés.

Interne au ministère, ce rapport classifié est un document préparatoire destiné aux seules entités ayant besoin d'en connaître. Quelques données ont néanmoins été rendues publiques[118].

En premier lieu, la feuille de route expose l'état de la lutte contre les cybermenaces aujourd'hui et inclut une cartographie des ressources dédiées du ministère, ainsi qu'une étude comparative européenne et internationale. Plus de 8 600 personnels du ministère ont été formés dans le domaine cyber et sont répartis sur l'ensemble du territoire national : 80 % d'entre eux sont dans le réseau territorial. Ainsi, le ministère dispose d'un maillage territorial fort, tissé avec des compétences incontestables et décisives en cas de crise majeure.

Le document décrit également la projection de la lutte contre les cybermenaces à l'horizon 2022, à travers une vision prospective de la menace, mais aussi le recensement de la trajectoire des services et du ministère. Une politique innovante de ressources humaines est en cours de mise en place, à travers le recrutement de 800 agents supplémentaires, consacrés à la lutte contre les cybermenaces au sein de l'ensemble des directions opérationnelles, et à la sécurité des systèmes.

---

(114) ***https://www.legifrance.gouv.fr/eli/decret/2017/1/23/INTA1635805D/jo***

(115) ***https://www.interieur.gouv.fr/Archives/Archives-ministre-de-l-Interieur/Archives-Gerard-Collomb-mai-2017-octobre-2018/Interventions-du-ministre/Discours-du-ministre-au-Forum-international-de-la-Cybersecurite-2018***

(116) Il s'agit du plan d'action de lutte contre les cybermenaces en matière de sécurité intérieure du 28 mai 2014 et de la stratégie ministérielle de lutte contre les cybermenaces établie en janvier 2017 : ***https://www.interieur.gouv.fr/Archives/Archives-des-actualites/2017-Actualites/Lutter-contre-les-cybermenaces***

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

(118) ***https://www.interieur.gouv.fr/Le-secretaire-d-Etat/Interventions-du-secretaire-d-Etat/Intervention-de-Laurent-Nunez-au-11eme-Forum-International-de-la-Cybersecurite***

Enfin, cette démarche collaborative a conduit à l'élaboration de différents projets structurants et organisationnels. La feuille de route a fait l'objet d'une présentation au ministre de l'Intérieur qui en a validé les termes et notamment la nécessité de renforcer l'équipe DMISC.

3.2. 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.

3.2.1. Les actions de prévention

3.2.1.1 Grand public

Les services du ministère de l'Intérieur ont participé tout au long de l'année 2018, à de nombreux salons, rencontres et conférences, ouverts au public, au cours desquels les problématiques liées aux cybermenaces ont été abordées.

À l'échelle nationale, de nombreuses actions de sensibilisation aux cybermenaces sont conjointement mises en œuvre par le ministère et des associations. Peuvent être cités : le dispositif national d'assistance aux victimes d'actes de cyber malveillance[119], le Centre expert contre la cybercriminalité français[120] (CECyF), le site d'information sur les *botnets* Antibot[121], la plateforme de lutte contre les spams vocaux et sms 33 700[122], ainsi que les associations Signal Spam[123], Phishing Initiative[124], Point de contact[125] et e-Enfance[126]. Quotidiennement, la police et la gendarmerie délivrent des messages sur le site du ministère, ainsi que sur les réseaux sociaux (comptes officiels sur Facebook, Twitter et Instagram).

Au niveau local, les services du ministère de l'Intérieur accomplissent de nombreuses actions de prévention grâce à leur présence sur le territoire.

Deux publics sont particulièrement vulnérables et exposés aux cybermenaces : **les jeunes et les séniors.** Aussi, ces derniers font l'objet d'actions de prévention ciblées de la part du ministère. La jeunesse constitue un point de vigilance particulier : les enfants et les adolescents peuvent être autant auteurs d'actes répréhensibles sur Internet (harcèlement, diffamation, discrimination, etc.) que victimes (vol de données, pédopornographie, embrigadement, radicalisation, etc.).

Le milieu scolaire est bien sûr un relais optimal des actions de sensibilisation auprès des **enfants,** mais aussi de leurs **parents** et de leurs **enseignants.** Entre septembre 2017 et juin 2018, la gendarmerie a sensibilisé plus de 33 000 élèves du primaire, près de 190 000 élèves du secondaire, plus de 5 000 étudiants, plus de 7 000 parents et 11 000 membres du corps enseignant[127].

Il convient de rappeler le **succès de l'opération « Permis Internet »,** le programme national de prévention pour un usage d'Internet vigilant, sûr et responsable à l'attention des enfants de CM2 et de leurs parents. Ainsi, plus de 7 700 actions de sensibilisation ont

*(119) Dispositif d'assistance aux victimes de cyber malveillance : **https://www.cybermalveillance.gouv.fr/***
*(120) Centre expert contre la cybercriminalité français : **https://www.cecyf.fr/***
*(121) Site d'information sur les botnets : **http://www.antibot.fr/***
*(122) Plateforme de lutte contre les spams vocaux et sms : **https://www.33700.fr/***
*(123) Plateforme de signalement des spams : **https://www.signal-spam.fr/***
*(124) Plateforme de signalement des sites de phishing francophones : **https://phishing-initiative.fr/contrib/***
*(125) Plateforme de signalement de contenus illicites sur Internet : **https://www.pointdecontact.net/***
*(126) L'Association de protection de l'enfance sur Internet : **https://www.e-enfance.org/***
(127) Hors permis internet.

été conduites, par les services de police et de gendarmerie, auprès de 160 000 élèves entre septembre 2017 et juin 2018. À ce jour, 2 000 000 d'enfants en ont bénéficié.

Des initiatives plus récentes ont vu le jour, comme la création, en octobre 2018, du **cahier de vacances sur la sécurité numérique,** « Les As du Web »[128]. À destination des enfants de 7 à 11 ans, ce document a été créé par la branche française de l'*Information Systems Security Association* (ISSA) avec le concours de la Gendarmerie nationale et de la Préfecture de Police, qui l'imprime pour les écoliers du ressort.

Figure 32 : Avec ce cahier, les enfants de 7 à 11 ans et les parents peuvent découvrir les bonnes pratiques de la sécurité informatique.
(Crédit Photo : Benjamin Girette)

Finalisée en janvier 2019, l'application Pro.T.E.C.T, le « Programme Territorial d'Education à la Cyber Tranquillité », a été conçue à l'initiative du groupement de gendarmerie départementale des Yvelines (GGD 78), en collaboration avec l'association e-Enfance et une *start-up* de la French Tech avec le soutien du CIPDR[129]. Son objectif est de sensibiliser les collégiens au cyberharcèlement, à l'emprise mentale et à la protection des données. Disponible sur tablette sous forme de jeu didactique, l'application sera expérimentée au cours de l'année dans plusieurs collèges du département par la gendarmerie et la police des Yvelines.

Par ailleurs, les services de police et de gendarmerie ont aussi pour mission de délivrer des conseils de prévention à destination des jeunes dans le domaine du cyber, souvent en relation avec **Net Ecoute**[130], le numéro vert national spécialisé dans les problématiques que rencontrent les enfants et les adolescents dans leurs pratiques numériques, et notamment le cyber-harcèlement.

À ces différentes initiatives s'ajoutent les actions de préventions réalisées dans le cadre de la lutte contre le racisme et l'antisémitisme, intégrant un volet cyber.

Enfin, la présence de la Préfecture de Police et de la DMISC comme membres « observateur » de l'association « Point de Contact »[131] démontre la détermination du ministère à participer aux actions de sensibilisation visant notamment à signaler les contenus illicites en ligne. Par ailleurs, cette association a piloté la réactualisation du **livre blanc « Pédopornographie et propagande terroriste en ligne,** *Traitement des contenus et protection des professionnels »*[132]*,* dont l'objet est de créer un socle commun de bonnes pratiques professionnelles en matière de traitement opérationnel des contenus choquants et potentiellement illicites, qui mettent en jeu la sécurité physique et l'équilibre psychologique des professionnels. Plusieurs services concernés du ministère de l'Intérieur ont activement participé à cette nouvelle version.

(128) Disponible au téléchargement : ***https://www.securitytuesday.com/wpcontent/uploads/2018/10/ISSA.Cahier.SecNum777.pdf***
(129) Comité interministériel de prévention de la délinquance et de la radicalisation.
(130) Numéro national 0800 200 000- ***https://www.netecoute.fr/***
(131) Cette association traite les signalements adressés par les internautes et les partenaires professionnels à la plateforme ***www.pointdecontact.net.*** *Elle est membre fondateur du réseau international INHOPE qui lutte contre les contenus pédopornographiques.*
(132) ***https://www.pointdecontact.net/wp-content/uploads/2019/01/Livre_blanc_FR.pdf - révision du document de 2014.***

3.2.1.2 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 préparer aux problématiques liées à la cybercriminalité et à la radicalisation. À titre d'illustration, les référents de la Gendarmerie nationale sensibilisent, dans le cadre de la politique publique d'intelligence économique, près de 6 000 entreprises – majoritairement TPE/TPI – aux risques informatiques chaque année.

Les services du ministère de l'Intérieur participent aux actions de sensibilisation menées par / ou avec leurs partenaires étatiques, en particulier avec l'ANSSI, en région parisienne ou dans les autres régions, lors d'événements dédiés aux PME/PMI, tel le Forum du Rhin supérieur sur les cybermenaces[133].

En 2018, la direction générale de la sécurité intérieure (DGSI) a organisé plus de 1 450 conférences sur la protection de l'information et la sécurité numérique, notamment à l'endroit des entreprises et des partenaires institutionnels. Près de 74 000 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 cette année, un accent a été porté sur la sensibilisation des personnels effectuant des voyages professionnels à l'étranger et les questions de chiffrement.

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 SDLC mène aussi des actions de sensibilisation du monde économique aux risques cyber, notamment à travers l'action du réseau des référents cybermenaces zonaux, qu'elle expérimente depuis mars 2018 (voir 3.3.3.3).

Elle participe également aux actions de communication menées par le ministère de l'Intérieur. À ce titre, elle collabore à la réalisation de supports de prévention à destination des entreprises tels que le *flyer* « savoir se prémunir face à une attaque informatique ». Elle diffuse également conjointement avec EC3 d'Europol des plaquettes de prévention contre le vol de données bancaires et de moyens de paiement et sur la sécurisation des achats sur internet.

(133) Organisé chaque année depuis 2008 à l'ENA à Strasbourg par la région de gendarmerie et la réserve citoyenne en Alsace.

La Préfecture de Police intervient auprès du MEDEF ou sensibilise directement des entreprises, éventuellement en association avec certaines banques (Société Générale, BNP Paribas), grâce à ses correspondants et référents sûreté, mais aussi aux spécialistes de la BEFTI et de la BFMP (brigade des fraudes aux moyens de paiements).

Par ailleurs, le service du haut fonctionnaire de défense du secrétariat général du ministère (SHFD) publie des documents intitulés « flash ingérence économique », outils de sensibilisation consacrés à des sujets variés (vulnérabilités sur les *smartphones*…), qui peuvent, pour certains, être communiqués aux entreprises. Il a aussi pour objet d'accompagner les agents du ministère de l'Intérieur dans la diffusion d'une culture de sécurité intérieure.

Enfin, les services du ministère de l'Intérieur participent aux événements de portée nationale réunissant des milliers de professionnels de la cybersécurité et de la lutte contre la cybercriminalité comme le Forum international de la cybersécurité (FIC), créé à l'initiative de la Gendarmerie nationale et organisé depuis plus de dix ans à Lille.

3.2.1.3 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 « Intelligence économique » a distingué et valorisé 309 notes de fond relevant d'atteintes à la sécurité économique et/ou de l'exploitation de l'information stratégique utile à l'entreprise. Près d'un quart de ces notes (22 %) concerne des atteintes de cybercriminalité. La cybercriminalité se place, ainsi, à la troisième place des atteintes relevées, derrière les prédations économiques (28,9 %), et les actes de malveillance (32,4 %). Les principales régions impactées par les atteintes de cybercriminalité sont la région Grand Est, l'Occitanie, la région Provence-Alpes-Côte d'Azur et la région Nouvelle-Aquitaine.

En coordination avec le SCRT, la Gendarmerie nationale dispose d'une section sécurité économique et protection des entreprises (SECOPE) à la sous-direction de l'anticipation opérationnelle (SDAO) de la DGGN. Cette section anime un réseau d'environ deux-cents référents[134]. Ils sont chargés de sensibiliser le tissu économique local à l'intelligence économique et de remonter le renseignement d'intérêt économique[135].

3.2.2. Protection des données

En application du règlement européen 2016/679 (RGPD) et de la loi n° 78-17 du 6 janvier 1978 dite « Informatique et libertés » modifiée, transposant notamment la directive européenne 2016/680 sur les traitements de données en matière de prévention et de détection des infractions

(134) Depuis fin 2017, les entreprises qui le souhaitent peuvent contacter et solliciter directement un référent sécurité économique et protection des entreprises, placé auprès d'une région de gendarmerie. Plus de 6 000 entreprises ont été sensibilisées par ces référents en 2018.

(135) Ces fiches de renseignement alimentent la Base de données de sécurité publique (BDSP).

pénales, de lutte contre les menaces à la sécurité publique et la prévention de telles menaces, le ministère de l'Intérieur a réformé en 2018 son organisation en matière de protection des données à caractère personnel.

L'objectif de cette organisation est de garantir la protection des droits et libertés des personnes physiques, notamment contre les risques résultant d'une attaque des systèmes d'information du ministère. Les textes exigent ainsi l'adoption de mesures organisationnelles et techniques en vue d'assurer la sécurité des traitements, la traçabilité des accès, la réalisation d'une analyse d'impact préalable en cas de traitement présentant un risque élevé, la mise en place d'une procédure de notification des autorités et des personnes en cas de violation des données, tout en conservant la nécessité d'un acte réglementaire et une saisine préalable de la CNIL pour la majorité des traitements du ministère de l'Intérieur.

Un **délégué ministériel à la protection des données** a été nommé et placé auprès du Secrétaire général du ministère. Il exerce les missions prévues à l'article 39 du RGPD et à l'article 70-17 de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Son rôle principal est notamment d'assister les responsables de traitement dans la réalisation des analyses d'impact relatives à la protection des données (AIPD), dans la tenue des registres de traitements et lors des notifications de violations de données à caractère personnel. Pour l'ensemble de ses missions, il anime et s'appuie sur un réseau de correspondants à la protection des données nommés dans chaque direction et service du ministère, ainsi que dans ses échelons territoriaux et ses opérateurs.

La direction des libertés publiques et des affaires juridiques (DLPAJ) conserve son rôle central en matière de protection des données à caractère personnel pour le ministère de l'Intérieur, en lien avec le délégué ministériel à la protection des données. Dans ce cadre, elle est chargée de l'instruction des dossiers relatifs aux traitements autorisés par un acte réglementaire pris après avis de la CNIL ainsi que ceux qui, au terme d'une analyse d'impact (AIPD), nécessitent une consultation de cette commission. Dans ce cadre, la DLPAJ apporte une expertise juridique aux directions du ministère. Par ailleurs, elle a à connaître l'ensemble des projets européens ou nationaux (législatifs ou réglementaires) relatifs à la protection des données à caractère personnel ou la consultation de traitements de données.

En raison de la spécificité de certains fichiers du ministère, qui ne relèvent pas du RGPD mais de la directive 2016/680 dite « Police-Justice », le délégué ministériel à la protection des données a défini une doctrine d'application des textes particulière au ministère. Sur la base de cette doctrine, des actions de formation des correspondants et de sensibilisation des agents ont été lancées par le délégué. En quelques mois, le ministère a présenté à la CNIL plusieurs analyses d'impact relatives à la protection des données, qui évaluent les risques pour les droits et libertés des personnes concernées et qui déterminent les mesures et garanties pour faire face à ces risques.

Enfin, il convient de noter que la Gendarmerie nationale a obtenu le label CNIL RGPD en 2018.

3.2.3. Protection et défense 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 acteurs de la sécurité des systèmes d'information, présents dans chaque entité du ministère, aussi bien en administration centrale que dans les territoires. Ce réseau est animé par le fonctionnaire des systèmes d'information (FSSI), placé auprès du haut fonctionnaire de

défense et de sécurité adjoint. Il compte près de 400 responsables de la sécurité des systèmes d'information (RSSI)[136], et plus de 1 100 assistants locaux et correspondants locaux.

Homologation des systèmes d'information

Conformément au cadre réglementaire en vigueur et aux bonnes pratiques en la matière, la protection des systèmes d'information du ministère s'appuie sur le processus d'homologation de sécurité. Ce processus implique les autorités dans les décisions liées à la sécurité numérique et permet d'ajuster les mesures de sécurité aux enjeux du système, des informations qu'il traite et des missions auxquelles il concourt.

Dans ce cadre, le ministère s'est donné pour objectif l'homologation de tous ses systèmes d'information, en priorisant les plus essentiels et les nouveaux systèmes[137]. L'année 2018 a vu de nombreux travaux d'analyse de risque en vue de préparer des homologations.

Au premier rang des systèmes concernés, le réseau bureautique du ministère doit être homologué au niveau « Diffusion restreinte ». Le programme « Homologation DR » consiste en une trentaine de mesures cohérentes, indépendantes les unes des autres et concourant toutes à la réduction du risque. Parmi les réalisations de l'année, on peut noter l'homologation du système d'information « poste de travail Linux GendBuntu » en novembre 2018.

On peut également noter que les deux infrastructures de gestion de clés cryptographiques utilisées pour la certification des agents et des services du ministère (celle de la gendarmerie nationale et celle du reste du ministère) ont fait l'objet d'un processus ayant abouti à leur qualification de conformité au RGS**.

Défense des systèmes d'information

La détection, la qualification et la réaction aux incidents SSI sont assurées 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. Le C2MI collabore activement avec les autres centres opérationnels externes, notamment celui de l'ANSSI et internes, notamment le groupe de sécurité opérationnelle au Service de traitement de l'information gendarmerie (STIG) à Rosny-sous-Bois.

Enfin, différentes actions de sensibilisation ont eu lieu auprès de l'ensemble des agents du ministère. En particulier, plusieurs campagnes de sensibilisation au risque de *phishing* ont été réalisées par le centre de cyberdéfense. Elles ont concerné 74 sites et près de 13 000 courriels de test ont été envoyés.

La résilience des systèmes

La résilience est un enjeu particulièrement important pour les systèmes d'information du ministère. Par exemple, le Service de traitement de l'information Gendarmerie (STIG) dispose d'une plateforme de très haute disponibilité (appelée IPMS, pour « infrastructure de production mutualisée et secourue ») certifiée conforme aux normes[138] depuis plusieurs années.

(136) La nomination d'un RSSI donne lieu à son inscription à une formation obligatoire, réalisée par le centre de formation de l'ANSSI.
(137) Par exemple, le système d'information PERCEVAL a été homologué en février 2018.
(138) Certifiée ISO 20.000 (gestion des services informatiques) depuis 2011, ISO 27.001 (sécurité de l'information) depuis 2015, et ISO 22.301 (continuité d'activité) depuis 2018. Ces certifications sont remises en jeu chaque année.

3.3. Enquêter

3.3.1 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.

Selon le recensement de la gendarmerie sur tout le territoire national, plus de 5 700 victimes sont accueillies chaque mois pour des infractions où le numérique intervient de manière principale. Par ailleurs, depuis le mois de février 2018, la brigade numérique assure l'accueil du public dans l'espace numérique, en lien permanent et dans la continuité de l'action de la gendarmerie sur le terrain. Plus de 65 000 sollicitations ont été enregistrées depuis la mise en service de la brigade numérique (cf.§ 3.4.3.3).

Outre la formation de tous les acteurs chargés de l'accueil des victimes, les services opérationnels finalisent des dispositifs de recueil de plaintes pour mieux partager et exploiter certaines données relatives à la cybercriminalité comme les escroqueries en ligne avec le projet THESEE (cf.§ 3.4.4.1). Les victimes peuvent déjà être orientées par certains services télématiques existants - pré-plainte en ligne et plateforme PERCEVAL (cf. § 3.4.4.2) ou encore le site cybermalveillance.gouv.fr (cf.§ 3.4.5).

En 2018, la plateforme Info Escroquerie de l'OCLCTIC a reçu 39 394 appels soit une augmentation de 39 % par rapport à 2017 (année qui avait connu une hausse de 24 %). 72 % d'entre eux étaient liés à des escroqueries sur Internet ou à la téléphonie (+7 points par rapport à 2017).

Les appels concernant les *malwares* ont connu une légère diminution en comparaison de l'année 2017, en l'absence d'attaques majeures liées à des rançongiciels. L'arnaque au faux support technique est en pleine progression, de même que les cas de *phishing* (+20 %) et ceux concernant le *trading*/opération binaire (cf.§ 2.2.3.2). En revanche, les appels pour les escroqueries à la téléphonie continuent de diminuer.

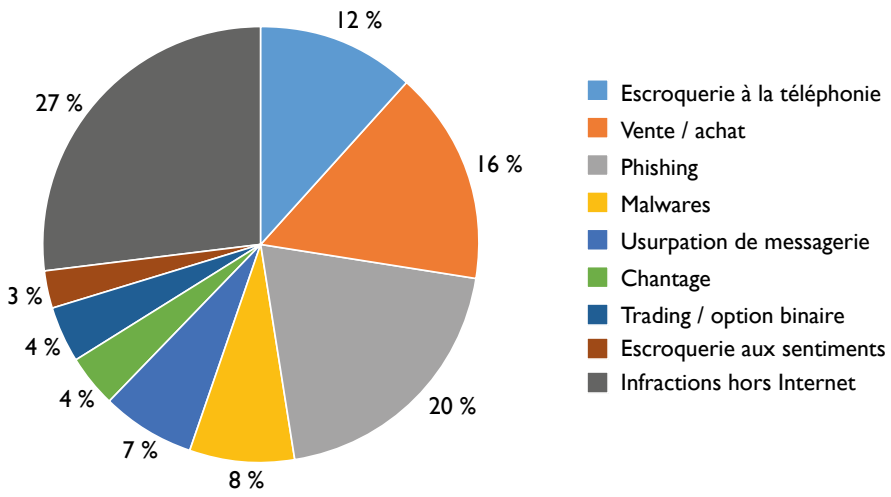


Figure 33 : Répartition des appels sur la plateforme Info Escroquerie

3.3.2 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 a conduit, dans ces deux domaines, à la mise en place d'un réseau territorial animé ou piloté par les services centraux.

OCLCTIC - SDLC

La section opérationnelle de l'OCLCTIC a ouvert 84 nouvelles enquêtes en 2018 (contre 72 en 2017, 88 en 2016), et procédé à 53 gardes à vue (39 en 2017, 60 en 2016) qui ont abouti à 17 écrous (17 en 2018, 25 en 2016). PHAROS a transmis, de son côté, 163 procédures (303 procédures en 2017) aux services territoriaux de police ou gendarmerie, principalement pour des faits d'atteintes aux mineurs (70 %) ou de faits constatés de discrimination (9 %)

La section d'assistance technique de l'OCLCTIC a analysé 1 562 supports numériques en 2018 (1 239 en 2017), à la fois pour les unités de la SDLC (395) que pour l'ensemble des autres services d'investigation (901) et la Sous-Direction de l'Anti-Terrorisme (319).

Développant une vraie dynamique forensic au niveau territorial, la police nationale a déployé 15 laboratoires d'investigation opérationnelle numérique (LION) afin de permettre un traitement déconcentré des supports numériques collectés au plus près des besoins du terrain. Par ailleurs, la SDLC anime le réseau des investigateurs en cybercriminalité (ICC) déployés dans les différentes directions de la police nationale.

Dès 2017, la SDLC a mis en place un « bureau d'aide à l'enquête » qui met directement à la disposition des enquêteurs les informations nécessaires et les assiste dans leurs démarches. En 2018, ce sont ainsi 1 354 assistances qui ont été réalisées pour régler une difficulté ou pour appuyer une demande.

CSIRT-PJ[139] de la SDLC

L'année 2018 a vu le développement de l'activité du CSIRT-PJ, partagée entre le soutien à l'activité opérationnelle et la participation à l'activité de la communauté des CSIRT français : l'Intercert. Sur le plan opérationnel, le CSIRT-PJ a effectué des analyses de compromission dans une vingtaine de dossiers judiciaires impliquant l'usage de logiciels malveillants. Le développement d'outils de soutien à l'enquête s'est poursuivi, permettant notamment le recensement des nœuds d'un réseau de « machines-zombies ». Dans le cadre de la participation à l'Intercert, le CSIRT-PJ a présenté sa plateforme d'échange de souches de logiciels malveillants, PLASMA (Plateforme de Soumission de Logiciels Malveillants).

Formation

Concernant la formation, la SDLC et la DCRFPN[140] ont poursuivi, en 2018, la conduite d'une politique globale de formation à l'enquête numérique. Les différents niveaux de formation permettent la diffusion dans les services de compétences adaptées aux besoins opérationnels. L'enjeu est double : d'une part répondre à un besoin de massification de l'enquête numérique, avec les primo intervenants en cybercriminalité (PICC) et les Enquêteurs sur Internet et les Réseaux Sociaux (EIRS), et d'autre part à un besoin de spécialisation pour les actes les plus complexes et les affaires à fort enjeu, avec les investigateurs en cybercriminalité (ICC).

La DCRFPN a également mis en ligne récemment, sur le e-campus de la Police nationale, une formation intitulée « Bases de l'Investigation Numérique » (BIN).

(139) CSIRT : Computer security and incident response team.
(140) Direction centrale du recrutement et de la formation de la Police nationale.

La cohérence du système repose sur une approche quantitative et qualitative par niveau de compétence requis. La SDLC a amorcé une diminution progressive des formations d'ICC pour stabiliser leur nombre entre 550 et 600 à terme, parallèlement à l'accroissement nécessaire du nombre de PICC. À ce jour :

> 507 ICC sont déployés dans les services de sécurité intérieure. 48 doivent être formés en 2019 ;
> plus de 260 PICC ont été formés. Le seuil optimal est évalué à 5 000 PICC ;
> près de 2 000 personnes ont validé la formation EIRS.

C3N - CyberGend

Action judiciaire du C3N

Le Centre de lutte contre les criminalités numériques (C3N) conduit des enquêtes judiciaires, souvent sur la base de constatations dressées d'initiative. 160 enquêtes ont été menées en 2018, dont 60,5 % d'initiative. Par ailleurs, le département d'enquête du C3N a identifié 156 suspects et transmis les investigations associées aux unités territoriales en vue d'interpellation.

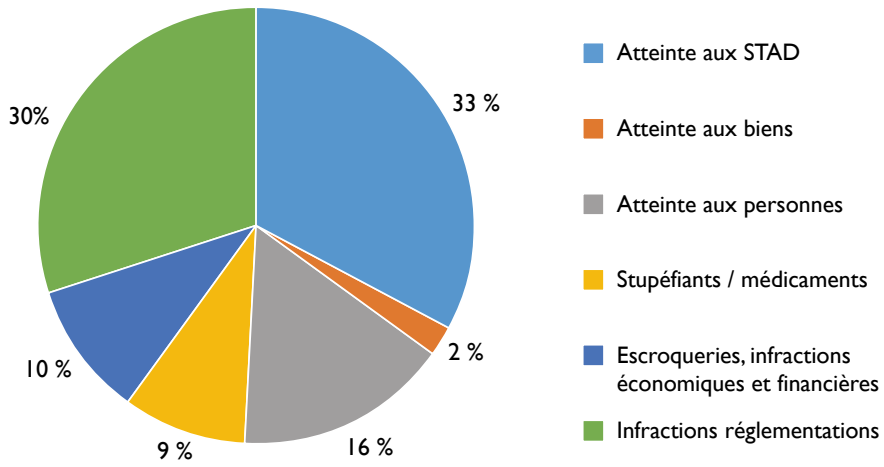


Figure 34 : Catégorisation des dossiers traités par le C3N

Appui judiciaire du C3N

Le C3N a également réalisé 43 missions d'appui judiciaire sur des affaires complexes, 55 environnements numériques et 184 rapprochements judiciaires.

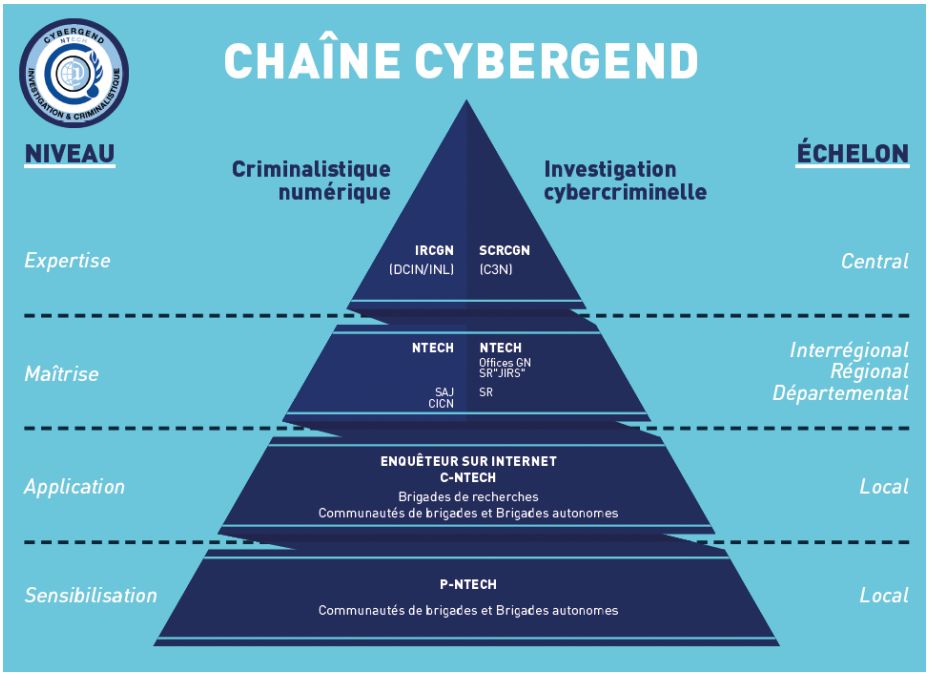
Outre le suivi des phénomènes cybercriminels, le C3N assure l'appui opérationnel du réseau décentralisé « **Cybergend** », comprenant tous les enquêteurs spécialisés (NTECH / C-NTECH), qu'il anime et coordonne. Il leur apporte une assistance en temps réel pour les investigations en téléphonie ou sur Internet par le biais de son guichet unique (GUTI) ; ce dernier a traité 2 580 assistances en 2018, ainsi que 7 325 appels sur la *« hotline »* dédiée. Par ailleurs, il s'est engagé dans la durée sur 5 affaires sensibles.

Formation et réseau « CyberGend »

Les évolutions technologiques permanentes amènent les unités de gendarmerie à adapter leurs méthodes de travail et la conduite des investigations. À cet effet, la Gendarmerie nationale poursuit son effort de formation pour avoir une chaîne territoriale réactive fonctionnant sur un principe de subsidiarité.

Au sein de chaque brigade, des primo-intervenants en nouvelles technologies numériques (P-NTECH) sont habilités à recueillir les plaintes des particuliers victimes d'infraction non spécifiques (telle que l'usurpation) et effectuer des opérations de préservation et de saisie de preuves numériques. Depuis octobre 2018, tous les élèves gendarmes sont formés P-NTECH.

Les correspondants en technologies numériques (C-NTECH), au nombre de 4 300 et formés en 5 jours, sont les premiers relais en matière de cybercriminalité. Ils procèdent aux saisies et scellés lors des perquisitions et peuvent réaliser des analyses simples sur des téléphones ou vérifier les données accessibles d'un ordinateur (extraction des données SMS ou de courriels). Pour répondre au besoin opérationnel d'analyse de masse des téléphones portables par les unités territoriales et circonscrire l'obsolescence de certains matériels, la DGGN a déployé depuis septembre 2018 de nouvelles capacités élémentaires d'extraction de données des téléphones portables. Les C-NTECH d'unités recherches peuvent compléter leur parcours de formation en suivant la qualification d'enquêteur sur Internet afin d'être en mesure d'effectuer des recherches complexes en sources ouvertes ou encore des enquêtes sous pseudonyme(141).



Enfin, les NTECH au nombre de 250, suivent une licence professionnelle en partenariat avec l'université de technologie de Troyes et un stage de remise à niveau. Affectés en Section de recherches (S.R.), offices centraux, PJGN, cellules d'identification criminelle et numérique

(141) Le C3N en charge de la formation « enquêteur sous pseudonyme » forme chaque année 48 gendarmes.

(CICN) ou en formations spécialisées, les NTECH interviennent en fonction de leur affectation soit sur un versant enquête soit sur un versant criminalistique numérique. Au sein des SR, des offices et du C3N, les NTECH développent des capacités d'enquête en matière cyber et mènent des investigations complexes visant à mettre à jour des groupes criminels utilisant les technologies numériques. Côté criminalistique numérique, dans chaque département, les CICN ont pour mission de rechercher les traces numériques et les indices (analyse des disques durs, exploitation des données recueillies sur tous supports…). Enfin les dossiers criminalistiques demandant un haut niveau de compétence sont traités par les experts du département Informatique- Électronique de l'Institut de recherche criminelle de la Gendarmerie nationale (IRCGN) de Pontoise.

Le C3N est membre de l'*European Cybercrime Training and Education Group* (ECTEG).

BEFTI

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

En 2018, la BEFTI a ouvert 205 enquêtes et en a clôturé 292. Elle a un important portefeuille de 185 enquêtes en cours. 72 personnes ont été mises en cause, dont 37 placées en garde à vue et 35 entendues librement. 9 ont été mises à disposition des magistrats et 20 ont fait l'objet de convocations au tribunal (COPJ/CRPC).

Par ailleurs, elle a réalisé 150 assistances au profit des services de la DRPJ et en moindre importance, de la DSPAP. 445 supports numériques ont été analysés pour un total de 135 To. En outre, la fonction de guichet unique de l'urgence de la BEFTI fluidifie les demandes souvent complexes des services de la Préfecture de Police de Paris auprès des opérateurs de l'Internet.

En matière de formation, des interventions de sensibilisation des entreprises ou de formation des agents publics ou d'universitaires sont mises en œuvre par la Préfecture de Police, par l'intermédiaire de la BEFTI et la BFMP, voire du conseiller aux questions liées à la cybercriminalité du préfet de Police.

DGSI

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 nuire aux intérêts fondamentaux de la Nation.

Création d'un département cyber

Afin de mieux répondre aux défis posés par les menaces cyber, la DGSI a créé un nouveau département cyber au sein de sa direction technique. Cette structure doit concourir aux missions de cyberdéfense telles que définies dans la revue stratégique cyber publiée en février 2018. La DGSI devra travailler notamment avec l'ANSSI pour lutter contre les menaces pesant sur les réseaux des OIV et des OSE français.

Ce département a également un rôle d'analyse et de sensibilisation à la menace cyber auprès des autorités et des partenaires de la DGSI.

Création du Service Technique National de Captation Judiciaire (STNCJ)

Pour contourner l'utilisation largement démocratisée des moyens de chiffrement, la loi du 14 mars 2011 dite LOPPSI II a créé une nouvelle catégorie de techniques spéciales d'enquête relative aux captations des données informatiques à distance (art. 706-102-1 à 706-102-6 du Code de procédure pénale). Celle-ci autorise les services spécialisés, sans le consentement des intéressés, à accéder à des données informatiques, de les enregistrer, les conserver et les transmettre, dans les affaires de terrorisme et relevant de la criminalité organisée.

Le STNCJ créé par arrêté le 9 mai 2018 et rattaché à la direction technique de la DGSI, a été chargé de fournir les outils techniques de captation.

Coopération technique et opérationnelle

Les actions de coopération en matière de cybercriminalité, sous la coordination de la DCI, ont augmenté ces dernières années, passant de 35 en 2016 à 82 en 2017 puis 92 en 2018. Elles prennent le plus souvent la forme d'actions de formation permettant ainsi de renforcer les liens opérationnels entre la France et les pays sources de cybercriminalité.

La DCI participe aussi au déploiement d'experts techniques internationaux (ETI) cyber depuis 2016 et compte à ce jour 3 ETI (1 en Afrique du Sud, 2 au Sénégal) et un officier de liaison aux États-Unis basé à Washington. Un ETI devrait prochainement être installé en Afrique de l'Ouest.

En 2018, en matière de coopération internationale opérationnelle, l'OCLCTIC a constaté une augmentation notable des dossiers traités avec Interpol (2053 en 2018, contre 1981 en 2017 et 1326 en 2016), notamment en raison de l'amélioration des circuits de remontée d'information en provenance de PHAROS et d'une politique renforcée de signalements. 849 messages ont été échangés avec Europol (808 en 2017) et 263 avec le réseau 24/7 de la Convention de Budapest et du G7. Il s'agit, dans ce dernier cas, des demandes de gel de données émises ou reçues par le point de contact national: 120 demandes de préservation de données ont été émises vers l'étranger (dont 77 pour les États-Unis) tandis que 143 demandes ont été adressées à la France pour des données hébergées principalement chez OVH et Online.

3.4. Innover

3.4.1 Recherche et développement

Pour la Gendarmerie nationale, la recherche et l'innovation reposent sur un édifice désormais consolidé, au sommet duquel a été placé un Conseil scientifique auquel participent de nombreuses personnalités extérieures, institutionnelles ou qualifiées. Il s'est réuni pour la troisième fois le 31 janvier dernier. Pièce centrale, l'Observatoire national des sciences et des technologies de la sécurité (ONSTS) déploie une plateforme partenariale avec le monde extérieur, services publics et industries de sécurité et de défense, qui complète les conventions conclues avec de grands centres de recherche. Le « cyber » constitue l'un des sept axes technologiques prioritaires de son plan stratégique de recherche et d'innovation à 5 ans.

De leur côté, l'École nationale supérieure de la Police (ENSP), l'Université de technologie de Troyes et l'Université Jean Moulin-Lyon 3 ont inauguré en 2019 une chaire de sécurité globale, qui englobe les thématiques de cybersécurité et lutte contre les cybermenaces. Elle vise des objectifs :

> de recherche par la production de connaissances sur les phénomènes sociaux et sociétaux, l'évolution de la menace, les stratégies et technologies mobilisables ;

> d'enseignement supérieur et formation par la diffusion des connaissances issues des travaux de recherche vers des dispositifs reconnus ou novateurs ;

> de valorisation par le développement de partenariats, le transfert de connaissances et la communication (publications, colloques scientifiques, ateliers de recherche…).

Les échanges techniques et technologiques avec le ministère des Armées se développent, en particulier 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, avec des partenariats avec le Centre national de recherche scientifique (CNRS), l'Institut national de recherche en informatique et en automatique (INRIA) et le Commissariat à l'énergie atomique et aux énergies alternatives (CEA).

Développements d'outils et projets de recherche académique

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 ou participent à des projets de recherche académique visant à finaliser des démonstrateurs. Ces outils logiciels ou matériels sont alors partagés par les différents services intéressés.

Face à la multiplication des contenus en accès libre sur Internet (réseaux sociaux, hébergeurs de contenu, sites de vente en ligne, blogs…), la collecte de données en source ouverte sur Internet nécessite des outils adaptés. En effet la diversité des sites, la volumétrie ainsi que les systèmes de protection de contenus (systèmes de suppression rapide, protections contre les automates…) rendent difficile l'exploration manuelle ou l'utilisation d'outils peu complexes. Face à l'augmentation continue des infractions sur Internet, l'enjeu est d'offrir au réseau CyberGEND les capacités de rechercher, fixer, capter et analyser des données publiquement accessibles sur Internet, caractérisées par un risque fort de suppression rapide (censure des réseaux sociaux et autres hébergeurs de contenus), des protections contre les automates *(darknet, captchas)* et des volumétries importantes. Les technologies utilisent des algorithmes de pointe et des calculateurs puissants, fruits d'une collaboration entre le réseau CyberGEND, le SIRPA, la SDAO, le Commandement Cyber des Armées et les polices suisse et belge. Deux projets phares sont conduits au PJGN au titre de la R &D :

> GENDscrapper, applicatif de capture de contenus, avec possibilité de paramétrage en profondeur des contenus à aspirer au sein des pages. L'outil permet entre autres à l'enquêteur de contourner d'éventuels filtres anti-robot afin de poursuivre son exploration automatique. De nombreux additifs sont actuellement en conception ;

> ALICE (Automatic Labelling for Image Collections Exploration). Ce projet de recherche, lancé en 2016 par le C3N, a pour but d'automatiser la recherche, le tri et l'identification des images susceptibles de matérialiser un crime ou un délit aggravé. Un processus d'analyse sémantique a été développé par *deep learning* pour l'identification des images d'armes à feu. Le développement actuel vise à élargir le spectre des images ciblées (stupéfiants, pédophilie…) en 2019 et à rendre le système d'analyse « portable » pour en doter les personnels de terrain.

La mission prospective et management de l'innovation de la Préfecture de Police et la BEFTI participent activement au programme "ASGARD" *(Analysis System for Gathered Raw Data)*. Il s'agit d'un projet européen du programme « Horizon 2020 » rassemblant des forces de police, des entreprises ainsi que des chercheurs (CEA) afin de développer des solutions « logicielles » dans l'analyse de données au profit des services opérationnels. Des sessions de travaux sont organisées chaque semestre dans un pays européen participant, ainsi que deux *hackathons* en 2018 qui ont été remportés par la BEFTI.

Par ailleurs, la BEFTI suit les travaux du LORIA (Laboratoire lorrain de Recherche en Informatique et ses Applications de l'Université de Nancy), visant à développer une technique permettant de détecter « l'ADN » des *malwares,* en vue de les comparer. Il a été mis au point une automatisation de requêtes spécifiques pour comprendre le fonctionnement d'un *malware* isolé. Ceci permet d'obtenir des informations plus précises sur le comportement des *malwares* identifiés dans les affaires judiciaires.

3.4.2 Partenariat Public-Privé

Le développement de partenariats public-privé permet de prendre en compte et de partager les données agrégées par les services de cybersécurité tels les CSIRT (centre de veille, d'échange et réponse aux attaques informatiques). Le partage de données et d'alertes est l'un des objets du Centre de réponse à incidents de la police judiciaire (CSIRT-PJ) de la division de l'anticipation et de l'analyse de la SDLC. Elle développe à ce titre des partenariats d'échange d'informations et de prévention du risque cyber avec le secteur privé. Elle comporte une cellule d'information du public axée sur l'identification des nouveaux modes opératoires pour diffuser les bonnes pratiques permettant de minimiser les risques (alertes en ligne, campagnes de sensibilisation aux dangers de l'Internet, etc.).

Dans le même esprit, les services du ministère de l'Intérieur poursuivent en tant que membres consultatifs, leurs relations avec l'association **Signal Spam** qui recueille des signalements utiles à la protection de l'internaute en luttant contre les sites malveillants et les *botnets* d'attaquants, ainsi qu'avec l'association pointdecontact.net pour les signalements de contenus illicites en ligne.

3.4.2.1 Le partenariat avec les opérateurs de l'Internet

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 Dropbox) 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 et de haine en ligne. Le GCP s'est réuni en formation plénière à 14 reprises entre mai 2015 et mars 2019. Il s'est réuni en formation restreinte sur le thème de la manipulation de l'information. Par ailleurs, la DMISC a organisé avec ces opérateurs une formation d'une journée au profit de plus de 200 enquêteurs, magistrats et douaniers en mars 2018.

Par ailleurs, la SDLC 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.

Le « bureau d'aide à l'enquête » de la SDLC a organisé des rencontres pédagogiques qui permettent aux acteurs du monde numérique de préciser leurs politiques en matière d'obligations légales et présenter les services qu'ils sont en mesure de fournir aux enquêteurs. Ces journées d'information s'adressent aux enquêteurs issus de toutes les directions : DGSI, DGGN, DCPJ, DCPAF, DCSP, douanes (MINEFI), etc. En 2018, deux journées ont été organisées comme cela avait été le cas en 2017.

Au plan européen, le dialogue avec les opérateurs de l'Internet est conduit dans le cadre de l'*EU Internet Forum*. L'objectif premier de ces travaux est d'obtenir qu'ils s'engagent à retirer les contenus terroristes dans l'heure qui suit leur publication, pour éviter leur dissémination sur la toile (on parle de la *Golden Hour*). Ils sont aussi encouragés à mettre en place des mesures proactives afin de détecter et de retirer de tels contenus.

3.4.2.2 Travaux de la filière des industries de sécurité

En 2013, 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 a représenté le ministre de l'Intérieur dans les travaux du CoFis et assuré le suivi des actions engagées dans ce cadre.

Dans le cadre du dialogue constant avec les industriels, le ministère de l'Intérieur, en lien avec le ministère de l'Économie et des finances, a activement œuvré pour le lancement d'une seconde phase dans la dynamique de filière industrielle de sécurité avec la **création d'un 18e comité stratégique de filière (CSF) au sein du Conseil national de l'industrie** (CNI), le 22 novembre 2018, en même temps que celui consacré aux infrastructures du numérique (17e CSF). Placé sous la présidence du Premier ministre, le CNI permet un travail entre les différentes filières et place chaque CSF sous la conduite d'un industriel avec un comité de pilotage rassemblant l'État et les industriels, avec des objectifs communs. Dans le cas du CSF Industries de sécurité, le copilotage de l'État sera assuré par les ministères de l'Économie (DGE) et de l'Intérieur (DMISC), le SGDSN avec l'ANSSI. Cette évolution permettra de consolider le développement et la croissance d'une filière de tout premier plan.

3.4.2.3 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), le cercle Montesquieu ou encore le Centre d'Étude 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 Tanks* comme les journées d'étude FRS 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.

Afin d'être au plus près des acteurs économiques, administratifs et politiques qui, dans les territoires, doivent insérer la sécurité numérique dans leur champ d'action et de développement, le CyberCercle organise en région des journées de rencontres territoriales sur la cybersécurité. Placées sous la dynamique des élus locaux, elles ont pour vocation de réunir l'ensemble des acteurs concernés par le sujet, autour de thématiques en adéquation avec les préoccupations du tissu économique local, à l'aune des enjeux de développement des territoires péri-urbains et ruraux. Ainsi ce « Tour de France de la cybersécurité » a vocation à aller sur le terrain pour sensibiliser les institutions locales et les petites entreprises aux cybermenaces. Après Pau et Lannion en 2018, la saison 2019 a débuté à Bourges fin février et a associé des acteurs comme la *CCI France* ou le groupe *La Poste,* mais aussi le ministère de l'Intérieur, représenté par la DMISC.

Plusieurs associations contribuent aussi aux échanges et à la réflexion, telles le CECyF (Centre Expert contre la cybercriminalité Français) et Cyberlex[142] qui ont produit conjointement début 2018, un rapport sur les évolutions possibles de la procédure pénale pour mieux lutter contre la cybercriminalité. Les membres du ministère de l'Intérieur participent aussi à des associations professionnelles comme l'AFSIN (Association francophone des spécialistes en investigation numérique), le CESIN ou le CLUSIF.

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 privés à leur réflexion, en particulier lors des séminaires ou des ateliers de recherche qu'ils organisent[143].

3.4.2.4 Transferts de compétences

Le MBA spécialisé « Management de la sécurité » a été créé par l'EOGN avec l'Université Paris II Panthéon-Assas associant HEC Paris et des cadres supérieurs et dirigeants d'entreprises. Il offre un cursus multidisciplinaire à destination des cadres du secteur sécurité/sûreté proposant une approche globale de la sécurité ; plus de quarante heures (soit un cinquième du temps de formation) sont ainsi consacrées à l'étude de la cybercriminalité et des risques numériques.

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

3.4.3.1 Projet Néo PN/GN

Initiés dans le département du Nord en septembre 2015, les projets NEOgend puis NEO ont été déployés respectivement par la Gendarmerie et la Police nationales en 2017 et 2018. Visant à offrir aux personnels en mobilité l'ensemble des outils dont ils ont besoin pour accomplir leurs missions, ils s'enrichissent régulièrement de nouvelles applications conçues dans une démarche collaborative. Depuis les opérations de prévention et de contrôle des flux aux actes d'enquête judiciaire, l'intégralité du spectre des missions 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 115 000[144] *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, fin 2017 (+150 %).

*(142) Cyberlex - L'association du Droit et des Nouvelles technologies - **http://www.cyberlex.org/***
*(143) CREOGN « Cybersécurité : TPE-PME : les oubliés de la cybersécurité? 12 décembre 2018 / Blockchain : la sécurité absolue? 27 juin 2018 **https://www.gendarmerie.interieur.gouv.fr/crgn/ARG-Colloque/Ateliers-recherche-de-la-gendarmerie/ARG-2018***
(144) 65 000 équipements déployés en gendarmerie, 50 000 équipements déployés en police.

3.4.3.2 Plateforme de signalement des violences sexuelles et sexistes

Annoncé par le Président de la République dans son discours du 25 novembre 2017, le portail de signalement en ligne des violences sexuelles et sexistes (VSS), commun à la police et la gendarmerie, fait partie des mesures phares pilotées par le ministère de l'Intérieur, notamment dans le cadre de la PSQ.

Inauguré le 27 novembre 2018, ce portail repose sur un dispositif national, disponible 24 heures sur 24 et 7 jours sur 7, et est accessible via le site internet service-public.fr ou directement à l'adresse www.signalement-violences-sexuelles-sexistes.gouv.fr. En fonction des zones de répartition, les demandes reçues sont traitées par la brigade numérique de Rennes (20 gendarmes) ou la plateforme du commissariat de Guyancourt (DDSP 78 - 16 policiers et une psychologue).

La discussion interactive instantanée (« tchat ») permet un échange individualisé (et anonyme) avec un policier ou un gendarme spécifiquement formé à la prise en charge des victimes de violences sexuelles et sexistes. La victime est orientée et accompagnée de chez elle dans ses démarches vers les commissariats et brigades ainsi que vers les dispositifs de prise en charge des victimes (psychologues, intervenants sociaux, permanence d'association) ou associations locales d'aide aux victimes qui peuvent lui venir en aide.

3.4.3.3 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 en mai 2017 d'une entité dédiée, la **mission numérique de la Gendarmerie nationale** (MNGN). L'un de ses premiers projets est la « brigade numérique ». La mission dirige également les évolutions du projet NEOgend et a mené, conjointement avec la Police nationale, le projet « portail des violences sexuelles et sexistes ».

Dans le cadre de la modernisation et de l'effort de contact avec les citoyens, la gendarmerie a décidé de s'engager dans une démarche de proximité numérique, passant entre autres par l'ouverture d'une **brigade numérique** à Rennes le 27 février 2018. Fonctionnant 7 J/7 et 24h/24 et constituée de 20 gendarmes spécialement formés, cette unité nationale réalise numériquement les fonctions de contact et d'accueil du public dévolues aux accueils des brigades territoriales (hors urgences). Elle recueille les informations que les citoyens souhaitent transmettre à la gendarmerie, effectue certains actes d'enquête, répond à leurs sollicitations et les oriente vers les téléservices. Cette offre a été complétée progressivement fin 2018 avec l'affichage des horaires d'accueil des brigades, la prise de rendez-vous en ligne ou encore une expérimentation de bornes tactiles et la présence dans des maisons de service au public.

Depuis son lancement, la brigade numérique a traité plus de 40 000 demandes et elle reçoit actuellement près de 200 sollicitations par jour. Concernant les canaux, le webchat (38 %) et Facebook (37 %) sont prépondérants et dominent le formulaire de contact/courriel (20 %), les messages privés Twitter (5 %) restant marginaux. En plus des comptes nationaux, la brigade numérique répond aux messageries de comptes de groupements de gendarmerie départementale : 50 Facebook Messenger et 4 Twitter.

La plupart des sollicitations concerne les questions de sécurité du quotidien, le recrutement et la communication d'informations, chacun représentant 23 % des demandes. Plus de 270 fiches de renseignement ou procès-verbaux ont déjà été effectués et près de 2 600 informations concernant des sujets extrêmement variés (radicalisation, pédopornographie, viols, véhicules volés, nuisances routières, tentatives de suicide,

remerciements, etc.) ont été retransmises, principalement vers les unités territoriales de la gendarmerie. Les nombreux échanges entre les gendarmes de la brigade numérique et les citoyens sont de qualité, avec un indice de satisfaction de 9 pour le chat et de 8,6 pour le formulaire.

3.4.3.4 La mise en place du réseau des référents cybermenaces

Un réseau des référents cybermenaces de la **Police nationale** a été lancé à titre expérimental le 9 mars 2018. Il a pour objectif de sensibiliser le tissu économique local au risque cyber dans le contexte de la mise en œuvre du RGPD et d'animer le réseau inter-directionnel local de la Police nationale dans ce domaine. Il crée les conditions d'un dialogue avec le tissu économique local, particulièrement exposé aux risques numériques. Trois cellules expérimentales sont actuellement déployées sur des régions pilotes : le Grand Est, la Bretagne et la Nouvelle-Aquitaine. Ce dispositif a vocation à être généralisé à l'ensemble du territoire.

Le réseau se structure de façon innovante en faisant intervenir dans chaque zone des acteurs spécialisés de la police judiciaire et des partenaires issus du secteur privé :

> un commissaire référent au sein de la direction interrégionale de Police judiciaire (DIPJ) du chef-lieu de la zone, anime le réseau inter-directionnel de la police nationale au niveau territorial, conçoit une stratégie locale, pilote le réseau zonal et assure le relai entre la SDLC et celui-ci ;
> un réserviste de haut niveau, issu du secteur privé, assure la sensibilisation du tissu économique local ;
> un réseau de partenaires volontaires, principalement des commissaires aux comptes, formés aux problématiques cyber par la SDLC et la DIPJ et assurant un relai quotidien auprès des entreprises locales.

Un dialogue interministériel permet d'articuler ce dispositif avec les autres intervenants, parmi lesquels : les délégués ANSSI, les délégués à l'information stratégique et à la sécurité économiques et les préfets délégués à la défense et à la sécurité, la sécurité publique et la police aux frontières.

3.4.3.5 L'activité des réseaux de réservistes *« cyber »*

Les réservistes opérationnels et les réservistes citoyens de défense et de sécurité de la Gendarmerie nationale ayant des compétences, une expérience et une appétence particulières dans les domaines de la sécurité du numérique, de la lutte contre la cybercriminalité et de la cyberdéfense, interviennent selon leur statut dans des missions et des groupes de travail variés (sensibilisation des entreprises aux côtés des gendarmes, renfort de la gendarmerie dans la sécurisation de ses systèmes d'information, élaboration de nouveaux outils et méthodes, organisation de forum et séminaires, etc.). Certains participent aux missions définies conjointement par les référents de la gendarmerie, du Commandement de cyberdéfense (ministère des Armées) et de l'ANSSI en région et par les instances nationales de cette gouvernance tripartite.

3.4.3.6 Communication de crise : Système d'Alerte et d'Information des Populations (SAIP) et Médias Sociaux en Gestion d'Urgence (MSGU)

La Direction générale de la sécurité civile et de la gestion des crises (DGSCGC) est chargée du pilotage d'un certain nombre de mesures facilitant l'information des citoyens en cas de crise. Travaillant de conserve, la Délégation à l'information et à la communication (DICOM) apporte son expertise en matière de réseaux sociaux dans les dispositifs rénovés mis en place.

L'alerte et l'information des populations

La DGSCGC demeure compétente en matière d'alerte des populations en situation de crise. Elle pilote toujours le volet « système d'alerte et d'information aux populations » -SAIP- dit *« historique »* (2 000 sirènes d'alerte) ainsi que d'autres dispositifs d'alerte et d'information à l'instar des conventions permettant aux pouvoirs publics de diffuser des messages sur les ondes de Radio France ou via les stations de France Télévisions.

Destiné à prévenir la population en cas d'attaque terroriste réelle ou supposée, le dispositif SAIP mobile, lancé en mai avant l'Euro 2016, a cessé fin mai 2018. Nécessitant un téléchargement sur *smartphone,* cette application n'a jamais connu l'audience espérée (900 000 à l'été 2017), limitant son impact en cas de crise. Sur le plan opérationnel, l'application a par ailleurs souffert de dysfonctionnements et les choix de déclenchement ou de non-déclenchement n'ont pas été compris, ce qui a limité sa crédibilité auprès des utilisateurs.

Aussi, dès lors que la menace terroriste reste élevée sur le territoire français, le ministère de l'Intérieur a souhaité que des outils plus efficaces et plus répandus soient utilisés pour alerter la population d'une situation susceptible de constituer un danger immédiat. Déjà chargée de la communication du ministère de l'Intérieur sur les réseaux sociaux via ses comptes sur Facebook, Twitter…, la DICOM s'est vu confier le pilotage de l'utilisation de ces vecteurs pour les situations de crise depuis le 1er juin 2018. Les messages d'alerte et de prévention du ministère seront diffusés de façon prioritaire sur Twitter, Facebook et Google, mais aussi certains canaux de communication de la RATP, Vinci Autoroutes, Radio France et France Télévisions. Concrètement, Twitter assurera une visibilité toute particulière aux messages du ministère en cas de crise grave avec un bandeau spécial en haut du fil des Tweets. Parallèlement, le ministère de l'Intérieur propose de s'abonner et activer les notifications du compte @Beauvau_alerte, lancé le 1er juin dernier.

Facebook offre la possibilité au ministère de communiquer via un dispositif de communication lié à son outil *« Safety Check »,* créé en 2014, et permettant aux utilisateurs de Facebook d'indiquer à leurs proches qu'ils se trouvent en sécurité. De son côté, Google relaiera sur son moteur de recherche, au travers de son outil *« Posts on Google »,* les messages du ministère de l'Intérieur pour les utilisateurs effectuant des recherches dans la zone impactée.

Enfin, les sociétés d'autoroutes (ASFA), la RATP, France Télévisions et Radio France relaieront aussi via leurs applications, réseaux sociaux ou panneaux d'information les messages du ministère si la situation le nécessite.

Tout un travail partenarial et de compréhension de l'univers numérique a été engagé par la DICOM et ces entités afin de prendre en compte les impératifs techniques et « métiers ». L'adaptation des conventions existantes et la mise en place de nouvelles (SNCF, Snapchat, Qwat…) s'effectuent en collaboration avec la DGSCGC.

Médias Sociaux en Gestion d'Urgence (MSGU)

Le développement des médias sociaux, la généralisation de leur usage par le grand public et l'instantanéité de la diffusion d'information ont conduit à leur prise en compte par la DGSCGC dans le cadre de la détection et du suivi des évènements.

La désintermédiation est au cœur du fonctionnement de ces médias, permettant à des personnes victimes ou témoins d'évènements ou d'incidents de transmettre directement leur expérience. Cela constitue un outil précieux pour la DGSCGC dans ses missions de gestion de crise, permettant d'anticiper les informations remontées par les canaux officiels et de les compléter. Cependant, le volume d'informations produit par ces médias, ainsi que le mélange de témoignages de première main et de rumeurs colportées font que ces outils sont complexes à exploiter (centaines de messages à analyser, sources à recontacter pour vérifier leur témoignage…).

Pour y parvenir, après 3 ans d'expérimentation, la DGSCGC s'est associée en 2016 avec des volontaires regroupés dans l'association VISOV (Volontaires Internationaux en Soutien Opérationnel Virtuel). Le centre opérationnel de gestion interministériel de crise (COGIC) est en contact direct avec VISOV, dont les membres rédigent et transmettent des comptes rendus sur des thématiques particulières. En 2018, le COGIC a activé les volontaires de l'association 2 à 3 fois par semaine, ce qui constitue une très forte augmentation par rapport aux années précédentes.

3.4.4 Mieux appréhender les phénomènes de masse

3.4.4.1 Projet Thésée

La SDLC porte le projet de « plainte en ligne » dit « THESEE » (Traitement Harmonisé des Enquêtes et Signalements pour les e-escroqueries) pour lutter plus efficacement contre le phénomène de masse que constituent les escroqueries sur Internet. Ce dispositif doit permettre pour les usagers la prise de plaintes en ligne contre X. Ce télé-service sera adossé à un outil d'analyse afin de centraliser et de recouper des informations communiquées par les internautes, pour diligenter des enquêtes. Le dispositif sera constitué de plusieurs briques :

> un télé-service adossé au site service-public.fr ;

> une interface de validation des demandes de plaintes ;

> un outil d'analyse.

Il s'appuiera sur deux autres projets, le nouveau logiciel de rédaction de procédure (SCRIBE) et la signature électronique de l'enquêteur actuellement en cours de développement au service des technologies et des systèmes d'information de la Sécurité intérieure (STSI²).

Le projet est entré dans une phase de test des outils informatiques déjà développés. La concertation avec le ministère de la Justice a permis de proposer une modification législative afin de désigner un futur Parquet référent national qui pourra centraliser les plaintes. Les modalités d'accès des autorités judiciaires à la future plateforme ont été définies.

3.4.4.2 Plateforme Perceval (pour rappel)

Développée par la Gendarmerie nationale, cette plateforme permet aux particuliers de signaler toute transaction par carte bancaire dont ils ne sont pas à l'origine (carte toujours en leur possession). La démarche est simple pour le citoyen et pourra servir de guide pour la demande de remboursement par la banque.

La plateforme vise ainsi à recueillir et analyser le contentieux massif des usages frauduleux de carte bancaire. Opérationnelle depuis juin 2018, son activité a été détaillée au chapitre 2.3.1.3.

3.4.5 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 le 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, 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 « Action contre la cybermalveillance » (GIP 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. Le groupement comprend, en mars 2019, 35 membres en dehors du collège étatique : 13 membres dans le collège « utilisateurs », 4 dans le collège « prestataires » et 18 dans le collège « fournisseurs de solutions »[145].

Fin janvier 2019, le nombre de prestataires référencés s'est établi à 1 500, permettant un maillage territorial complet pour l'ensemble des menaces recensées. Il y a eu au total plus de 40 000 mises en relation victimes/prestataires depuis le lancement national.
Un kit de sensibilisation a été réalisé en 2018[146] ; son objectif est d'adresser le particulier à travers le canal professionnel. Plus de 21 000 entités ont téléchargé ce kit soit plus de 11 millions de collaborateurs potentiellement adressés.
En 2019, 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 publics dans la sensibilisation de tous ces publics.

(145) *Il s'agit d'acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles, des assureurs, des opérateurs, des constructeurs, des éditeurs…*
(146) ***https://www.cybermalveillance.gouv.fr/contenus-de-sensibilisation/***

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 modes 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 de phénomènes de masse, comme les arnaques au faux support technique, pris en compte par les services judiciaires.

3.4.6 L'identité numérique

3.4.6.1 Le cadre juridique

À ce jour, 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 prévoit que la preuve de l'identité numérique aux fins d'accéder à un service de communication en ligne peut être apportée par un moyen d'identification électronique. Ce même article énonce en outre que ce moyen d'identification est présumé fiable jusqu'à preuve du contraire lorsqu'il répond aux prescriptions du cahier des charges, établi par l'Agence nationale de sécurité des systèmes d'information (ANSSI). Ce cahier des charges fait l'objet d'un décret qui sera très prochainement examiné par le Conseil d'État. Il établit le niveau de garantie qu'un moyen d'identification électronique doit avoir pour être présumé fiable et fixe les titres d'identités reconnus comme sources faisant autorité pour la preuve et la vérification de l'identité des personnes physiques lors de la délivrance d'un moyen d'identification électronique présumé fiable (carte nationale d'identité, passeport, titre de séjour).

3.4.6.2 Le parcours d'identification

Le développement des usages numériques crée, pour chaque utilisateur, de multiples besoins de s'identifier au quotidien, aussi bien dans la sphère publique (démarches administratives en ligne) que privée (commerce en ligne). Or, dans la plupart des cas, l'identification sur Internet présente un faible niveau de garantie (identifiant et mot de passe) et induit un risque vis-à-vis de l'utilisation des données personnelles.

Diverses, les menaces touchent autant l'administration que le citoyen sur l'ensemble de la chaîne de valeur associée à la délivrance d'un service numérique : usurpation d'identité lors de l'entrée en relation, vol et fuite des données ou encore attaque en déni de service.

C'est pourquoi l'État a souhaité la mise en place d'un parcours d'identification numérique comportant au moins deux niveaux de garantie, dont un niveau élevé au sens du règlement européen e-IDAS[147]. Ce texte instaure un cadre commun en la matière et

(147) Règlement (UE) n ° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE.

prévoit une obligation de reconnaissance mutuelle des solutions notifiées au sein de l'Union européenne à partir de septembre 2018.

Pour ce faire, le Premier ministre a confié conjointement au ministre de l'Intérieur, à la ministre de la Justice et au secrétaire d'État chargé du Numérique le soin de mettre en place un programme interministériel[148] pour la conception et la mise en œuvre de ce parcours d'identification numérique.

Ce parcours a vocation à constituer un service public d'une nouvelle nature. En premier lieu, il permettra au citoyen de prouver son identité lors de ses interactions dans l'environnement numérique. En second lieu, il favorisera la sécurisation des schémas d'identification, ainsi que la fiabilisation des données d'identité transmises par les citoyens. Ainsi, il réduira le risque d'usurpation d'identité en ligne et s'inscrira pleinement dans la logique de protection des données personnelles. Enfin, l'identité numérique concourt à l'exigence de simplicité, nécessaire à une appropriation par le citoyen des nouveaux services en ligne que pourra offrir l'État mais également d'autres acteurs.

Dans une logique d'interopérabilité, le parcours d'identification numérique devra s'intégrer au sein du dispositif FranceConnect, développé par la Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC).

L'année 2018 a permis à la direction de programme de réaliser de nombreux travaux collaboratifs, contribuant à l'enrichissement du cahier des charges de l'État à l'occasion des Assises de l'identité numérique[149], en avril 2018.

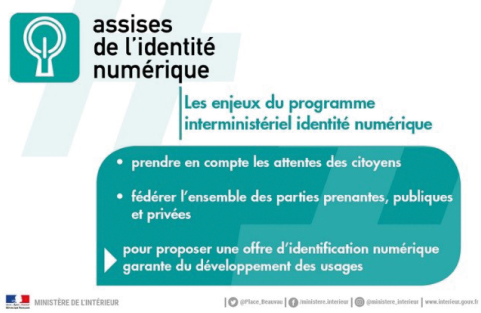


Figure 35 : Assises de l'identité numérique

Réunis lors d'un comité stratégique en décembre 2018, les ministres commanditaires ont validé les orientations majeures d'une stratégie française de l'identité numérique : déployer, dans un premier temps, une carte nationale d'identité électronique (CNIe) à partir de 2021, puis faciliter ultérieurement le développement d'offres privées d'identification.

Aussi, l'année 2019 sera plus opérationnelle et consacrée aux expérimentations, notamment celles des parcours utilisateurs et de la solution régalienne sur *smartphone* portée par le ministère de l'Intérieur (Alicem[150]). Le succès et la généralisation de ces expérimentations constitueront ainsi les prémices d'une politique publique de l'identité numérique, fondée sur le triptyque neutralité-interopérabilité-sécurité.

(148) *Lettre de mission consultable sur :* ***https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Mise-en-place-de-solutions-d-identite-numerique-securisee-lancement-d-un-programme***

(149) *Dossier de presse consultable sur :* ***https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Lancement-des-Assises-de-l-identite-numerique***

(150) *La Direction de la modernisation et de l'action territoriale est en charge de ce projet -* ***https://www.modernisation.gouv.fr/sites/default/files/pia_laureats_vague2.pdf***

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 :

Le constat de menaces persistantes ou nouvelles

Généralités

- **L'évolutivité** des menaces liées au numérique, leur **sophistication** croissante et leur **opportunisme** sont unanimement constatés.
- La **cybercriminalité élargit son spectre d'action** année après année, grâce au développement d'un modèle basé sur la notion de *« cybercrime as a service »* et l'intégration croissante de capacités cyber dans les réseaux criminels traditionnels.
- Corollaire à l'apparition de nouvelles technologies (*Cloud,* IA, *IoT,* 5G…) et aux nouveaux usages, **la surface d'attaque augmente continuellement.** En particulier, en ciblant des périphériques connectés mal sécurisés, les cybercriminels pourront mener des attaques plus préjudiciables et accéder aux réseaux domestiques ou de *smart cities,* voire contrôler des infrastructures critiques tant dans le domaine industriel que celui de la santé.
- Une **complémentarité entre la massification et le ciblage des attaques** est également observée.

Focus sur ces menaces persistantes ou nouvelles

- Les **contenus illicites** représentent un défi majeur et quotidien pour les États. En matière de la lutte contre le terrorisme, le retrait rapide et durable des contenus radicaux implique des efforts partagés, à étendre aux discours de haine. Viralité de l'information sur les réseaux sociaux, phénomènes de manipulation de l'information, enfermement cognitif des usagers, autant de situations qui peuvent rendre nécessaires des mécanismes de régulation spécifiques comme le montrent les travaux des états généraux des nouvelles régulations numériques (EGRN).
- Les ***darknets*** demeurent des plateformes essentielles dans l'organisation de nombreux trafics. La fermeture des grands marchés mondiaux a conduit les cybercriminels à opérer sur des marchés secondaires ou plus spécifiques. Ces *darknets* complexifient le travail des services d'enquête.
- Après les campagnes d'attaques massives par rançongiciel de 2017, un changement de stratégie des cybercriminels peut être observé. Autrefois indiscriminées, les **attaques par rançongiciel** semblent davantage cibler les grandes entreprises ayant la capacité de payer des rançons très élevées.
- La **délinquance liée aux cryptoactifs** se développe : *cryptojacking* (minage clandestin), attaques de plateforme d'échanges, levée de fonds ICO, utilisation de *Bitcards,* escroqueries pyramidales basées sur les cryptoactifs… Elle se tourne vers des cryptomonnaies présentant un anonymat renforcé des transactions.
- Les cybercriminels semblent privilégier des modes opératoires plus difficiles à détecter comme le ***spear-phishing*** ou le ***cryptojacking.*** L'ingénierie sociale reste l'une des techniques cybercriminelles les plus utilisées.
- Les *malwares* bancaires semblent en plein essor sur les *smartphones* et les attaques de distributeurs bancaires par ***jackpotting*** se sont intensifiées et diversifiées.
- Les **applications fausses ou malveillantes** sur *smartphones (Appstores, Play Stores, Markets, etc.)* constituent également un point de vigilance majeur.

Les réponses à apporter aux menaces

Des défis stratégiques

- Le concept de **souveraineté numérique**[151] pose la question de la capacité de l'État à préserver et protéger les intérêts de la Nation. Le champ du numérique étant dominé par des acteurs internationaux[152], la stratégie française devra permettre de faire face à l'ensemble de ces risques ou menaces à travers une gouvernance adaptée. Constituant un patrimoine économique considérable, l'ensemble des leviers doit être aussi utilisé pour **protéger les données.** Sur ce point, le RGPD apparait comme un premier acte européen de souveraineté dans le cyberespace.
- **La gestion des crises cyber** doit être mieux organisée, avec notamment une planification à 360° des actions interministérielles.
- **La maîtrise de la sécurisation de l'identité numérique des citoyens,** dans leurs relations avec l'administration ou les entreprises, est une préoccupation majeure au cœur du projet gouvernemental ; elle permettra de développer des usages numériques plus fluides, de mieux protéger les données et de mieux lutter contre la fraude.

Des défis technico-juridiques

- La protection des systèmes d'information critiques pour la Nation mais aussi celle des intérêts économiques reposent sur un ensemble de fonctions clés pour lesquelles il convient d'avoir recours à des technologies maîtrisées, car leur déficience aurait des conséquences de grande ampleur. La maîtrise de ces **technologies clés du numérique**[153] permettra d'assurer de l'autonomie stratégique nationale.
- Lutter efficacement contre les menaces actuelles ou émergentes implique une **veille efficiente** des modes opératoires et des technologies sous-jacentes, ainsi qu'un développement d'**approches adaptées en matière d'investigations,** tout en intégrant tous les outils et procédés disponibles (IA…).
- Les outils de **chiffrement des données** et d'**anonymisation sur Internet** soulèvent des questions techniques, juridiques et opérationnelles dans la lutte contre la criminalité et le terrorisme ; ils rendent l'accès à la preuve numérique plus complexe.
- L'**exploitation à des fins malveillantes de l'intelligence artificielle** (IA) par des cybercriminels est à envisager à la fois comme vecteur d'attaque mais aussi comme cible d'une attaque. Par exemple, l'usage de techniques de *machine learning* dans les campagnes de *phishing* ou la conception de *DeepFake* dans le premier cas, l'utilisation détournée de *chatbots* dirigés par l'IA dans l'autre.

Des défis culturels

- La **prise de conscience** de chacun face aux risques cyber représente un enjeu majeur. L'état de vigilance que la population a adopté dans le monde physique doit être le même dans le monde numérique, dans **un esprit de continuum de sécurité :** personne ne laisse la porte de son domicile ouverte en son absence, mais beaucoup ne protègent pas leur ordinateur ou leur *smartphone*.
- Il y a trop peu de **dépôts de plaintes.** Pourtant cette démarche positive est primordiale pour l'État (connaissance des modes opératoires) afin d'améliorer la qualité des investigations mais aussi de mettre en œuvre une **prévention plus ciblée** et de meilleure qualité (bulletins d'alerte). Elle est également essentielle aux victimes, particuliers et organisations, qui peuvent être accompagnées ou prises en charge. Par ailleurs ce qui peut apparaitre comme un évènement de faible intensité, peut en réalité faire partie d'un **phénomène de masse** avec des préjudices globaux élevés.

---

(151) Dans son ouvrage éponyme dédié à la souveraineté numérique, Pierre Bellanger la définit comme « la maîtrise de notre destin sur les réseaux informatiques. C'est l'extension de la République dans cette immatérialité informationnelle qu'est le cyberespace ».

*(152) **GAFAM** (Google, Apple, Facebook, Amazon et Microsoft), **NATU** (Netflix, AirBnB, Tesla et Uber), **BATX** (Baidu, Alibaba, Tencent et Xiaomi)…*

(153) Trois exemples de telles technologies clés sont cités dans la revue stratégique de cyberdéfense de février 2018 : les technologies de chiffrement des communications, les radiocommunications sécurisées et les sondes de détection des attaques informatiques.

- Une **gouvernance spécifique de l'éthique en intelligence artificielle et des algorithmes** devrait être adoptée pour faire émerger des technologies conformes à nos valeurs et nos normes sociales[154]

Des défis territoriaux

- L'organisation et la mise en cohérence des **actions de prévention dans les territoires** constituent une voie de progrès pour le ministère de l'Intérieur ainsi que les autres acteurs impliqués dans la sécurité de l'espace numérique.
- Face à la concentration de l'offre de sécurité numérique dans les espaces urbains, le développement d'une **offre de proximité** est pourtant indispensable dans les territoires et pour tous les publics.

Des publics de plus en plus vulnérables et insuffisamment sensibilisés

Les particuliers

- À l'instar de la cyberattaque lors de la cérémonie d'ouverture des JO d'hiver 2018, les **grands événements** constituent aujourd'hui des surfaces d'attaque à prendre en compte, notamment en vue de la tenue en France de la coupe du monde de rugby 2023 ou des JO 2024, tant pour les organisateurs, les sportifs que le public.

Les organisations : entreprises, administrations, collectivités territoriales…

- À mesure que l'environnement numérique se complexifie, les dispositifs de cybersécurité deviennent de moins en moins efficaces. Les *hackers* cherchent à compromettre la **chaîne de valeur des organisations,** qu'elle soit physique (terminaux de l'entreprise ou appareils des collaborateurs – *BYOD*) ou logicielle (cas du logiciel de comptabilité ukrainien *MeDoc* lors de la crise *NotPetya* ou *CCleaner*).
- Dans un contexte où les flux sont à la fois physiques et numériques, l'interdépendance des entreprises les expose à la défaillance d'un membre de leur écosystème. En conséquence, la **chaîne d'approvisionnement** *(supply chain)* constitue un véritable défi pour la sécurité numérique des entreprises.
- Lors de crises cyber majeures, il est régulièrement constaté la mise hors service de terminaux informatiques. Afin de permettre de limiter l'impact de ces destructions, leur remplacement doit être prévu dans le **plan de continuité d'activité** (PCA). Les entreprises sont vivement encouragées à élaborer systématiquement, tester et évaluer de tels plans.
- La **protection des espaces intelligents** publics ou privés (territoires, quartiers, bâtiments…) constitue un défi, compte tenu de la diversité et de l'hétérogénéité des niveaux de sécurité des capteurs et objets connectés. Si l'entrée en vigueur du RGPD a sensibilisé les collectivités territoriales à l'atteinte aux données en 2018, cette prise de conscience des risques numériques liés aux espaces intelligents doit se poursuivre.

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

Annexe I : 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 (Gendarmerie nationale)
CESIN	Club des Experts de la Sécurité de l'Information et du Numérique
CJUE	Cour de justice de l'Union européenne
CLUSIF	Club de la sécurité de l'information français
CNIL	Commission nationale informatique et libertés
Cryptolocker	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
DGSI	Direction générale de la sécurité intérieure
EC3	*European Cybercrime Centre* (Europol)
FOVI	Escroquerie aux faux ordres de virement internationaux
GCP	Groupe de contact permanent (État - 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
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
OCRVP	Office central pour la répression des violences aux personnes
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 d'un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services
PJGN	Pôle judiciaire de la Gendarmerie nationale, localisé à Pontoise (95)
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. Entré en application le 25/05/18
SCRC	Service central de renseignement criminel (Gendarmerie nationale)
SDLC	Sous-direction de lutte contre la cybercriminalité (direction centrale de la police judiciaire - 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

Annexe 2: Synthèse du rapport *« Internet Organised Crime Threat Assessment »* (IOCTA) 2018

Les rançongiciels demeurent un phénomène criminel préoccupant.

Les cyber-attaquants, motivés par l'appât d'un gain financier, privilégient encore les rançongiciels aux chevaux de Troie bancaires. Cette tendance devrait se poursuivre au cours des prochaines années.

De nombreux rapports publics attribuent de plus en plus de cyberattaques mondiales aux États. L'objectif poursuivi n'est alors plus exclusivement financier mais aussi de déstabilisation.

Quant aux *malwares* qui se propagent via les *smartphones,* s'ils n'ont pas été spécifiquement signalés à l'agence européenne en 2017, ils sont résolument identifiés comme un risque numérique dont on doit se prémunir.

La protection des données est un enjeu majeur.

Les criminels utilisent souvent les données piratées pour réaliser d'autres activités illicites. En 2017, le détournement de données le plus important concernait *Equifax,* affectant plus de 100 millions d'utilisateurs dans le monde.
Avec l'entrée en vigueur du règlement européen général sur la protection des données à caractère personnel (RGPD) le 25 mai 2018, le signalement d'une intrusion dans les systèmes entrainant un détournement des données personnelles est désormais une obligation légale dans l'ensemble de l'UE. Le non-respect de cette obligation de communication est sanctionné par de lourdes amendes. Le RGPD est considéré par Europol comme un nouveau challenge pour les entreprises.

Les attaques par déni de service distribué (DDoS) ont continué à proliférer, devenant l'une des principales menaces pour presque tous les secteurs exposés à l'Internet.

65 % des forces de police européennes ont rapporté des cas de DDoS et un tiers d'entre elles ont souligné un nombre croissant de cas tout au long de l'année 2017.
Le secteur financier considère aussi le DDoS comme l'une des principales menaces. L'ENISA rapporte que plus d'un tiers des organisations ont subi une attaque DDoS en 2017, contre 17 % pour l'année 2016. D'autres rapports du secteur privé suggèrent que les attaques en DDoS représentent environ 70 % de tous les incidents compromettant l'intégrité du réseau.
Ces types d'attaque peuvent provenir de sources variées, notamment les « hacktivistes », les cybercriminels qui cherchent à en tirer un profit financier ou encore les groupes de pirates informatiques travaillant pour le compte d'un État. Les motivations peuvent ainsi être variées : idéologiques, politiques ou financières.
Les attaques DDoS sont désormais démocratisées : le processus pour lancer des attaques DDoS est aujourd'hui très simple et ne nécessite aucune compétence technique particulière. Les logiciels permettant de perpétrer ces attaques sont facilement accessibles et très abordables. D'où l'accroissement des attaques DDoS, aussi bien en termes de fréquence que d'échelle (en seconde place après les *malwares* en 2017).

Une production de plus en plus importante du matériel pédopornographique.

La quantité de matériel pédophile en ligne issu de l'exploitation sexuelle d'enfants, y compris le « matériel explicite auto-généré » (SGEM – c'est-à-dire du matériel fourni par l'enfant ou l'adolescent contraint d'envoyer des photos de lui ou d'elle nu(e)), continue d'augmenter. 60 % des États membres constatent une augmentation de la diffusion de matériel pédopornographique sur Internet.
Bien que la majorité du matériel pédopornographique reste partagée sur des plates-formes P2P, des contenus plus extrêmes sont diffusés sur les *darknets*.
En outre, les investigations sur les abus sexuels des enfants à distance (LDCA – c'est-à-dire la diffusion d'un abus sexuel en direct et en *streaming*), sont particulièrement difficiles à diligenter, notamment en raison de l'aspect transfrontalier de ces enquêtes et des technologies d'anonymisation et de chiffrement utilisées par les auteurs.

Alors que de plus en plus de jeunes enfants ont accès à Internet et à des plateformes de médias sociaux, le risque de contrainte (en vue d'obtenir des photos ou vidéos sexuellement explicites) et d'extorsion en ligne continue de croître.
La popularité des applications de médias sociaux offrant des possibilités de *streaming* intégré a entraîné une augmentation significative de la quantité de matériel pédopornographique diffusé en direct sur ces plateformes.

Les fraudes sans présence de la carte (*card-not-present* ou CNP) sont aujourd'hui les plus courantes, mais l'usage de la technique du *skimming* perdure.

Désormais moins répandues que les fraudes CNP, les fraudes en présence de la carte restent tout de même d'actualité dans la plupart des États membres de l'UE, à l'image du *skimming*. Cette fraude tend toutefois à diminuer en raison de l'adoption d'un certain nombre de mesures efficaces visant à restreindre l'utilisation de la carte à l'étranger *(card control)*. Il s'agit notamment du géoblocage ou géocontrôle : la carte ne peut être utilisée que dans certains pays.
Les données des cartes *« skimmées »* sont souvent vendues via les *darknets* et l'argent décaissé dans des zones où la mise en œuvre du standard *Europay MasterCard Visa* (EMV) est lente ou inexistante.
La « fraude au péage » a fait l'objet d'une attention particulière cette année. Les groupes criminels utilisent en effet des cartes de paiement contrefaites (y compris cartes d'essence) pour éviter de payer des frais de péage.
De nombreux États membres ont également signalé une augmentation de la création de sociétés factices pour accéder illégalement à des points de vente, et pour tirer parti des informations ainsi compromises.
La fraude sans présence de la carte reste une menace majeure pour les États membres de l'UE. Elle se déroule sans utilisation concrète de la carte, mais les coordonnées bancaires de son propriétaire sont volées et utilisées illégalement. Les secteurs du transport et de la vente au détail sont particulièrement ciblés.

Le développement des cryptomonnaies.

Les rapports iOCTA précédents indiquaient que les criminels utilisaient de plus en plus des cryptomonnaies pour financer leurs activités criminelles.
Bien que le *Bitcoin* ait perdu des parts dans le marché global des cryptomonnaies, il reste la devise principale rencontrée par les services de police dans leurs enquêtes.
Les marchands de devises, les services de création de crypto-devises et les détenteurs de portefeuilles sont confrontés à des tentatives de piratage, d'extorsion de données à caractère personnel et de vol.
Les cryptomonnaies sont de plus en plus utilisées afin de blanchir des fonds provenant d'une activité illicite. Le recours aux cryptomonnaies est de plus en plus facilité par des phénomènes émergents, tels que les échanges décentralisés qui permettent des échanges sans aucune obligation de connaître son client *(« Know Your Customer »)*.

Le *cryptojacking* ou minage de cryptomonnaie malveillant : une nouvelle menace

Les logiciels malveillants de minage de cryptomonnaie ont été l'une des formes les plus prolifiques de logiciels malveillants distribués par les cybercriminels en 2018. Ils détournent secrètement la puissance de traitement des machines infectées pour générer de la cryptomonnaie pour le compte du cybercriminel. Le *cryptojacking* peut ralentir l'ordinateur de la victime. Il peut aussi cacher ou préparer d'autres attaques.

L'ingénierie sociale reste l'une des techniques cybercriminelles les plus utilisées

Le *phishing* par courrier électronique reste la forme d'ingénierie sociale la plus fréquente, les *vishing* (par téléphone) et les *smishing* (par SMS) étant moins courants.
L'objectif poursuivi est d'obtenir des données personnelles, pirater des comptes, voler des identités, initier des paiements frauduleux ou convaincre la victime de poursuivre toute autre activité contraire à son intérêt personnel, telle que le transfert d'argent ou le partage de données personnelles.

Les marchés cybercriminels prospèrent sur les darknets en dépit d'une certaine instabilité.

En 2017, les services de police ont fermé trois des plus grands marchés du *Darknet :* AlphaBay, Hansa et RAMP. Ces opérations policières ont incité les utilisateurs à migrer vers d'autres marchés ou plateformes, telles que les applications de communication cryptées.
La fermeture de ces grands marchés mondiaux du *Darknet* a entraîné une augmentation du nombre de marchés secondaires (souvent plus petits) ouverts à des groupes linguistiques particuliers ou de nationalités spécifiques.

La convergence du cyber et du terrorisme.

L'État islamique (EI) continue d'utiliser Internet pour diffuser de la propagande et pour inciter à la commission d'actes de terrorisme.
Les actions menées par les services de police et par les entreprises du web ont conduit les sympathisants de Daesh à s'adapter. Ils s'organisent via des services de messagerie cryptée (Telegram est cité) pour assurer une présence sur les grands médias sociaux (Twitter, Gmail et Instagram).
Même si les sympathisants de Daesh ont exprimé leur volonté d'acheter des outils et des services aux fins de lancer des cyberattaques, leurs propres capacités internes semblent limitées. Les sympathisants de l'EI ont réussi un petit nombre de défacements et des piratages de faible niveau (tel que le piratage de la station de radio suédoise en novembre 2017 durant lequel le pirate a joué un *Nashid* de recrutement pour l'EI). En mars 2018, l'EI a tenté de mettre à disposition de ses sympathisants un réseau social *« Muslim's Network »*, mais ce fut un échec. Enfin, le recours aux monnaies virtuelles pour financer des attaques terroristes reste marginal.

Annexe 3 : Contacts utiles pour lutter contre les cybermenaces

Plateformes de signalement

> ***https://www.pre-plainte-en-ligne.gouv.fr/ :*** Ce service vous permet d'effectuer une déclaration pour des faits dont vous êtes directement et personnellement victime et pour lesquels vous ne connaissez pas l'auteur, concernant une atteinte aux biens (vols, dégradation, escroqueries…) ou un fait discriminatoire (discrimination, diffamation, injure, provocation individuelle à la haine). Cette démarche vise à vous faire gagner du temps lors de votre présentation à l'unité ou service choisi.

> ***https://www.internet-signalement.gouv.fr :*** plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (PHAROS) du ministère de l'Intérieur, elle traite notamment des contenus illicites du web et constitue un point d'entrée unique des signalements liés à l'ensemble des infractions pénales.

> ***https://www.service-public.fr/cmi :*** cette plateforme permet de signaler en ligne les violences sexuelles et sexistes, 24 heures sur 24 et 7 jours sur 7, ainsi qu'un échange individualisé (« tchat »).

> ***https://www.service-public.fr/particuliers/vosdroits/R46526 :*** Signaler une fraude à la carte bancaire sur PERCEVAL : plateforme électronique de recueil des coordonnées bancaires et de leurs conditions d'emploi rapportées par les victimes d'achat frauduleux en ligne.

> ***https://www.signal-spam.fr/ :*** cette plateforme donne la possibilité aux internautes de signaler tout ce qu'ils considèrent être un *spam* dans leur messagerie afin de l'assigner ensuite à l'autorité publique ou au professionnel qui saura le mieux prendre l'action qui s'impose pour lutter contre le *spam* signalé.

> ***https://phishing-initiative.fr/contrib/ :*** cette plateforme offre aux internautes la possibilité de lutter contre les attaques d'hameçonnage en signalant de manière simple des liens suspects, analysés par des experts : les liens effectivement frauduleux sont alors retranscrits sur les listes noires des principaux navigateurs web.

> ***https://www.pointdecontact.net/ :*** Cette plateforme de l'association *Point de Contact* permet le signalement anonyme de contenu choquant et la qualification juridique des contenus illicites.

> À venir, Thésée : dépôt de plainte en ligne pour certaines escroqueries sur Internet.

Assistance téléphonique/électronique et remédiation

> ***0 805 805 817 :*** Info Escroqueries est une plateforme téléphonique à l'attention des particuliers et/ou des entreprises, composée de policiers et de gendarmes, chargée d'informer, conseiller et orienter les personnes victimes d'une escroquerie.

> ***https://www.cybermalveillance.gouv.fr/ :*** plateforme du dispositif national d'assistance aux victimes de cyber malveillances (GIP ACYMA), visant à améliorer la prévention et l'assistance aux victimes, qu'il s'agisse de collectivités territoriales, d'entreprises ou de particuliers.

> ***https://www.nomoreransom.org/fr :*** *No more ransom !* est un portail mis en place par EUROPOL pour aider les victimes d'un *ransomware* (ou rançongiciel).

Sensibilisation et bonnes pratiques sur les réseaux sociaux

Twitter :

> @Place_Beauvau

> @Gendarmerie ; @PoliceNationale ; @prefpolice

Facebook :

> @ministère.intérieur

> @gendarmerienationale ; @PoliceNationale ; @prefecturedepolice

Instagram :

> @ministère.intérieur

> @gendarmerie_nationale_officiel ; @policenationale

Télécharger le rapport relatif à l'état de la menace liée au numérique 2017 :
https://www.ladocumentationfrancaise.fr/rapports-publics/174000226/index.shtml

Télécharger le rapport relatif à l'état de la menace liée au numérique 2018 :
https://www.ladocumentationfrancaise.fr/rapports-publics/184000391/index.shtml

ÉQUIPE ÉDITORIALE

Le présent rapport a été établi grâce aux contributions :

- de la Préfecture de Police de Paris ;
- des directions générales du ministère : police nationale, gendarmerie nationale, sécurité intérieure, sécurité civile et gestion des crises ;
- du service statistique ministériel de la sécurité intérieure ;
- du secrétariat général du ministère : service du haut fonctionnaire de défense, direction des libertés publiques et des affaires juridiques, délégation à l'information et à la communication, délégué ministériel à la protection des données ;
- de la direction de programme « identité numérique » ;
- et du ministère de la Justice (pôle d'évaluation des politiques pénales de la direction des affaires criminelles et des grâces et section F1 du parquet de Paris).

Sa rédaction a été réalisée par la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, sous la direction du colonel Philippe Baudoin : commissaire divisionnaire Adeline Champagnat, madame Alexandra Ketcheyan, commissaire divisionnaire François Thierry et monsieur Thierry Vinçon.

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

CONCEPTION RÉALISATION

MI-SG/DICOM