Conseil de
l'Union européenne

Bruxelles, le 26 novembre 2015
(OR. fr)

7588/2/15
REV 2 DCL 1

GENVAL 9
CYBER 23

DÉCLASSIFICATION

du document:	7588/2/15 REV 2 RESTREINT UE/EU RESTRICTED
en date du:	9 septembre 2015
Nouveau statut:	Public
Objet:	**Rapport d'évaluation sur la septième série d'évaluations mutuelles "Mise en œuvre pratique et fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci"** - **Rapport sur la France**

Les délégations trouveront ci-joint la version déclassifiée du document cité en objet.

Le texte de ce document est identique à celui de la version précédente.

Conseil de
l'Union européenne

Bruxelles, le 9 septembre 2015
(OR. fr)

7588/2/15
REV 2

RESTREINT UE/EU RESTRICTED

GENVAL 9
CYBER 23

RAPPORT

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
Objet:	**Rapport d'évaluation sur la septième série d'évaluations mutuelles "Mise en œuvre pratique et fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci"** - **Rapport sur la France**

TABLE DES MATIÈRES

1 RESUME

- La mission d'évaluation en France s'est déroulée dans un climat très positif. Elle a bénéficié d'une excellente préparation par les autorités françaises et notamment du soutien remarquable du Secrétariat Général aux Affaires européennes (SGAE) qui a coordonné l'exercice. Cet aspect mérite d'autant plus d'être souligné que la visite en France était la première du 7e cycle d'évaluation, en sorte que les autorités nationales n'avaient pu bénéficier de l'expérience de précédentes visites.

- Tous les services rencontrés sur place étaient très bien préparés et ont pu s'exprimer en toute transparence, en faisant preuve d'une grande capacité d'écoute et d'ouverture. L'équipe d'évaluation a été agréablement frappée par le haut degré de motivation et d'investissement des praticiens interrogés.

- Après avoir mis l'accent sur les enjeux de cyberdéfense et cybersécurité, la France a enclenché un processus national de réflexion, aujourd'hui très avancé, en matière de lutte contre la cybercriminalité ; un groupe de travail pluridisciplinaire a notamment été constitué sous l'égide d'un haut magistrat (Groupe de travail interministériel sur la lutte contre la cybercriminalité présidé par le procureur général Marc ROBERT) pour établir une stratégie complète dans ce domaine. Cette stratégie est en cours de mise en œuvre. L'équipe d'évaluation salue cette initiative remarquable dont les autres Etats membres pourraient s'inspirer.

- L'une des principales conclusions du rapport du groupe interministériel sur la lutte contre la cybercriminalité présidé par le procureur général Marc ROBERT, publié en février 2014, est que la priorité doit être donnée à une prise en compte plus efficace du caractère transversal du phénomène cybercriminel ; l'approche française, tout en étant très volontariste, est jusqu'à présent relativement cloisonnée : il n'y a pas encore d'instance nationale de coordination et la coopération entre les nombreux acteurs publics concernés reste empirique, au risque de lacunes et de chevauchements.

- Depuis l'adoption de la loi informatique et libertés de 1978, la France s'est progressivement dotée d'un arsenal juridique important qui incrimine aussi largement que possible les faits relevant de la cybercriminalité. La législation pénale française opère un renforcement graduel des peines et facilite les investigations policières selon la gravité des infractions, en particulier pour viser la criminalité organisée. Cet ensemble de normes est régulièrement mis à jour pour assurer la transposition des instruments européens et s'adapter aux évolutions des comportements criminels. Il persiste cependant des contraintes procédurales qui nécessiteraient une meilleure adaptation des règles de recherche et d'obtention des preuves à la réalité du monde numérique.

- Les autorités policières ont manifestement fait de l'enjeu une priorité et se sont en général dotées de moyens et d'outils à sa hauteur ; des formations spécifiques sont dispensées aux praticiens concernés ; l'action respective des différents corps spécialisés est intense et paraît très efficace, bien qu'elle paraisse pouvoir être mieux coordonnée.

- Par contraste, les autorités judiciaires ne traitent pas la cybercriminalité comme un phénomène en tant que tel ; la politique des poursuites est insuffisamment consolidée au plan central et il n'y a pas de filière judiciaire spécialisée apte à compléter la chaîne pénale et à en assurer l'efficacité globale ; les formations offertes aux magistrats dans ce domaine mériteraient d'être renforcées. Pour pallier ces difficultés et donner suite au rapport du groupe interministériel sur la lutte contre la cybercriminalité présidé par le procureur général Marc ROBERT le Ministère de la Justice vient de créer un service horizontal partiellement dédié à la lutte contre la cybercriminalité.

- Les partenariats public-privé sont nombreux ; certains sont d'envergure nationale et de nombreux autres, plus ponctuels, sont réalisés à l'initiative des praticiens et en particulier des services de police et de gendarmerie qui multiplient les bonnes pratiques dans ce domaine.

- Les autorités françaises ont regretté que d'importants obstacles à la coopération européenne et internationale subsistent, même en ce qui concerne l'échange d'informations élémentaires telles qu'une adresse IP. L'assistance fournie par Europol/EC3 est très appréciée. Les possibilités offertes par Eurojust pour faciliter la coopération judiciaire, y compris avec les Etats tiers, sont encore relativement mal connues et sous-utilisées.

2 INTRODUCTION

À la suite de l'adoption de l'action commune 97/827/JAI du 5 décembre 1997[1], un mécanisme d'évaluation de l'application et de la mise en œuvre au niveau national des engagements internationaux en matière de lutte contre la criminalité organisée avait été mis en place. Conformément à l'article 2, le groupe "Questions générales, y compris l'évaluation" (GENVAL) a décidé, lors de la réunion du 3 octobre 2013, que la septième série d'évaluations mutuelles serait consacrée à la mise en œuvre pratique et au fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci.

Les États membres ont accueilli favorablement le choix de la cybercriminalité comme objet de la septième série d'évaluations mutuelles. Toutefois, compte tenu du large éventail d'infractions qui relèvent de la cybercriminalité, il a été décidé de concentrer l'évaluation sur les infractions auxquelles les États membres estiment qu'il convient d'accorder une attention particulière. À cette fin, l'évaluation porte sur trois domaines spécifiques, à savoir les cyberattaques, les abus sexuels commis en ligne contre des mineurs et la pédopornographie sur Internet, et la fraude en ligne aux cartes de paiement; elle devrait fournir un examen complet des aspects juridiques et opérationnels de la lutte contre la cybercriminalité, de la coopération transfrontière et de la coopération avec les agences compétentes de l'UE. La directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants ainsi que la pédopornographie[2] (date de transposition: 18 décembre 2013) et la directive 2013/40/UE relative aux attaques contre les systèmes d'information[3] (date de transposition: 4 septembre 2015) revêtent une importance particulière dans ce contexte.

1 Action commune 97/827/JAI du 5 décembre 1997, JO L 344 du 15.12.1997, p. 7-9.
2 JO L 335 du 17.12.2011, p. 1.
3 JO L 218 du 14.8.2013, p. 8.

En outre, dans ses conclusions de juin 2013 concernant la stratégie de cybersécurité de l'UE[4], le Conseil rappelle l'objectif visant à ratifier dans les meilleurs délais la convention du Conseil de l'Europe du 23 novembre 2001 sur la cybercriminalité (convention de Budapest)[5] et souligne dans ses considérants que "l'UE ne préconise pas la création de nouveaux instruments juridiques internationaux concernant les questions inhérentes au cyberespace". La convention de Budapest s'accompagne d'un protocole relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques[6].

L'expérience des évaluations précédentes montre que la mise en œuvre des instruments juridiques concernés est à des stades différents selon les États membres; le processus d'évaluation en cours pourrait aussi apporter une contribution utile aux États membres qui n'auraient pas mis en œuvre tous les aspects des divers instruments. L'évaluation se veut néanmoins large et interdisciplinaire; elle ne se concentre pas uniquement sur la mise en œuvre des différents instruments en matière de lutte contre la cybercriminalité mais aussi sur les aspects opérationnels dans les États membres.

Dès lors, outre la coopération avec les services chargés des poursuites, elle couvrira également la coopération entre les autorités de police, d'une part, et Eurojust, l'ENISA et Europol/EC3, d'autre part, et le retour d'information de ces acteurs vers les services de police et les services sociaux compétents. L'évaluation se concentre sur la mise en œuvre des politiques nationales en ce qui concerne l'élimination des cyberattaques et de la fraude en ligne, ainsi que de la pédopornographie. Elle couvre également les pratiques opérationnelles des États membres pour ce qui est de la coopération internationale et de l'assistance proposée aux personnes qui sont victimes de la cybercriminalité.

4 Doc. 12109/13 POLGEN 138 JAI 612 TELECOM 194 PROCIV 88 CSC 69 CIS 14 RELEX 633 JAIEX 55 RECH 338 COMPET 554 IND 204 COTER 85 ENFOPOL 232 DROIPEN 87 CYBER 15 COPS 276 POLMIL 39 COSI 93 DATAPROTECT 94.

5 STE nº 185, ouverte à la signature le 23 novembre 2001 et entrée en vigueur le 1er juillet 2004.

6 STE nº 189, ouverte à la signature le 28 janvier 2003 et entrée en vigueur le 1er mars 2006.

L'ordre des visites dans les États membres a été adopté par le groupe GENVAL le 1 avril 2014. La France est le premier État membre évalué au cours de cette série d'évaluations. Conformément à l'article 3 de l'action commune, une liste d'experts a été établie par la présidence en vue des évaluations à mener. Les États membres ont désigné des experts possédant une connaissance pratique étendue dans le domaine concerné sur la base d'une demande écrite que le président du groupe GENVAL a adressée aux délégations le 28 janvier 2014.

Les équipes d'évaluation se composent de trois experts nationaux, assistés de deux fonctionnaires du Secrétariat général du Conseil et d'observateurs. Pour la septième série d'évaluations mutuelles, le groupe GENVAL a approuvé la proposition de la présidence selon laquelle la Commission européenne, Eurojust, Europol/EC3 et l'ENISA devraient être invités en tant qu'observateurs.

Les experts chargés de l'évaluation de la France étaient MM. Konstantinos SKOUVARIS (Grèce), Laurent THYES (Luxembourg) et Yves VANDERMEER (Belgique). Quatre observateurs étaient également présents: M[mes] Julie RUFF (Commission), Catherine DEBOYSER (Eurojust) et Andrea DUFKOVA (ENISA) et M. Benoît GODART (Europol/EC3), ainsi que M. Gilles DUVAL et M[me] Claire ROCHETEAU du secrétariat général du Conseil.

Le présent rapport a été élaboré par l'équipe d'experts avec l'assistance du Secrétariat général du Conseil, sur la base des constatations issues de la visite d'évaluation effectuée en France du 28 au 31 octobre 2015, ainsi que des réponses détaillées de la France au questionnaire d'évaluation, accompagnées de ses réponses détaillées aux questions qui ont suivi.

3 QUESTIONS GENERALES ET STRUCTURES

3.1 Stratégie Nationale en matière de Cybersecurité

L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) est l'autorité française chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de défense et de sécurité des systèmes d'information. L'ANSSI est au cœur de la définition et de la mise en œuvre de la politique de cyberdéfense et de cybersécurité en France.

Spécialisée dans la protection, la défense et la restauration des systèmes d'information des infrastructures critiques, publiques et privées, cette agence bénéficie de moyens conséquents, à la hauteur de la priorité donnée à ses missions ; les ressources humaines pluridisciplinaires qui lui sont affectées sont en augmentation depuis sa création en 2009 (100 postes) et devraient atteindre près de 700 postes en 2017. Ces moyens sont nettement plus élevés que ceux qui sont affectés aux autorités répressives pour la lutte contre la cybercriminalité (par comparaison, les différents services centraux de police judiciaire spécialisés dans ce domaine comportent en tout environ 250 enquêteurs).

L'ANSSI ne traite pas la cybercriminalité en tant que telle mais de ses conséquences sur les systèmes d'information ; elle informe les victimes de leur droit de porter plainte sans signaler elle-même aux autorités compétentes les faits délictueux dont elle a connaissance.

L'ANSSI a publié, en février 2011, une stratégie nationale[7] qui est actuellement en cours d'actualisation ; sa nouvelle version devrait être disponible mi-2015.

7 La partie publique de la stratégie française est disponible à l'adresse http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/une-autorite-nationale-et-une-strategie-pour-defendre-et-proteger-la-france.html
Une version EN et une version DE sont disponibles.

Cette stratégie nationale se décline en quatre objectifs :

- être une puissance mondiale de cyberdéfense et appartenir au premier cercle des nations majeures dans ce domaine tout en conservant son autonomie,
- garantir la liberté de décision de la France par la protection de l'information de souveraineté,
- renforcer la cybersécurité des infrastructures vitales nationales,
- assurer la sécurité dans le cyberespace,

et sept axes d'action:

- le développement des capacités d'anticipation et d'analyse,
- L'amélioration des capacités de détection, d'alerte et de réaction,
- L'augmentation et la pérennisation des capacités scientifiques, techniques, industrielles et humaines,
- La protection des systèmes d'information de l'État et des opérateurs d'infrastructures vitales,
- L'adaptation du droit,
- Le développement des collaborations internationales,
- La communication pour informer et convaincre.

3.2 Priorités nationales en matière de cybercriminalité

La lutte contre la cybercriminalité est visée par le 4e objectif de la stratégie de cybersécurité mentionnée ci-dessus. Intitulé "*Assurer la sécurité dans le cyberespace*", cet objectif encourage :

- l'adaptation du droit aux évolutions technologiques et aux nouveaux usages de l'internet,
- le renforcement de l'entraide judiciaire internationale en matière de répression des infractions commises sur ou à travers les réseaux de communications électroniques,
- l'information et la sensibilisation des entreprises et des particuliers aux risques encourus,
- l'information des victimes et leur accompagnement.

3.2.1 Stratégie du Ministère de l'Intérieur sur les cybermenaces

Sur ces bases et sur celles issues des travaux du groupe de travail ayant réuni l'ensemble de ses directions générales le Ministère de l'Intérieur a élaboré sa propre **stratégie ministérielle sur les cybermenaces,** qui définit 6 axes stratégiques :

- axe 1 : disposer en permanence d'une vision claire et actualisée de l'état des cybermenaces ;
- axe 2 : adapter et renforcer les capacités de réponse du Ministère contre les cybermenaces ;
- axe 3 : améliorer le niveau de sensibilisation et de prévention contre les cybermenaces des particuliers, des acteurs économiques et des collectivités territoriales ;
- axe 4 : préparer l'avenir par un effort de recherche et développement, associant le monde académique et les industriels ;
- axe 5 : renforcer le niveau de sécurité des systèmes d'information propres au Ministère ;
- axe 6 : promouvoir l'action internationale du Ministère dans le domaine de la lutte contre les cybermenaces.

Ce plan d'action est piloté depuis décembre 2014 par le préfet chargé de la lutte contre les cybermenaces à qui a été confié la mission de préfiguration d'une délégation à la lutte contre les cybermenaces qui sera rattachée au cabinet du Ministre de l'Intérieur.

L'une des premières concrétisations de la mise en œuvre de cette stratégie ministérielle et, en particulier de l'axe n°2, est la création de la Sous-Direction de la Lutte contre la Cybercriminalité (SDLC) au sein de la Direction Centrale de la Police Judiciaire (DCPJ) en avril 2014.

Cette création vise à adapter le dispositif de la police nationale à la généralisation de l'utilisation des nouvelles technologies dans la commission des infractions, par la mise en place d'une structure traitant de toutes les dimensions de la lutte contre la cybercriminalité, dans les domaines de l'opérationnel, de la formation et de la prévention du grand public et du tissu économique.

L'équipe d'évaluation salue cette réorganisation très utile, dont elle a trouvé une description détaillée dans la réponse française au questionnaire GENVAL. Les évaluateurs souhaitent souligner ici le projet de renforcement des capacités nationales **de protection des systèmes d'information** apportant un soutien aux petites et moyennes entreprises et au grand public en matière de cyberattaques, faisant l'objet d'un travail interministériel copiloté par le Ministère de l'intérieur et l'ANSSI.

3.2.2 Groupe de travail interministériel sur la lutte contre la cybercriminalité

Enfin, en juin 2013, un **groupe de travail interministériel sur la lutte contre la cybercriminalité** a été spécifiquement constitué par les ministres compétents (Justice, Economie et Finances, Intérieur, Economie numérique).

Le mandat donné au président du groupe de travail interministériel, M. le Procureur Général Marc ROBERT, portait sur **l'élaboration d'une stratégie globale de lutte contre la cybercriminalité.**

Ce groupe a présenté, en février 2014, un rapport [8] très détaillé dont les constats débouchent sur une série de 55 recommandations qui couvrent aussi bien des aspects d'organisation, de législation, de prévention et de sensibilisation du public, d'adaptation des moyens d'enquête et de répression, de formation des professionnels et de renforcement de la coopération internationale.

Un constat préalable fait par le groupe de travail réside dans la nécessité de **mieux définir et connaître le phénomène de la cybercriminalité**. Pour ce faire, il propose de clarifier cette notion, de créer un observatoire chargé de rassembler et de mettre en cohérence toutes les données relatives à ce phénomène et de développer des enquêtes de victimation auprès des particuliers et des entreprises.

Autre point essentiel développé par le rapport : la **prévention de la cybercriminalité**. Pour la renforcer, le groupe préconise notamment le lancement de campagnes de sensibilisation destinées au grand public, la formation de l'internaute - « premier acteur de sa propre sécurité » - et la mobilisation de tous les professionnels concernés pour trouver des réponses techniques appropriées.

[8] http://www.Justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

Pour les auteurs de ce rapport, il apparaît également nécessaire de **renforcer les moyens de lutte contre la cybercriminalité**. Plusieurs dispositions sont proposées pour parvenir à cette fin : la mise en place d'un centre d'alerte et de réaction aux attaques informatiques (il est préconisé que ce CERT grand public soit sous forme associative cf. recommandation n° 6), un renforcement de la formation des magistrats, des policiers, des gendarmes et des douaniers ainsi que la création d'une délégation interministérielle et la création, au sein du Ministère de la Justice, d'un service horizontal dédié à la lutte contre la cybercriminalité.

Les autorités françaises n'ont pas précisément indiqué lesquelles des recommandations du groupe ROBERT seraient en définitive retenues et sur quels critères les choix seraient faits. Toutefois l'importance que ces recommandations soient suivies d'effet a été soulignée à de nombreuses reprises au cours de la visite sur place.

Le 15 janvier 2015 le Ministère de la Justice a informé l'équipe d'évaluation qu'il venait de mettre en œuvre une première recommandation le concernant, relative à la création d'un service horizontal dénommé "mission de coordination de la lutte contre les atteintes à la probité et la cybercriminalité". Ce service sera notamment chargé de coordonner les actions de prévention et de lutte contre la cybercriminalité en mettant en œuvre les recommandations du rapport ROBERT, de coordonner la définition des instructions générales de politique pénale adressées aux procureurs généraux ainsi que la contribution française aux travaux des instances européennes et internationales dans son domaine de compétence.

3.2.3 Liens avec la priorité "Cybercriminalité" de l'UE

Les priorités nationales prennent en compte en partie les objectifs stratégiques définis par l'UE dans le cadre de la priorité "Cybercriminalité". De même les travaux du groupe ROBERT s'inscrivent dans la stratégie européenne définie en février 2013 et les recommandations contenues dans son rapport ont été élaborées en tenant compte des outils européens existants en matière de lutte contre la cybercriminalité.

A titre d'exemples d'initiatives françaises rejoignant des priorités européennes, l'on peut citer :
- le livre blanc sur la défense et la sécurité nationales de juin 2008, puis le nouveau Livre Blanc d'avril 2013,
- la création de l'Agence Nationale de Sécurité des Systèmes de l'Information en juillet 2009,
- la création d'une plate-forme de signalements des contenus illicites de l'internet
- la mise en place de groupes de travail spécialisés, tels que l'Observatoire de la sécurité des cartes de paiement établi auprès de la Banque de France.

La France met également en œuvre une politique axée sur la prévention, le développement des signalements et la formation des acteurs notamment en matière de prévention.

Ainsi elle participe au programme européen ***Safer Internet***, financé par la Commission européenne, placé en France sous l'égide de la Délégation aux usages de l'internet depuis 2005. Safer Internet France fédère trois services complémentaires en matière d'éducation et de protection des mineurs :

- Le programme national de sensibilisation des jeunes aux risques et enjeux de l'internet *« Internet sans crainte* »
- Le service de signalement des contenus choquants « *Pointdecontact* » géré par l'association des fournisseurs d'accès et de service sur internet (AFA).
- Le numéro national d'accueil et d'assistance pour la protection des jeunes « Net Ecoute » géré par l'association E-enfance.

Le gouvernement français a lancé fin 2013 une campagne nationale de prévention pour agir contre le harcèlement et la cyberviolence à l'école.

3.3 Statistiques sur la cybercriminalité

3.3.1 Grandes tendances de la cybercriminalité

Les renseignements détaillés fournis par les différents services de police compétents dans la réponse française au questionnaire GENVAL convergent sur les grandes tendances empruntées par le phénomène cybercriminel. Ces constatations rejoignent la synthèse insérée dans le rapport du groupe ROBERT.

1) Le nombre de cybercriminels augmente, en raison, notamment, d'une offre technique qui évolue, se vulgarise et devient facilement accessible sans connaissances approfondies. Le marché parallèle des virus et autres programmes malveillants est florissant sur internet. L'utilisation croissante de moyens d'anonymisation des connexions entraîne une forte progression des comportements délinquants du fait du sentiment d'impunité qu'elle génère.

2) La cybercriminalité emprunte des formes de plus en plus diversifiées.

- L**es cybercriminels de droit commun** sont de loin les plus nombreux : délinquants sexuels (*pédopornographie, proxénétisme organisé),* cyberviolents *(menaces, insultes, diffamations, harcèlements via internet, dérives sectaires),* cyberescrocs: la masse des escroqueries prend des formes de plus en plus diverses *(hameçonnage, escroquerie à l'emploi, blocage avec demande de rançon, etc.)* - et les fraudes bancaires sont florissantes (*interception des données bancaires sur internet, skimming, piratage des terminaux de paiement chez les commerçants, etc.*) ainsi que les contrefaçons liées à l'extension du commerce en ligne *(contrefaçons de marques, de logiciels, de produits relevant de la propriété intellectuelle, de médicaments...,* cybertraficants *(drogues de synthèse, blanchiment du produit du crime, etc.).*

- **les cybercriminels qui concentrent leurs attaques sur les entités étatiques et les opérateurs d'importance vitale :** cybermercenaires, cyberespions (le cyberespionnage économique constitue une menace majeure) et cyberterroristes, animés par des idéologies extrémistes

3) Les cibles de la cybercriminalité n'épargnent aucune catégorie de victimes : particuliers, entreprises commerciales, services publics.

Les enfants, les personnes vulnérables et les personnes âgées sont particulièrement visés par les délinquants sexuels et les cyber-escrocs. Les petites et moyennes entreprises et les industriels sont, quant à eux, les cibles privilégiées des cyberattaques contre les systèmes de traitement automatisé de données. Selon une étude récente réalisée par une société éditrice de logiciels anti-virus, plus d'un tiers des entreprises françaises de moins de 250 salariés auraient été victimes de telles attaques en 2013, en augmentation de 42% par rapport à l'année antérieure. La cible des PME et des sous-traitants permet aussi d'atteindre indirectement les grands groupes industriels et commerciaux. L'Etat et les entreprises sensibles au titre de la souveraineté nationale ne sont pas épargnés ; la France a recensé ces quatre dernières années, sans toujours les rendre publiques, une centaine d'attaques informatique de grande envergure, par exemple contre des institutions politiques, des ministères, des services répressifs, des opérateurs d'importance vitale, etc.

4) Les modes opératoires se diversifient et se complexifient.

L'une des tendances majeures actuellement observées en France consiste dans l'utilisation croissante de logiciels malveillants. Ces logiciels de piratage informatique, principalement en vente sur des sites hébergés aux Etats-Unis, permettent à un utilisateur même novice de prendre à distance le contrôle d'autres ordinateurs dans un but illicite ou malveillant (attaques en déni de service, prises de contrôle à distance de l'ordinateur ciblé par l'attaque, captation frauduleuse de données personnelles et surtout bancaires).

5) Concernant les abus sexuels contre les enfants et la pédopornographie la police française constate : la persistance des échanges "peer-to-peer" classiques ou par le biais de logiciels spécialisés tel Gigatribe qui permet des échanges privés et chiffrés ; une utilisation de plus en plus fréquente de l'internet caché (Darknet) ; le développement du phénomène de live streaming (visionnage en direct, rémunéré, d'agressions sexuelles à l'égard de mineurs).

Les autorités françaises dans leur réponse au questionnaire et les praticiens rencontrés au cours de la visite sur place ont également insisté sur **l'augmentation sensible de la part de l'analyse informatique dans l'enquête.**

La capacité de stockage se développe rapidement et augmente la quantité de données à exploiter. Les analyses s'avèrent en outre plus délicates à réaliser, du fait du niveau croissant de connaissances des délinquants et du développement d'outils d'effacement, de dissimulation ou de chiffrement mis à leur disposition.

3.3.2 Nombre de cas répertoriés de cybercriminalité

La visite sur place et les éléments de réponse fournis par les autorités françaises mettent en évidence deux points importants en ce qui concerne la fiabilité des statistiques administratives en matière de cyber délinquance.

1. Actuellement le dispositif statistique français ne fournit pas une idée précise du nombre et de la nature des cyberinfractions constatées et/ou sanctionnées, ni du nombre de personnes ayant fait l'objet d'enquêtes, de poursuites et de condamnations pour des actes de cybercriminalité.

Comme de nombreux autres pays, la France se heurte à la difficulté de quantifier à un niveau de précision satisfaisant un phénomène criminel de plus en plus large et qui recouvre à la fois des infractions dont la définition légale identifie la dimension cybercriminelle et des infractions de droit commun commises au moyen des technologies de l'information.

C'est pourquoi, à partir de 2015, le service statistique du Ministère de l'Intérieur produira les chiffres de la cybercriminalité en fonction de nouveaux indicateurs actuellement en cours d'expérimentation. Les chiffres issus d'autres sources publiques ou privées seront évalués et exploitées progressivement dans le courant de l'année 2015.

Les données statistiques dont dispose le Ministère de la Justice concernent essentiellement les infractions identifiées comme cybercriminelles et qui ont débouché sur une condamnation. Les chiffres sont très limités, soit parce que les infractions signalées n'ont pas été poursuivies ou ont fait l'objet d'une relaxe, soit parce qu'elles ont donné lieu à des condamnations sous d'autres données statistiques.

Les atteintes à des systèmes d'information ayant donné lieu à une condamnation s'élevaient à un total de 114 infractions en 2008, 157 en 2009, 254 en 2010, 167 en 2011 et 185 en 2012. Les condamnations pour abus sexuels commis contre les enfants via internet et la pédopornographie représentent un total de 330 infractions en 2008, 319 en 2009, 349 en 2010, 426 en 2011 et 569 en 2012. Le groupe des infractions dont les ordinateurs et les systèmes informatiques ont constitué l'arme ou la cible atteignent le chiffre total de 596 infractions en 2008, 602 en 2009, 519 en 2010, 366 en 2011 et 504 en 2012. En termes de pourcentage par rapport à l'ensemble des infractions ayant donné lieu à condamnation sur les 5 années en question, les infractions identifiées comme relevant de la cybercriminalité représentaient 0,10% en 2008, 0,11% en 2009, 0,11% en 2010, 0,10% en 2011 et 0,13% en 2012.

En France le contentieux judiciaire relatif à la cybercriminalité, tel qu'il est décompté, apparaît à la fois insignifiant en proportion de la réalité du phénomène criminel connu dans ce pays, et bien trop stable en terme d'évolution.

2. Le "chiffre noir" de la cybercriminalité, c'est-à-dire celui des infractions, même graves, qui ne sont pas signalées aux autorités répressives est très élevé.

- Selon le rapport ROBERT, nombre de victimes ne signalent pas l'infraction aux autorités répressives, soit parce qu'elles ont une voie d'indemnisation plus facile en vertu de la loi (fraudes bancaires), soit parce qu'elles n'en voient pas l'intérêt ; ce cas est majoritaire chez les particuliers, et beaucoup d'entreprises s'abstiennent aussi de porter plainte, pour des raisons tenant essentiellement à leur image.

Quant aux professionnels de l'internet, leur obligation de dénonciation reste cantonnée à quelques infractions graves.

- L'équipe d'évaluation s'est aperçue que le transfert d'informations entre les différentes entités publiques en charge du bon fonctionnement de l'internet pouvait être amélioré, notamment en matière de signalement aux autorités répressives des infractions pénales dont ces entités auraient connaissance.

Lors de la visite sur place l'équipe d'évaluation s'est aperçue que des entités publiques ne signalaient pas systématiquement aux autorités judiciaires compétentes les infractions dont ils ont connaissance, tout en informant à chaque fois les victimes de leur droit de déposer plainte. Pourtant l'article 40 du code de procédure pénale français oblige "*toute autorité constituée, tout officier public ou fonctionnaire qui, dans l'exercice de ses fonctions, acquiert la connaissance d'un crime ou d'un délit (à) en donner avis sans délai au procureur de la République*".

Après la visite les autorités françaises ont souhaité préciser qu'en plus d'informer les victimes sur leur droit à déposer plainte et dans certains cas de les y inciter fortement, l'ANSSI coopérait directement et de manière régulière avec les services compétents du ministère de l'intérieur et s'engageait à coopérer avec le ministère de la justice dans le cadre d'investigations judiciaires dans le domaine des technologies de l'information et de la communication; que le détachement d'un officier de police judiciaire de manière permanente au sein de l'ANSSI, situation inédite au niveau européen, traduit la volonté d'harmoniser les opérations techniques de réponse à incident avec les services répressifs; que cet officier de police informe la victime de ses droits et peut dans certains cas inciter fortement la victime à déposer plainte; que l'ANSSI répond également aux questions relatives aux particularités des procédures relatives aux technologies de l'information et de la communication.

Les autorités françaises ont ajouté que l'ANSSI n'œuvre que sur une portion très restreinte des infractions liées à la cybercriminalité (atteintes aux STAD); que ses liens permanents avec les services répressifs font que ceux-ci sont informés de la quasi-totalité des engagements de l'Agence, voire y sont associés lors d'une saisine judiciaire; qu'en outre, l'ANSSI n'ayant pas de liens organiques avec les magistrats, praticiens de la Cybercriminalité, le fait de porter des éléments relatifs à des infractions à leur connaissance est laissé à l'appréciation des services spécialisés, interlocuteurs réguliers et légitimes de ces autorités judiciaires.

Les autorités françaises considèrent qu'il n'existe par conséquent aucune « dissimulation » pour ces faits ni pour leur prise en compte au niveau national.

L'équipe d'évaluation est bien consciente que la dénonciation obligatoire aux autorités répressives peut compromettre la confiance envers l'Etat dans les cas où la victime tient à rester anonyme. Mais en définitive, le défaut de signalement des infractions cybercriminelles par les organes d'Etat conduit à la privatisation du déclenchement de l'action publique. L'opportunité des poursuites ne devrait pas être laissée à l'appréciation des seuls opérateurs qui décideront des suites à donner à une menace criminelle en fonction, non pas de l'intérêt général, mais de leur intérêt commercial ou financier propre.

En outre, le signalement systématique des cyberattaques aux autorités répressives nationales permettrait, même en dehors de toute poursuite, la mutualisation de certaines informations avec leurs homologues étrangers et faciliterait l'évaluation de la menace criminelle, son impact et les contremesures à mettre en œuvre.

Malgré ces difficultés les autorités françaises s'efforcent d'exploiter au mieux les données disponibles (casier judiciaire, fichiers opérationnels de police et de gendarmerie, enquêtes de victimation etc.). Ces éléments sont mis à la disposition de l'Observatoire National de la Délinquance et des Réponses Pénales qui publie chaque année les chiffres-clés relatifs à la criminalité en France[9]. En 2013, 2 735 atteintes aux systèmes de traitement automatisé des données (STAD) ont été recensées par la police et la gendarmerie. Entre 2012 et 2013, le nombre d'atteintes aux STAD constatées augmente (+ 20 % soit + 462 faits). Un peu moins de 48.000 infractions de délinquance astucieuse commises par le biais d'internet ont également été enregistrées en 2013, contre 30.000 l'année précédente. Cette même année, 2.905 atteintes à la dignité et à la personnalité commises par internet sont constatées par la police et la gendarmerie (contre 2.300 en 2012), ainsi que 550 atteintes sexuelles commises par le biais d'internet (contre 455 en 2012).

3.4 Dotations budgétaires nationales pour la prévention de la cybercriminalité et la lutte contre celle-ci et contribution financière de l'UE

Il n'y a pas d'approche globale en ce qui concerne les budgets alloués à la lutte contre la cybercriminalité. La France a fourni les renseignements suivants :

- Au sein de la gendarmerie nationale, outre les budgets dédiés d'initiative par les unités centrales et territoriales, un budget spécifique important est consacré par la direction générale de la gendarmerie nationale à la formation et à l'équipement des enquêteurs spécialisés dans la lutte contre la cybercriminalité. A cet effet, un financement de l'Union européenne est recherché dans le cadre des fonds de sécurité intérieure et du programme Hercule III.

9 http://www.inhesj.fr/sites/default/files/ra-2014/synthese_ra-2014.pdf

- Le Groupe internet de la Brigade de Protection des Mineurs de la Préfecture de police de Paris bénéficie de dotations budgétaires spécifiques, notamment au titre des nouvelles technologies, émanant de la Préfecture de police ainsi que du plan pluri-annuel d'équipement. En 2013, outre les crédits alloués au service informatique de la Direction Régionale de la Police Judiciaire de Paris, chargé de répondre aux besoins des services, cette direction a bénéficié d'un crédit supplémentaire de 53.000 € destinés à l'achat de logiciels visant à lutter contre la cybercriminalité et du matériel informatique dédié.

- S'agissant des financements de l'UE, dans le cadre ISEC 2013, un appel à projet ciblé « cybercriminalité » a été publié par la DG HOME. Aucun projet n'a été présenté par le Ministère de l'Intérieur mais un projet proposé par une société privée française a été sélectionné aux fins de cofinancement européen. Intitulé « EU-PI, European Union anti-Phishing Initiative », il est présenté par la société LEXSI et sera réalisé en partenariat avec les sociétés SMILE (LU), l'association Signal-Spam (FR), ECSG (NL), le Ministère de l'Economie et du Commerce Extérieur (LU), EUROPOL (EC3) et l'association Phishing-Initiative (FR). Son budget est 553.222,64 € ; le cofinancement européen s'élèvera à 488.871,64 € (soit un taux de cofinancement européen de 88,37 %).

- Dans le cadre du financement FSI police-gestion partagée, le renforcement des capacités des autorités répressives françaises en prévention, détection, et répression de la cybercriminalité figure parmi les priorités du projet de programme national de la France. Sous réserve de validation par la Commission européenne, il est prévu de mettre l'accent sur les partenariats public-privé, et sur la coopération avec les pays tiers générateurs d'infractions dont sont victimes les citoyens européens.

Par ailleurs, le projet de programme national de la France prévoit de cofinancer le cycle politique de l'UE. Un cofinancement par l'enveloppe nationale du FSI POLICE pourra être sollicité pour la mise en œuvre de projets EMPACT en lien avec la lutte contre la cybercriminalité.

3.5 Conclusions

- L'Agence Nationale de Sécurité des Systèmes d'Information (ANSSI) est la pièce maîtresse du dispositif français dans le domaine de la cybersécurité et bénéficie à ce titre de moyens importants, à la hauteur des enjeux dont elle a la charge. La coopération avec les autorités répressives et en particulier judiciaires est limitée au traitement des attaques informatiques visant des opérateurs d'importance vitale. Dans les autres cas, elle n'est pas organisée, voire parfois évitée, par souci de protéger la confidentialité.

- Le Ministère de l'Intérieur a élaboré récemment sa stratégie ministérielle sur les cybermenaces qui comporte un volet "cybercriminalité" ; celle-ci inclut, entre autres, une réorganisation très utile des services de ce ministère. Dans le cadre de la mise en oeuvre de cette stratégie, un préfet chargé de la lutte contre les cybermenaces a été nommé, préfigurant la création d'une délégation chargée de la lutte contre les cybermenaces, courant 2015.

- Le Ministère de la Justice, qui est en charge de la politique pénale générale en France, n'a pas encore déployé de stratégie.

- Le rapport du groupe de travail interministériel ROBERT (mars 2014) dresse un tableau complet de la situation en matière de lutte contre la cybercriminalité et intègre de nombreux éléments prospectifs ; il contient une liste de recommandations particulièrement pertinentes et innovantes en vue de développer une stratégie nationale de lutte contre la cybercriminalité. Ce travail de réflexion entamé par la France doit être salué et les autres Etats membres doivent être encouragés à s'engager dans une démarche similaire.

- Le rapport ROBERT contient 55 recommandations. La mission d'évaluation GENVAL a permis de vérifier la validité d'un grand nombre d'entre elles. Il est souhaitable que, suite à cet excellent travail, une méthodologie soit définie afin de déterminer lesquelles de ces recommandations sont prioritaires et d'arrêter le calendrier de leur mise en œuvre.

- Le chiffre noir de la cybercriminalité en France est entre autres imputable à un déficit de signalement aux autorités judiciaires, non seulement par les victimes, mais également par des entités publiques (ANSSI, CNIL) qui ont connaissance d'infractions sérieuses par leur nature ou leur ampleur.

- En outre, ce défaut de signalement systématique des infractions compromet l'efficacité de la lutte contre la menace cybercriminelle. Excepté en ce qui concerne les victimes d'atteinte à un système automatisé de traitement de données, les personnes ou les entreprises dont les données sont compromises ne sont pas systématiquement identifiées et informées et, en conséquence, ne peuvent prendre les mesures adéquates en vue de limiter leur préjudice ; les auteurs ne sont pas poursuivis et peuvent ainsi reproduire les mêmes effets sur d'autres cibles, tant au niveau national qu'international.

- Les dispositifs actuels de comptage des infractions avec lesquels travaillent les autorités répressives françaises donnent lieu à des exploitations qualitatives très utiles, mais ne permettent pas d'appréhender quantitativement la cybercriminalité constatée, dans son ensemble et par nature d'infraction. Cet état de fait est un symptôme de la difficulté plus large que les autorités françaises rencontrent encore, comme c'est le cas dans nombre d'autres pays, pour développer une méthodologie globale de lutte contre un phénomène criminel ample et diversifié.

4 STRUCTURES NATIONALES

4.1 Système judiciaire (poursuites et juridictions)

4.1.1 Structure interne

Il n'existe pas, en France, de services de poursuite ni de tribunaux pénaux spécialisés en matière de cybercriminalité. Tous les ressorts du pays ont vocation à traiter des affaires en lien avec une forme ou une autre de cybercriminalité, sur la base des critères généraux de compétence territoriale définis par la loi, à savoir, par ordre de priorité, le lieu de commission de l'infraction, celui du domicile du suspect, celui du lieu d'arrestation ou de détention de ce dernier.

La visite sur place a révélé que les modalités d'attribution des dossiers à l'une ou l'autre juridiction ne sont pas claires et que les décisions en la matière sont semble-t-il prises au cas par cas. En conséquence et en raison de la complexité de la matière qui rebute beaucoup de praticiens insuffisamment formés, l'on assiste à de nombreux dessaisissements de la part des parquets (par exemple sur la base du critère de localisation du domicile, dès que l'auteur des faits est identifié). Ce phénomène conduit parfois à une certaine démotivation des services de police concernés. Il y aurait, selon les magistrats entendus lors de la visite en France, de nombreux dossiers en déshérence partout en France, surtout en province.

Il existe quelques aménagements aux règles de compétence sus-énoncées :
- En matière de terrorisme, le parquet de Paris dispose d'une compétence spécifique ;
- En cas de procédures initiées parallèlement par plusieurs services de poursuite, un regroupement de celles-ci pourra avoir lieu dans le ressort principal ;

- Les huit juridictions interrégionales spécialisées (JIRS) créées en 2004 sont susceptibles d'intervenir dans certaines affaires de cyberattaques ou de fraude en ligne mais leur compétence est limitée aux cas de grande complexité, résultant notamment du grand nombre d'auteurs, de complices ou de victimes ou du ressort géographique sur lequel elles s'étendent. Cette situation est assez répandue en matière de cybercriminalité et pourtant, en pratique, les JIRS ne sont que rarement saisies.

Dans les faits, les parquets les plus concernés quantitativement par la cybercriminalité sont ceux de la région parisienne et des plus grandes villes de province. La pratique observée au sein de ces juridictions montre que les affaires liées à la cybercriminalité (hors pédopornographie et presse) sont en général traitées par les sections économiques et financières des parquets saisis. En outre certains d'entre eux se sont organisés, en leur sein, pour désigner un "magistrat référent" en matière de cybercriminalité, qui apportera un soutien technique à ses collègues saisi d'une affaire dans ce domaine. Le parquet de Paris, qui vu sa localisation se trouve compétent dans la plupart des cyber-attaques revêtant une certaine importance, a créé une cellule spécialisée, à laquelle sont affectés deux procureurs et un assistant. S'il faut se féliciter de cette spécialisation qui semble unique sur le territoire français, les effectifs de cette cellule paraissent insuffisants au regard du nombre de dossiers relevant de la juridiction parisienne.

4.1.2 Capacités disponibles et obstacles à l'aboutissement des poursuites

A. Capacités.

- Les magistrats référents en cybercriminalité

Un "référent en cybercriminalité" est désigné au sein de chaque service local de poursuite de France pour être l'interlocuteur privilégié des collègues et des services d'enquête. Le référent cybercriminalité met en place un système de veille législative et jurisprudentielle et fait partager à ses collègues cette documentation.

La visite sur place a mis en évidence que le système des référents est largement perfectible : le "turn-over" y est important ; les référents ne reçoivent pas systématiquement de formation pour remplir leur mission ; leur "visibilité" auprès de leurs collègues n'est pas toujours assurée.

- Les relations des magistrats avec les services d'enquête spécialisés

Certains parquets mettent en place avec les services d'enquête spécialisés des rencontres régulières pour avoir une meilleure connaissance des spécificités de chacun et du partage des compétences entre les services. En outre, cela permet de savoir quels actes d'investigation peuvent être demandés aux commissariats locaux pour ne pas surcharger les services spécialisés.

B. Obstacles. Les autorités françaises indiquent que la principale difficulté constatée pour l'aboutissement des poursuites est celle de l'identification des auteurs de l'infraction. D'autres difficultés concrètes ont été identifiées par les services d'enquête :

- absence de plainte des victimes, par découragement ou par crainte pour la réputation professionnelle,
- moyens répressifs inadaptés pour traiter les phénomènes de masse (ex : escroquerie en ligne),
- techniques spéciales d'investigation encore trop peu employées (enquêtes sous pseudonyme),
- besoin d'une coordination accrue des enquêtes,
- lenteur des procédures judiciaires (en particulier les demandes d'entraide judiciaire internationales),

- nécessité de simplifier au niveau européen, les actes de base (ex : identification d'une adresse IP, d'une adresse mail, d'un numéro de téléphone ou de compte bancaire) ; la lenteur judiciaire empêche notamment les interceptions rapides des serveurs informatiques impliqués dans les cyber-attaques.
- absence d'obligation de réponse des opérateurs étrangers - réactivité inégale et souvent trop lente aux réquisitions, notamment de la part des opérateurs étrangers dont les moyens sont sous-dimensionnés pour répondre (Facebook, Yahoo, Amazon, Google…) (N.B. la France est l'un des 3 pays qui font le plus de demandes dans le monde),
- difficulté de remonter les connexions internet opérées par smartphones (difficultés techniques et/ou réticences des opérateurs),
- disparité des statuts juridiques des opérateurs étrangers qui répondent en fonction de leur propre règle de confidentialité ou pour les seules connexions formellement identifiées en France ou en Europe,
- absence fréquente de journalisation de certains serveurs PROXY ou VPN, ou dans de nombreux équipements de sécurité informatique (malgré la disponibilité de la fonctionnalité) procurant une totale anonymisation des criminels par absence de trace ou par :
    - durée insuffisante (ou absence) de conservation des données dans les pays partenaires y compris européens,
    - disparité au niveau international, des critères d'admissibilités de la preuve,
    - insuffisance ou absence de juridictions spécialisées,
    - déficit de sensibilisation/formation des magistrats.

Ces points ont été soulevés par le groupe de travail interministériel sur la cyber criminalité qui les ont traduit en plusieurs recommandations dans le rapport final. Le groupe de travail du Ministère de l'Intérieur sur les cyber-menaces en tient également compte dans son plan d'action.

4.2 Autorités répressives

4.2.1 Les services centraux et territoriaux spécialisés en matière de cybercriminalité

Au sein du Ministère de l'Intérieur, les services centraux et territoriaux chargés de la lutte contre la cybercriminalité sont rattachés à la Direction Générale de la Police Nationale (DGPN), à la Préfecture de police de Paris et à la Direction Générale de la Gendarmerie Nationale (DGGN). Il faut également citer, pour mémoire, la Direction Générale de la Sécurité Intérieure (DGSI) qui assure la compétence répressive concernant les enquêtes de cyberattaques ayant une dimension de sécurité nationale.

I - Services de police

LES SERVICES CENTRAUX :

►**La Sous-Direction de la lutte contre la cybercriminalité (SLDC)**

Ce service, créé en avril 2014 dans le cadre de la stratégie du Ministère de l'Intérieur, intègre les missions de prévention et de répression en matière de cybercriminalité et se veut également un lieu de définition des stratégies à mettre en œuvre dans les domaines de l'opérationnel, de la formation et de la prévention du grand public et du tissu économique. La S.D.L.C. a été conçue pour être le point de convergence des actions menées par le Ministère de l'Intérieur au plan national, pleinement identifiable par ses partenaires institutionnels, les acteurs de l'économie numérique et les particuliers. Elle héberge notamment un **Bureau de coordination stratégique** et une **Division de l'anticipation et de l'analyse, ainsi que :**

- **<u>L'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (O.C.L.C.T.I.C.)</u> qui a pour missions:**

- d'animer et coordonner la mise en œuvre opérationnelle de la lutte contre les auteurs d'infractions liées aux technologies de l'information et de la communication ; les directions régionales de police judiciaire participent étroitement au fonctionnement du dispositif national centralisé de lutte contre la cybercriminalité, en étroite coordination avec l'OCLCTIC.
- de procéder, à la demande de l'autorité judiciaire, à tous actes d'enquêtes et travaux techniques d'investigations ;
- d'apporter, à leur demande, une assistance aux services de police, de gendarmerie et de douane en cas d'infractions liées aux hautes technologies ;
- d'intervenir d'initiative, avec l'accord de l'autorité judiciaire, pour s'informer sur place des faits relatifs aux investigations conduites localement ;
- de centraliser et diffuser l'information sur les infractions technologiques à l'ensemble des services répressifs.

L'OCLCTIC est le rôle de point de contact opérationnel 24h/24 et 7j/7 au sens de la Convention de Budapest. Le point de contact peut être saisi par téléphone ou sur une adresse mail dédiée. La demande doit être rédigée en anglais et correspondre au formalisme requis (précisions sur le cas d'enquête, les horodatages, etc..). Une fois la conformité de la demande vérifiée, elle est adressée par ou à l'hébergeur/ fournisseur français si elle provient d'un pays étranger, ou au point de contact étranger si elle émane d'un service de police français.

Le point de contact est à même de faire procéder à la préservation des données et d'apporter un premier conseil technique ou judiciaire au service qui en ferait la demande.

En ce qui concerne les attaques contre les systèmes d'information de l'Etat ou des opérateurs d'importance vitale, il existe un point de contact opérationnel 24/7 à l'ANSSI, dans son Centre Opérationnel de Sécurité des Systèmes d'Information (COSSI).

L'OCLCTIC est en charge de la formation des investigateurs en cybercriminalité (ICC) ouverte à l'ensemble des directions de la police nationale (DCPJ, DCSP, IGPN, DCPAF, Préfecture de Police de Paris) et de la DGSI. 377 investigateurs en cybercriminalité répartis sur l'ensemble du territoire ont été formés par l'OCLCTIC.

►**L'Office central pour la répression des violences aux personnes (OCRVP) :**

L'OCRVP dépend de la sous-direction de la lutte contre la criminalité organisée et la délinquance financière du Ministère de l'Intérieur. Cet office a pour compétence toutes les cyberinfractions ayant trait à la pédopornographie et pour missions d'animer, de coordonner et de centraliser les investigations de police judiciaire dans ce domaine en lien avec le centre national d'analyse des images de pédopornographie (CNAIP). Il est aussi chargé de fournir une assistance documentaire et analytique aux services territoriaux de la police ou de la gendarmerie nationales. L'une des priorités qui lui est assignée consiste à développer les techniques d'enquête sous pseudonyme en formant des "cyberpatrouilleurs" sur tout le territoire.

LES SERVICES TERRITORIAUX DE POLICE JUDICIAIRE SPÉCIALISÉS :

Les directions inter-régionales de la police judiciaire (DIPJ) et les directions régionales de la police judiciaire (DRPJ). Au niveau régional, la police judiciaire comprend :

- Neuf directions inter-régionales de police judiciaire (DIPJ de Bordeaux, Dijon, Lille, Lyon, Marseille, Orléans, Rennes, Strasbourg et Pointe-à-Pitre) composées d'un ou de plusieurs services régionaux de police judiciaire (SRPJ) et d'une ou de plusieurs antennes de police judiciaire ;
- Trois directions régionales de la police judiciaire (Paris, Versailles et Ajaccio).
- Leur ressort territorial de compétence couvre, selon les cas, de 2 à 8 départements. Les DIPJ et DRPJ participent étroitement au dispositif national centralisé mis en place pour la lutte contre le crime organisé ou la délinquance spécialisée.

Au sein de ces services territoriaux la Direction Régionale de la Police Judiciaire de Paris, rattachée à la Préfecture de police de Paris, dispose de services spécialisés à compétence régionale (Paris et les départements limitrophes). Ces services dont au nombre de 7, dont 3 sont compétents en matière de cybercriminalité :

- **La Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information**

Premier service créé en matière de lutte contre la cybercriminalité (1994), la "BEFTI" traite les affaires les plus complexes, les dossiers simples étant traités par les services de police locaux. En cela et vu l'ampleur de ses activités sur le territoire le plus dynamique de France, elle peut être considérée comme un service central.

La BEFTI est compétente pour les infractions concernant les atteintes aux systèmes d'informations et aux données personnelles qu'ils recèlent, aux contrefaçons de logiciels et bases de données, aux atteintes par les fournisseurs et prestataires de communication électroniques. Elle assiste en criminalistique, analyse légale des supports numériques et en investigations numériques tous les services de son ressort. Elle assure en ce domaine des actions de formation à destination d'autres policiers et des actions de sensibilisation du public, des entreprises ou des administrations. Cette brigade très active participe à de nombreux séminaires, conférences et associations pour partager les connaissances et améliorer les pratiques.

- **La Brigade des Fraudes aux Moyens de Paiement**

Les missions de la "BFMP" englobent les enquêtes liées aux infractions relatives aux moyens de paiement numériques ; elle est notamment en charge des fraudes à la carte bancaire , du E-commerce avec usages frauduleux de références de cartes bancaires, des fraudes aux crédits : Vols d'identités, Faux documents, Crédits frauduleux, Ouvertures frauduleuses de comptes bancaires.

- **Brigade de Protection des Mineurs:**

Cette brigade a une compétence exclusive en matière de mineurs victimes sur le territoire du "grand Paris". Le Groupe Internet de la BPM a pour mission de traiter les affaires pour lesquelles apparaît une composante "cyber". Ce groupe est organisé en deux pôles :

- Le Pôle "Investigation Innovation Recherche Assistance Technologique" *(PIIRAT),* qui a la charge des enquêtes sur la détention et la diffusion d'images pédopornographiques, la corruption de mineurs via internet et l'utilisation d'internet pour la commission de violences sexuelles, ainsi que l'assistance technique aux autres groupes, aux fins d'exploitation de supports divers pouvant contenir des images à caractère pédopornographique. Il recherche des solutions innovantes permettant d'assurer une exploitation rapide et la plus complète possible des supports de données, dans le temps de la garde à vue, en parallèle des auditions.

- Le Pôle "Cyberinfiltration et Initiative Internet" qui regroupe les enquêteurs spécialement habilités à l'enquête sous pseudonyme afin de lutter contre les atteintes sexuelles contre les mineurs commises via un réseau de télécommunication électronique. Œuvrant d'initiative, les cyber-enquêteurs créent et alimentent des profils de prédateurs et de potentielles victimes, afin de rentrer en contact avec des pédophiles.

II - Services de Gendarmerie

La Gendarmerie française est une force de sécurité à statut militaire rattachée au Ministère de l'Intérieur. Elle est structurée suivant un modèle intégré, c'est-à-dire que ses différentes missions, dont celle de police judiciaire, sont assurées à tous les échelons territoriaux de la France y compris en matière de lutte contre la cybercriminalité. Dans ce domaine le pilotage de ses actions est assuré par le centre de lutte contre les criminalités numériques (C3N)10, en coordination avec les autres services du Ministère de l'Intérieur.

►Le centre de lutte contre les criminalités numériques (C3N) :

- assure la coordination et le pilotage des actions de la Gendarmerie en matière de lutte contre la cybercriminalité qui associe investigations et criminalistique ;
- constitue le point de contact « Gendarmerie » avec tous les offices centraux de police judiciaire.
- articule son action autour de trois blocs d'activités :

10 Depuis la venue de la mission d'évaluation, le centre de lutte contre les criminalités numériques (C3N) de la gendarmerie a pris la suite du plateau d'investigation cybercriminalité et analyses numériques (PICyAN) et de la division de lutte contre la cybercriminalité.

A. Un bloc investigations : Le C3N assure :

- la surveillance des différents espaces de l'internet en vue de détecter et caractériser les infractions . Cette surveillance peut prendre la forme d'enquêtes sous pseudonyme. Le C3N assure aussi la coordination des enquêtes sous pseudonyme des unités territoriales de la Gendarmerie.
- la direction d'enquêtes ou l'appui aux offices centraux de la gendarmerie et aux unités territoriales en ayant la direction, ainsi que la direction d'opérations présentant une particulière envergure, gravité ou sensibilité.
- l'administration de CALIOPE, la base nationale des contenus pédopornographiques issus des enquêtes pénales, en lien avec INTERPOL et les homologues étrangers du CNAIP.

B. Un bloc criminalistique : Le C3N réalise à la demande des magistrats et des enquêteurs les expertises et les examens techniques complexes relatifs à la preuve numérique :

- l'extraction de données à partir de supports électroniques, magnétiques ou optiques,
- l'analyse de systèmes et de réseaux.

C. Un bloc d'appui et d'animation du réseau territorial de la gendarmerie: Le C3N englobe également :

- un guichet unique téléphonie et Internet (GUTI) assurant l'interface entre les opérateurs et les enquêteurs de la gendarmerie et le lien avec la plateforme nationale des interceptions judiciaires : il a traité en 2013 plus de 7.300 dossiers,
- une mission de soutien de la communauté des enquêteurs spécialisés des unités en termes de formation, d'équipement et d'information,
- une mission de recherche et développement.

Au niveau régional, les sections de recherches et de sections d'appui judiciaire disposent de 260 d'enquêteurs spécialisés formés aux technologies numériques (criminalistique et investigation) à un niveau licence professionnelle (NTECH) et/ou à l'enquête sous pseudonyme. En outre, des groupes interrégionaux de lutte contre la cybercriminalité viennent d'être créés dans les sections de recherches placées auprès des juridictions interrégionales spécialisées (JIRS).Ces groupes assurent une surveillance ciblée de l'internet, dirigent leurs propres enquêtes ou appuient celles des autres groupes de leur unité pour les infractions relevant de la compétence des JIRS.

Au niveau départemental, les brigades de renseignements et d'investigations judiciaires comprennent plus de 200 enquêteurs NTECH (environ 260 NTECH au total, toutes unités confondues) qui assurent un appui essentiellement criminalistique aux enquêteurs des leurs unités de leur ressort.

Au niveau local, près de 1700 correspondants en technologies numériques (C-NTECH), déchargent les NTECH d'actes simples de criminalistique ou d'investigation. Ces correspondants appuient les unités élémentaires, pour lesquelles a été mise en ligne une formation relative aux technologies numériques (P-NTECH).

4.3 Autres services

Bien qu'ils ne figuraient pas au programme de la visite sur place, les services de la Direction Générale des Douanes et des Droits indirects et ceux de la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes ont été mentionnées à plusieurs reprises comme parties prenantes du dispositif français de lutte contre la cybercriminalité. Cette action a notamment été soulignée dans le cadre de la présentation du fonctionnement de la plateforme PHAROS et à travers l'action de l**a cellule "Cyberdouane"**, qui a pour mission de recueillir et exploiter les renseignements visant la lutte contre les fraudes sur internet en matière de trafics de marchandises prohibées, réglementées ou fortement taxées. Cette veille débouche ponctuellement sur des enquêtes judiciaires mené par le Service National des Douanes Judiciaires.

4.4 Partenariat public-privé

En France les exemples de partenariat public-privé pour la prévention et la lutte contre la cybercriminalité sont nombreux :

- les liens évoqués ci-dessus de l'OCLCTIC avec une centaine de partenaires ;
- l'observatoire de la sécurité des cartes de paiement (OSCP), évoqué en 6.2 ;
- l'association Signal Spam, créée en 2003 ;
- l'association Phishing Initiative, créée en 2011 et regroupant Microsoft, Paypal et le CERT-LEXSI, pour prévenir le hameçonnage d'informations bancaires personnelles ;

• le partenariat avec certains professionnels non principalement liés au numérique, comme celui de la gendarmerie avec l'assureur AXA pour le "Permis internet" évoqué en 5.A.5, que la police nationale va étendre à son champ de compétence.

• le partenariat avec les associations de protection de l'enfance, comme celui de l'éducation nationale avec e-Enfance contre le cyber-harcèlement en milieu scolaire, ou celui de la gendarmerie avec Innocence en danger pour la fourniture d'un outil de détection de contenus pédopornographiques sur les réseaux pair-à-pair ;

• la participation au programme européen Safer Internet financé par la commission européenne au travers du programme Safer Internet France pour des actions de sensibilisation et d'accompagnement des jeunes.

• le partenariat avec les universités (ex : partenariat de la gendarmerie avec l'université de technologie de Troyes pour la formation de ses enquêteurs en technologies numériques) ou les autres établissements d'enseignement et de recherche (ex : la police avec l'école d'ingénieurs en informatique EPITA pour certains projets) ;

• le forum des droits de l'internet, initiative de 2004 en matière juridique, ainsi que toutes les autres associations de professionnels publics et privés autour des technologies numériques.

• une convention qui facilitera la promotion et la diffusion de la culture de la sécurité économique auprès des chambres de commerce et d'industrie, des entreprises, des filières et des pôles de compétitivité dans les territoires sera prochainement signée avec le Ministère de l'intérieur.

• La mise en place au sein la Préfecture de police de Paris de conventions pour recourir à des stagiaires d'école informatique de renom en vue d'échanges de connaissances et des partenariats pérennes avec la Chambre régionale de commerce et de l'industrie d'Ile de France pour diffuser l'information vers les TPE-PME.

Enfin, **un centre expert contre la cybercriminalité français (CECyF) a été créé**. Cette structure est une des réalisations du projet européen 2CENTRE financé par la Commission européenne, qui vise à créer en Europe des centres d'excellence dans le domaine de la lutte contre la cybercriminalité, réunissant institutionnels, académiques et industriels. Le CECyF a pour objectif de fédérer les initiatives de manière visible et de lancer, supporter, conduire ou faire financer des projets collaboratifs dans ce domaine en matière de formation, d'animation, de veille, de recherche et de développement. Il compte de nombreux membres, parmi lesquels les fondateurs sont la gendarmerie, la douane, le fisc, l'université de technologie de Troyes, l'université de Montpellier I, l'EPITA, Thalès Communication & Security, Orange France, Microsoft France, CEIS (co-organisateur du FIC avec la gendarmerie), l'association francophone des spécialistes de l'investigation numérique (AFSIN), l'alliance internationale de lutte contre les botnets (AILB ; organisatrice de la BotConf).

4.5 Coopération et coordination au niveau national

- Pour la partie « Infractions portant atteinte à des systèmes d'information, liées en particulier à des cyberattaques » de la définition proposée par le questionnaire GENVAL pour la cybercriminalité, la coordination des actions préventives et réactives est effectuée par l'ANSSI, autorité nationale de sécurité et de défense des systèmes d'information évoquée plus haut. Cette agence a la responsabilité de conduire ou de coordonner l'ensemble des actions destinées à prévenir la réussite des attaques contre les systèmes d'information, et à réagir en cas d'atteinte à leur confidentialité, à leur disponibilité ou à leur intégrité. Son action s'exerce principalement au profit de l'État et des opérateurs d'importance vitale du secteur privé.

- Contrairement à la cyberdéfense, la lutte contre la cybercriminalité est sectorisée : elle est menée indépendamment par chacun des ministères concernés – principalement le Ministère de l'Intérieur, le Ministère de la Justice, les administrations spécialisées telles que la Douane. Au sein même du Ministère de l'Intérieur services de police et de gendarmerie sont, pour l'essentiel de leur travail opérationnel, coordonnés par des entités différentes.

Il existe au sein du Ministère des Affaires étrangères et du développement international une Ambassadrice chargée de la lutte contre la criminalité organisée qui coordonne les travaux de ce Ministère dans le domaine de la cybercriminalité, en lien avec l'Ambassadrice désignée en tant que « coordinatrice pour le cybersécurité ».

Enfin, plusieurs instances de coordination ou de régulation existent en matière économique et financière :

- l'Autorité de Régulation des Jeux en Ligne (ARJEL), créée par la loi n°2010-476 du 12 mai 2010 ;
- la Haute Autorité pour la protection des œuvres et la protection des droits sur internet (HADOPI);
- le Groupement Carte Bancaire (GCB), créé en 1984 ;
- l'Observatoire de la sécurité des cartes de paiement (OSCP), créé par la loi n°2001-1062 du 15 novembre 2001.

4.5.1 Obligations légales ou de principe

- En matière de cyberdéfense le rôle et les moyens d'action de l'ANSSI ont été renforcés en 2013; elle peut désormais imposer des règles de sécurité informatiques définies de manière collaborative avec les opérateurs d'importance vitale qui sont tenus de mettre en œuvre sur leurs systèmes d'information critiques. Ces opérateurs sont désormais tenus de déclarer certains incidents intervenant sur ces systèmes d'information. Le Premier ministre peut diligenter des contrôles de sécurité sur ces systèmes. L'organisation de crise est testée régulièrement au travers des exercices Piranet. Ce plan gouvernemental fait actuellement l'objet d'une actualisation qui sera achevée fin 2015. L'exercice Piranet 2015 qui aura lieu fin 2015 aura vocation à tester les capacités de remontée d'informations vers l'ANSSI.

- La responsabilité et les prérogatives des fournisseurs d'accès à internet et des hébergeurs à l'égard des contenus illicites qu'ils diffusent ou qu'ils hébergent sont régies par la loi 2004-575 du 21 juin 2004 "sur la confiance dans l'économie numérique" qui transpose la directive E-Commerce. Celle-ci impose aux hébergeurs, de supprimer rapidement les contenus manifestement illicites dont ils ont connaissance sous peine de voir leur responsabilité civile et pénale engagées.

Sur justification d'un préjudice, la loi prévoit aussi la possibilité de demander la suppression des contenus illicites à l'autorité judiciaire, selon une procédure d'urgence afin de prévenir un dommage ou de faire cesser un dommage occasionné par ces contenus.

Cette loi impose aux fournisseurs d'accès à internet et aux hébergeurs de concourir à la lutte contre la diffusion des contenus les plus choquants (pédopornographie, racisme, images attentatoires à la dignité humaine, etc.) ; ils doivent aussi mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données. **C'est dans ce cadre que l'OCLCTIC signe avec des hébergeurs et éditeurs de contenus des conventions relatives au signalement de contenus illicites à la plate-forme PHAROS.**

Les hébergeurs ou fournisseurs d'accès doivent préserver les données de nature à permettre l'identification et répondre également aux requêtes dès lors qu'une demande a été adressée via le canal 24h/24 et 7j/7.

Le secteur privé est tenu d'appliquer les décisions de l'autorité judiciaire ou de répondre à ses réquisitions comme à celles des autorités répressives.

- S'agissant de la conservation des données de trafic, les fournisseurs d'accès et les hébergeurs ont une obligation de les conserver pendant un an.

En ce qui concerne la prévention et la réponse aux attaques informatiques, les opérateurs d'importance vitale du secteur privé sont tenus :
- de mettre en place à leurs frais les mesures techniques prévues par l'ANSSI ;
- de déclarer certains incidents intervenant sur leurs systèmes d'information critiques ;
- de se soumettre à des contrôles de sécurité de leurs systèmes d'information critiques ;
- en cas de crise majeure, de mettre en œuvre les mesures techniques identifiées par l'ANSSI .

4.5.2 Ressources affectées à l'amélioration de la coopération

L'Observatoire de la sécurité des cartes de paiement (OSCP)

L'Observatoire a été créé par la loi n°2001-1062 du 15 novembre 2001. Composé d'élus, du Gouverneur de la Banque de France, de représentants des Ministères, d'émetteurs de cartes de paiement, du Conseil national de la consommation, d'entreprises de commerce, il comprend notamment un représentant du ministre de la Justice, un représentant du ministre de l'Intérieur et un représentant du ministre de la défense.

L'OSCP a essentiellement pour mission de favoriser la concertation en matière de sécurité des cartes de paiement, de sensibiliser les émetteurs et commerçants, d'assurer une veille technologique en matière de cartes de paiement et de suivre l'évolution des fraudes. Cette évolution est mesurée annuellement à partir des données fournies par les établissements financiers.

Le modèle de l'OSCP a été porté au niveau européen avec la création du « Forum SecuRe Pay », dont la vocation est toutefois plus large car il a compétence sur l'ensemble des moyens de paiement.

Le groupe de travail interministériel sur la cybercriminalité a recommandé d'étendre le champ de compétences de l'OSCP à l'ensemble des instruments de paiement autres que le chèque afin de couvrir, en plus des cartes de paiement (art. L133-4 du code monétaire et financier) :

- la banque en ligne (ciblée massivement par la criminalité numérique au travers de virus informatiques spécialisés) ;
- les virements SEPA (notamment lorsqu'ils sont créées par voie électronique) ;
- les monnaies et comptes de paiement électroniques ;
- voire l'unité de compte numérique que constitue le *bitcoin* (principalement utilisée pour des transactions légales ou illégales sur internet et au sujet de laquelle les autorités monétaires ont récemment émis une mise en garde, compte-tenu du caractère hautement spéculatif de cette unité de compte et des piratages dont font souvent l'objet les portefeuilles numériques).

Les enquêteurs spécialisés de la gendarmerie et de la police disposent de la formation et de l'équipement leur permettant de faire face aux contraintes technologiques de la lutte contre la fraude aux cartes de paiement.

Enfin en ce qui concerne le **renforcement et l'amélioration de la coopération avec le secteur privé:**

- L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) entretient un partenariat avec une centaine d'associations, d'hébergeurs et de fournisseurs de services communautaires.

Cet office s'apprête en outre à mettre en place un **Bureau de l'internet** qui doit devenir une interface entre les fournisseurs de service internet (hébergeurs, FAI, réseaux sociaux, etc.) et les services d'enquête. Cette unité recensera les coordonnées des fournisseurs de service pour les mettre à disposition des enquêteurs des services locaux. Elle jouera un rôle de médiation en cas de difficulté pratique ou juridique pour obtenir des données d'enquête.

- Côté Gendarmerie, les experts en cybercriminalité ont investi dans plusieurs partenariats fructueux mentionnés en 9.5. En outre, son guichet unique téléphonie et internet (GUTI), placé auprès du centre de lutte contre les cybercriminalités numériques (C3N) du service central du renseignement criminel (SCRC) a pour rôle de faciliter les échanges entre les enquêteurs de la gendarmerie et les opérateurs de téléphonie et autres fournisseurs d'accès à internet.

- Ce rôle d'interfaçage est également dévolu au département opérationnel (gendarmes et policiers) de la plate-forme nationale des interceptions judiciaires (PNIJ), actuellement en phase finale de développement auprès de la délégation aux interceptions judiciaires (DIJ) du Ministère de la Justice.

- La Préfecture de police de Paris réalise des interventions au profit du secteur privé, de la société civile et lors de grands événements (foire de Paris, salon des séniors...) et au profit du secteur public aux côtés des fonctionnaires de sécurité des systèmes d'informations des ministères. Elle participe également aux clubs d'experts de la sécurité numérique des entreprises, aux rencontres avec les CERTS, avec les éditeurs de logiciels de sécurité qui ont une vision sur les cyber menaces. Elle entretient des relations avec les avocats des sociétés qui demandent des conseils. Cela permet de créer et de renforcer des liens développant des réflexes de coopération et des échanges. Toutefois peu de ressources peuvent y être consacrées malgré une réelle demande du secteur privé.

- Au sein de la DGSI, des conférenciers internes ont pour mission d'organiser des colloques de sensibilisation des entreprises sur l'ensemble du territoire national aux menaces relatives aux cyberattaques. Ces colloques permettent également d'échanger les bonnes pratiques en matière de cybersécurité avec les entreprises et de contribuer au renforcement de la politique de cyberdéfense nationale.

- Un réseau de la Réserve Citoyenne de Cyberdéfense (RCC) regroupant les réservistes citoyens issus des trois armées et de la Gendarmerie nationale a été mis en place en juillet 2012. Il vise à sensibiliser, organiser et susciter des événements autour du renforcement de la politique de cyberdéfense en assurant la continuité entre la société civile et le domaine de la sécurité et de la défense. La RCC comprend notamment un groupe « PME/PMI » afin de sensibiliser ces dernières aux questions de cybersécurité et cyberdéfense.

- Enfin le Ministère de l'Intérieur s'apprête à signer une convention qui facilitera la promotion et la diffusion de la culture de la sécurité économique auprès des chambres de commerce et d'industrie, des entreprises, des filières et des pôles de compétitivité dans les territoires.

4.6 Conclusions

- D'un point de vue institutionnel, la situation française se caractérise par la multiplicité des entités détenant des compétences touchant à la cybercriminalité, relevant de différents ministères ou organismes ; les relations entre ces instances s'inscrivent dans le cadre des échanges administratifs, sans véritable coordination. L'une des principales conclusions du rapport souligne la nécessite de tenir compte du caractère transversal du phénomène cybercriminel et préconise la mise en place d'une structure nationale de coordination de l'action de tous les acteurs concernés, recommandation que l'équipe d'évaluation reprendra à son compte.

- Après la visite d'évaluation les autorités françaises ont informé l'équipe d'évaluation de la nomination, le 4 décembre 2014, d'un préfet chargé de la lutte contre les cybermenaces. Il a pour mission de coordonner et de fédérer les initiatives au sein du ministère chargé de la sécurité intérieure et de représenter le ministère dans les travaux interministériels.

- Le Ministère de la justice et les tribunaux appliquent en matière de cybercriminalité une approche morcelée qui rend difficile la prise de mesure réelle de la cybercriminalité et une lutte efficace contre celle-ci ; conscient de cette situation, qui est longuement développée dans le rapport du groupe de travail ROBERT, le ministère de la justice vient de créer un service horizontal en charge de la cybercriminalité au sein de la Direction des Affaires criminelles et des Grâces. L'organisation et les méthodes de travail des juridictions françaises sont insuffisamment adaptées aux enjeux soulevés par la cybercriminalité. Le groupe ROBERT a notamment recommandé la création de pôles judiciaires spécialisés en matière de lutte contre la cybercriminalité en bande organisée et une compétence nationale particulière de la juridiction de Paris pour les atteintes aux systèmes de traitement automatisé de données visant les services de l'État et les opérateurs d'importance vitale.

- La France dispose de plusieurs services d'enquête spécialisés, à très haute compétence technique, qui travaillent chacun de manière efficace et créative. Leur formation et leur dotation en moyens humains, matériels et logiciels spécifiques doivent faire l'objet d'un effort constant afin de suivre l'évolution des technologies et des pratiques criminelles.

- La dynamique du dialogue public/privé est bien engagée ; de nombreuses initiatives, variées et intéressantes, existent en matière de partenariats entre les deux secteurs. Cet aspect déterminant de la lutte contre la cybercriminalité devrait être entretenu en permanence, être renforcé chaque fois que nécessaire et faire l'objet d'une coordination attentive.

- L'Observatoire de la Sécurité des Cartes de Paiement, création française qui a inspiré celle du Forum européen "SecuRe Pay", est un outil intéressant de concertation et de veille ; l'élargissement de son champ d'action à tous les moyens de paiement électronique est souhaité par les praticiens.

5 ASPECTS JURIDIQUES

5.1Droit pénal matériel en matière de cybercriminalité

5.1.1 Convention du Conseil de l'Europe sur la cybercriminalité

La Convention du Conseil de l'Europe sur la cybercriminalité a été signée par la France le 23 novembre 2001 et ratifiée par la loi n° 2005-493 du 19 mai 2005 autorisant à la fois l'approbation de cette Convention et de son Protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques.

Les autorités françaises ont souhaité souligner qu'en ce qui concerne plus spécifiquement la lutte contre le terrorisme, la lutte contre l'usage d'Internet à des fins terroristes s'inscrit dans le cadre de la lutte contre la cybercriminalité dont les instruments de coopération internationale sont principalement liés à la Convention de Budapest sur la cybercriminalité de 2001. Le plus important de ces instruments est le réseau international d'urgence 24/7, qui permet le gel des données numériques, facilitant ainsi la conservation des preuves numériques. Un réseau similaire mis en place à l'initiative du G8 en 1997 (G8 24/7 High Tech Crime Network) existe également. La coopération avec les hébergeurs (hébergeurs et plateformes numériques) étrangers s'opère principalement hors du cadre juridique international. Trois obstacles demeurent aujourd'hui à la mise en place d'une coopération véritablement efficace : la complexité des modalités d'entraide judicaire, la diversité des législations liées à la rétention des données et le caractère informel de la coopération avec les hébergeurs.

5.1.2 Description de la législation nationale

A l'examen de la réponse détaillée de la France au questionnaire GENVAL, l'équipe d'évaluation s'est facilement convaincue que **la législation française et plus spécifiquement son droit pénal matériel applicable à la cybercriminalité est particulièrement complète et efficace**.

De nombreuses incriminations pénales existent et paraissent couvrir largement le champ des situations délictuelles actuellement envisageables. La France s'efforce d'adapter constamment son droit pénal à l'évolution de la cybercriminalité. Ce domaine fait donc, depuis plusieurs années, l'objet d'actualisations régulières.

Au moment de la visite sur place le Parlement français était saisi d'au moins deux projets de loi qui complètent la législation dans cette matière. L'un de ces deux projets de loi a été adopté le 13 novembre 2014. Il s'agit de la loi N°2014-1353 renforçant les dispositions relatives à la lutte contre le terrorisme. Cette loi a transféré les délits de provocation et d'apologie du terrorisme commis par des moyens publics de la loi du 29 juillet 1881 sur la liberté de la presse dans le code pénal en créant l'article 421-2-5. Cette loi a également prévu l'aggravation des peines lorsque ces délits sont commis sur Internet et la possibilité pour le juge des référés d'ordonner l'arrêt d'un service de communication en ligne pour les faits prévus à l'article 421-2-5 du code pénal lorsqu'ils constituent un trouble manifestement illicite. (nouvel article 706-23 du CPP). Cette loi a également modifié la loi n°2004- 575 du 21 juin 2004 pour la confiance dans l'économie numérique en mettant en place un dispositif administratif de blocage et de déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie ainsi que des sites diffusant des images et représentations de mineurs à caractère pornographique. Les autorités administratives disposent désormais de trois possibilités : le retrait, le blocage et le déréférencement.

Enfin, pour s'adapter aux nouvelles techniques de stockage des données, les enquêteurs peuvent désormais perquisitionner à distance les "clouds".

Lorsque les incriminations de droit commun (ex. escroquerie, abus de confiance) ont un libellé suffisamment souples elles sont applicables en l'état ; dans d'autres cas le législateur a estimé judicieux de créer une circonstance aggravante liée à l'utilisation des nouvelles technologies, ou encore de créer des infractions spécifiques.

La complicité, la tentative lorsqu'elle est prévue par la loi et la récidive[11] sont toujours punissables. De même, le principe de la responsabilité des personnes morales a été généralisé en droit français, et ne nécessite pas de dispositions spécifiques.

A/ Décision-cadre 2005/222/JAI du Conseil et Directive 2013/40/UE relatives aux attaques contre les systèmes d'information

En matière de cyberattaques le droit pénal national est fort bien conçu.

Tout accès ou maintien frauduleux dans un système de traitement de données, toute atteinte intentionnelle à l'intégrité ou au fonctionnement d'un tel système, ou à l'intégrité des données qu'il contient est rendu punissable. Des circonstances aggravantes ou des infractions autonomes sont prévues pour punir plus sévèrement les cas où les conséquences de l'attaque sont les plus sérieuses, ou selon la cible qui était visée (système étatique), ou encore lorsque délit est commis en bande organisée.

Est également réprimé le fait, sans motif légitime d'importer, de posséder ou de mettre à disposition d'autrui gratuitement ou non un programme informatique spécialement adapté pour commettre les infractions ci-dessus.

Enfin, les interceptions illégales de données informatiques sont réprimées par plusieurs incriminations, ainsi que les atteintes au secret des correspondances électroniques.

Les peines maximales encourues s'étendent de un à dix ans d'emprisonnement selon la gravité des faits, en plus d'amendes conséquentes et de peines complémentaires.

B/ Directive 2011/93/UE du Parlement Européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil

La France a transposé, sans rencontrer de difficultés particulières lors de leur mise en œuvre, tant la décision-cadre 2004/68/JAI que la directive 2011/93/UE qui l'a remplacée.

11 La récidive n'est pas prévue pour les contraventions des quatre premières classes.

Au-delà de ces transpositions, la protection pénale des mineurs contre toutes les formes de pédophilie et de proxénétisme paraît faire l'objet d'un soin particulier. La législation pénale française dans ce domaine constitue un maillage serré qui prend bien en compte la diversité des pratiques criminelles dans un contexte d"usage banalisé de l'internet et des réseaux de télécommunication par les mineurs.

Le seul fait pour un majeur de faire une proposition sexuelle à un mineur de 15 ans à une personne se présentant comme telle en utilisant un moyen de communication électronique est puni de 2 ans d'emprisonnement et 30.000 euros d'amende. Les peines encourues sont aggravées lorsque la proposition a été suivie d'une rencontre (5 ans/75 000 euros) lorsqu'il y a eu abus sexuel et que le mineur a été mis en contact avec l'auteur des faits grâce à l'utilisation pour la diffusion de messages à destination d'un public non déterminé d'un réseau de communication électronique (10 ans/ 150.000 euros), ou lorsque pour la diffusion d'images ou de la représentation d'un mineur à caractère pornographique à destination d'un public non déterminé il a été utilisé un réseau de communications électroniques (7 ans /100.000 euros). Elles peuvent aller jusqu'à 10 ans d'emprisonnement et 500.000 euros d'amende lorsque les faits ont été commis en bande organisée.

Cette législation pénale ne protège pas seulement les enfants en tant que personnes, mais également leur représentation sous une forme quelconque. Seule la littérature est susceptible d'y échapper, ce que les enquêteurs rencontrés durant la visite sur site ont indiqué avoir parfois regretté, dans certaines affaires où cette pratique pouvait constituer un indice de passage à l'acte.

C/ Fraude en ligne aux cartes de paiement

Escroquerie en ligne. En droit français l'incrimination de droit commun "Escroquerie" est celle qui permet de réprimer les fraudes réalisées par la récupération des données personnelles , dont le numéro de carte bancaire, par le biais des techniques d'hameçonnage (*phishing*). L'utilisation frauduleuse du numéro de carte bancaire d'autrui pour acheter sur internet, ainsi que l'accès frauduleux à un compte bancaire par internet constituent aussi le délit d'escroquerie. L'escroquerie est punie de 5 ans d'emprisonnement et la peine peut aller jusqu'à 10 ans si le délit est commis en bande organisée.

Infractions aux cartes bancaires. La falsification de moyens de paiement, dont la carte bancaire, est réprimée sévèrement (jusqu'à 10 ans d'emprisonnement et 1.000.000 € d'amende si elle est commise en bande organisée). Celui qui accepte sciemment le paiement frauduleux et celui qui fabrique, possède, ou met à disposition le moyen de commettre l'infraction sont punissables des mêmes peines.

D/ Autres phénomènes de cybercriminalité

Le droit pénal spécial français est riche d'autres incriminations en matière de cybercriminalité, en matière d'usurpation d'identité, de messages malveillants, d'infractions en matière de propriété intellectuelle (contrefaçon), de terrorisme y compris la provocation et l'apologie du terrorisme, d'utilisation d'internet comme vecteur de menaces, de diffamation et injures, de provocation et apologie du crime, de racisme et xénophobie, d'interceptions illégales, d'atteintes au secret des correspondances, etc…

En outre, le dispositif législatif français a été étoffé par la loi du 13 novembre 2014 qui prévoit notamment la possibilité, pour l'autorité administrative, de demander le blocage des sites internet provoquant ou faisant l'apologie du terrorisme ainsi que le « déréférencement » à partir d'un moteur de recherche ou annuaire. La loi a été mise en application par un décret du 5 février 2015, qui donne notamment un pouvoir de contrôle à la Commission nationale Informatiques et libertés.

5.2 Questions de procédure

5.2.1 Techniques d'investigation

Toutes les techniques d'investigation mentionnées dans le questionnaire GENVAL sont autorisées par la loi française : perquisition et saisie de systèmes d'information ou de données informatiques, interception et collecte en temps réel de données de trafic et de contenu, conservation de données informatiques, injonction de produire toutes données stockées, injonction de communiquer des données concernant l'utilisateur.

Deux autres techniques utilisées en France méritent d'être signalées.

- L'enquête sous pseudonyme. Cela consiste à interagir avec les suspects par échanges électroniques afin de recueillir des éléments de preuve d'une infraction, et ce sans aucune provocation à la commettre. Actuellement cette technique d'investigation spéciale est essentiellement utilisée par les services répressifs français en faveur de la protection des mineurs contre toute exploitation sexuelle mais, elle est également applicable contre la traite des êtres humains, le proxénétisme, les jeux d'argent et de hasard, la criminalité organisée, le terrorisme et le trafic des produits de santé. Le groupe ROBERT recommande son extension la plus large possible.

Bonne pratique suggérée par la France. Des services spécialisés dans la protection des enfants ont développé une technique d'enquête sous pseudonyme en binôme, qui permet aux enquêteurs de travailler avec une plus grande efficacité opérationnelle tout en étant mieux armés sur le plan psychologique.

- La captation de données informatiques (« cheval de Troie » légal). Cela consiste à accéder, par un dispositif spécial, aux données telles qu'elles s'affichent à l'écran telles qu'elles sont introduites au clavier ou telles qu'elles sont reçues ou émises par des périphériques audiovisuels. Elle est applicable uniquement dans le cadre de la lutte contre la criminalité organisée et les dispositifs matériels ou logiciels mis en œuvre doivent recevoir l'agrément de l'ANSSI; les critères d'admission sont sévères. Une note d'analyse remise par les autorités françaises, soutenue par les praticiens rencontrés sur place, souligne que, bien qu'il n'ait jamais été testé dans les faits, le régime d'autorisation préalable auquel la captation des données à distance est soumise apparait complexe et diffus, et laisse craindre des lenteurs administratives liées à la délivrance de l'agrément de l'ANSSI qui pourraient réduire considérablement l'intérêt de recourir à cette mesure : créée en 2011, la captation de données n'a encore jamais été utilisée.

5.2.2 Examen criminalistique et chiffrement

- Examens criminalistiques par la voie électronique ou à distance

Le code de procédure pénale français prévoit la possibilité d'examiner les données figurant sur l'ordinateur du suspect et sur les informations auxquelles il a accès, à condition de ne pas avoir préalablement déterminé que ces informations se trouvaient en dehors de notre ressort national.

En outre la mise en œuvre des dispositions de l'article 32 de la Convention de Budapest, aux termes desquelles une Partie peut, sans l'autorisation d'une autre Partie, accéder à des données informatiques stockées situées dans un autre Etat si elle obtient le consentement légal et volontaire de la personne légalement autorisée à les divulguer, suppose qu'ait été recueillie la preuve du stockage des données sur le territoire de cet Etat.

- Chiffrement

Les problèmes rencontrés liés au chiffrement sont de plusieurs ordres :

- chiffrement de données par des pirates dans le cadre d'exfiltration d'informations depuis un réseau attaqué,
- chiffrement de données par des pirates lors d'attaques avec demande de rançon (exemple des attaques avec c*ryptolocker*),
- chiffrement par un mis en cause de ses supports informatiques,
- chiffrement des flux internet par les fournisseurs de services en ligne (services bancaires, messageries chiffrées etc…) lors d'interception de données.

Deux principales difficultés sont rencontrées au cours des enquêtes propres à l'OCLCTIC, ou dans les enquêtes pour lesquelles il intervient en assistance d'un autre service. En premier lieu, il s'agit de la découverte en perquisition d'un support numérique chiffré contenant potentiellement des éléments de preuve. En second lieu, il s'agit, à l'occasion d'une interception judiciaire de données internet ou mobiles, de l'utilisation par le mis en cause d'une messagerie instantanée ou VOIP utilisant un protocole chiffré (Skype, Viber etc.).

Concernant les supports physiques chiffrés, une première tentative de déchiffrement est réalisée par les enquêteurs souvent en coopération avec le propriétaire du support. S'il ne coopère pas, une tentative de déchiffrement est réalisée par un expert ou un institut spécialisé (SDPTS, IRCGN..) pour décrypter déchiffrer les fichiers placés sous scellé.

Dans les situations techniques les plus complexes et notamment lorsque la clé de chiffrement est trop évoluée, les fichiers cryptés chiffrés sont transmis à l'organisme technique soumis au secret de la défense nationale et désigné par décret (article 230-2 du code de procédure pénale).

Compte tenu de l'utilisation croissante des logiciels de chiffrement par les criminels, le groupe Robert avait préconisé dans sa recommandation n° 43 que l'officier de police judiciaire puisse requérir lui-même un expert ou un organisme, et que le magistrat ait la possibilité de saisir directement l'organisme technique soumis au secret de la défense nationale. Ces évolutions ont été consacrées par la loi du 13 novembre 2014.

Concernant le chiffrement des messageries instantanées et VOIP interceptées au cours des enquêtes, il n'y a pas, à l'heure actuelle, d'autre solution que de solliciter par la voie de la commission rogatoire internationale le pays sur le ressort duquel est installée la société éditrice de la messagerie, pour tenter d'en obtenir la mise au clair.

Les autorités françaises soulignent qu'en matière de demande de déchiffrement des messageries sur internet, la procédure de la coopération judiciaire internationale est longue et le résultat est aléatoire.

La possibilité de déchiffrement en coopération avec une société privée est prévue par le droit français. Conformément à l'article 230-1 du code de procédure pénale, toute personne physique ou morale peut être requise pour effectuer des opérations techniques permettant d'obtenir la version en clair de ces informations ou pour obtenir une convention secrète de déchiffrement dans le cas où un moyen de cryptologic a ćtć utilisć.

Dans le cas d'un auteur refusant de communiquer la convention secrète de déchiffrement permettant de mettre au clair les données chiffrées, celui-ci s'expose aux sanctions prévues à l'article 434-15-2 du code pénal (3 ans d'emprisonnement et 45000 € d'amende).

5.2.3 E - e v i d e n c e (preuves électroniques)

La législation française connaît toutes les notions indiquées au point 2.B.3 du questionnaire GENVAL, à l'exception de la notion de "réseaux gérés ou contrôlés par des personnes soupçonnées de cybercriminalité », qui sera définie dans le cadre de la transposition en cours de la directive du 14 Aout 2013.

Dans tous les cas la preuve doit être recueillie loyalement, c'est-à-dire sans stratagème ni provocation à l'infraction, et de manière proportionnée à la gravité de l'infraction.

Les modalités de collecte, conservation et transfert des preuves électroniques et informatiques sont prévues par le code de procédure pénale.

Preuves collectées lors de perquisitions. Les services de police peuvent accéder aux données stockées sur le lieu de perquisition ainsi qu'à des données à distance ou situées à l'étranger (dans le respect des accords internationaux). Le support de stockage peut être copié ou saisi. Ces interventions auront lieu avec l'autorisation du propriétaire des lieux ou celle d'un magistrat selon le cas (enquête préliminaire, enquête de flagrance, commission rogatoire du juge d'instruction). Les praticiens appellent cependant de leurs vœux la modernisation du régime actuellement applicable à la saisie de données à distance qui, en étant assimilé à une perquisition, réduit fortement les possibilités d'enquête (article 57-1 du code de procédure pénale).

Données informatiques saisies auprès des opérateurs.

- La France dispose d'une législation relative à la conservation des données de trafic, qui oblige tous les opérateurs de systèmes de communication électronique à conserver celles-ci (à l'exclusion du contenu des communications) pour une période d'un an. Ces données peuvent être obtenues par les services de police sur simple réquisition à l'opérateur concerné. Les praticiens regrettent que l'annulation de la directive européenne sur la "conservation des données" ait réduit les perspectives d'amélioration de la coopération transfrontalière s'agissant de l'échange de données de base (une adresse IP par ex.)
- Des données portant sur les contenus consultés par un suspect peuvent faire l'objet d'une obligation de conservation par l'opérateur pendant une année, sur ordre de l'autorité judiciaire dans le cadre d'une enquête en cours.

Données obtenues lors d'infiltrations policières ou d'enquête sous pseudonyme.

La loi autorise également les enquêteurs spécialement habilités à surveiller des personnes suspectes en se faisant passer pour un coauteur, un complice ou un receleur. Cette autorisation est valable pour les infractions commises en bande organisée (infiltration) et en ligne (enquête sous pseudonyme) uniquement en matière de traite des êtres humains, de proxénétisme, de pédopornographie ou de mise en péril des mineurs en général, de criminalité organisée, de terrorisme, de jeux illégaux en ligne et de trafic de produits de santé.

Données obtenues lors d'interception de correspondances. Ces interceptions sont toujours supervisées par un magistrat.

5.3 Protection des droits de l'homme / libertés fondamentales

La France a une tradition de protection des droits de l'homme et à ce titre, internet est largement protégé par les principes de liberté d'expression, d'information et de communication ainsi que par le secret de la vie privée, des données personnelles et des correspondances.

La législation française prévoit évidemment que des droits fondamentaux et des libertés fondamentales puissent être limités dans le cadre des enquêtes et des poursuites en matière de cybercriminalité, afin de concilier le respect des libertés avec la sauvegarde de l'ordre public, pour qu'internet ne soit pas une zone de non-droit. Les restrictions concernent:

La liberté d'expression et la liberté d'information. La lutte contre les contenus illicites passe par des mesures de blocage et de filtrage (un fournisseur d'accès à internet peut être contraint par les autorités compétentes à ne plus donner accès à un site qui véhicule des contenus punissables); la loi française impose aussi aux opérateurs techniques des obligations de signalement et de retrait des contenus illicites; ces restrictions concernent également la communication commerciale abusive sur internet (spams).

Le droit au respect de la vie privée et la protection des données à caractère personnel. La France a adopté une législation relative à la conservation des données de trafic pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales. Les données sont conservées par les opérateurs techniques pour être mises à la disposition des autorités répressives à leur demande, dans le cadre d'une procédure pénale. Les données en question ne peuvent jamais porter sur le contenu des correspondances échangées ou des informations consultées.

L'équipe d'évaluation relève que s'agissant de la conservation des données de trafic visées par la directive 2006/24/CE qui a fait l'objet d'une annulation par la Cour de Justice de l'UE, la législation française, adoptée antérieurement à ladite directive, apporte des garanties supérieures en matière de protection des données et de contrôle des demandes d'accès aux données.

5.4 Compétence

5.4.1 Principes appliqués pour enquêter sur la cybercriminalité

La compétence territoriale française en matière de cybercriminalité permet d'enquêter, poursuivre et sanctionner la quasi-totalité des infractions relatives à la cybercriminalité qui ont, de près ou de loin, un rapport avec la France par un rattachement territorial dû à la nationalité de l'auteur ou sa qualité de résident, par le rayonnement territorial d'un élément constitutif du délit, par la situation de la victime ou du complice de l'infraction.

En particulier, afin de mieux lutter contre le tourisme sexuel la France a adopté une disposition rendant sa loi applicable aux citoyens et résidents français qui commettent de telles infractions à l'étranger, notamment lorsque le mineur victime a été mis en contact avec l'auteur des faits par le biais d'un réseau de communications électroniques.

5.4.2 Règles en cas de conflits de compétence et d'aiguillage à Eurojust

La décision-cadre 2009/948/JAI relative à la prévention et au règlement des conflits de compétence a été mise en œuvre par la France. Depuis lors celle-ci n'a jamais trouvé à saisir Eurojust pour résoudre de tels conflits.

Selon les autorités françaises les conflits de compétence trouvent plutôt des solutions grâce aux instruments d'entraide pénale telles que les dénonciations officielles et les transmissions spontanées d'information. Eurojust et le Réseau Judiciaire Européen peuvent être sollicités utilement dans ce cas si l'occasion s'en présente.

5.4.3 Compétence pour les actes de cybercriminalité commis dans le "nuage"

Comme énoncé ci-dessus les règles de compétence territoriale édictée par la France sont larges. La victime ne sait pas toujours où ses données sont hébergées, mais accepte en général de fournir son accès privatif dans le Cloud. En ce qui concerne les suspects, les autorités répressives françaises sollicitent l'hébergeur Cloud ; en l'absence de réponse de sa part, une demande d'entraide judiciaire est formulée si le pays concerné est partie à la Convention de Budapest.

5.4.4 Perception de la France à l'égard du cadre juridique pour lutter contre la cybercriminalité

Selon la réponse de la France au questionnaire et l'avis des praticiens français rencontrés lors de la visite sur place,

- Le cadre juridique français est pléthorique, de sorte que le nombre de dispositions applicables et leur éparpillement pourraient justifier une sorte de codification, au moins sous la forme d'un manuel pratique à l'usage de tous les acteurs concernés.
- Pourtant ce cadre juridique ne permet pas aux services de police français d'obtenir, et encore moins de communiquer à une autorité étrangère, des données élémentaires d'identification (par ex. une adresse IP, un numéro de téléphone) en dehors du cadre d'une demande d'entraide pénale internationale. Cet état de fait regrettable ralentit considérablement le cours des enquêtes criminelles internationales.

5.5 Conclusions

La France s'est dotée d'un arsenal juridique complet, qui est régulièrement mis à jour, pour incriminer très largement les comportements relevant de la cybercriminalité dans tous les domaines où celle-ci surgit; cette législation dense est régulièrement augmentée et mise à jour, toutefois :

- Les peines encourues sont élevées mais il a été rapporté, lors de la visite sur place, qu'elles font en général l'objet d'un usage insuffisant par les autorités judiciaires, ce qui crée un déséquilibre entre les moyens d'enquête mis en œuvre et les résultats atteints ;

- Les règles relatives à la mise en œuvre de certains moyens d'enquête et d'obtention des preuves numériques restent insuffisamment définies dans certains cas (ex. régime applicable à la recherche et l'analyse d'un système informatique) ou trop contraignantes dans d'autres (ex. captation à distance), conduisant à leur inefficacité, au regret des praticiens rencontrés (juges d'instruction, procureurs et policiers).

- Le droit français a devancé celui de l'Union européenne en matière de conservation des données de télécommunications (données de connexion, à l'exception du contenu des correspondances). Dans l'attente de son remplacement par un nouvel instrument, l'annulation de la directive européenne en la matière a réduit considérablement les perspectives d'échanges d'informations dans le cadre de la coopération transfrontalière.

6 ASPECTS OPERATIONELS

6.1 Cyberattaques

6.1.1 Nature des cyberattaques

La France a répondu que la nature des cyberattaques évolue constamment. Si les années 2011 à 2013 ont été particulièrement marquées par des attaques qui peuvent être qualifiées de « cyber-hacktivisme », ceci englobant ainsi des défigurations revendicatives et des attaques en déni de service faisant appel au militantisme. L'année 2013 a été marquée par une hausse importante des attaques en déni de service, méthode rendue populaire les années précédentes. Néanmoins, un grand nombre de ces attaques n'ont plus fait l'objet de revendications militantes.
En parallèle, les atteintes aux données personnelles ont également connues une hausse importante qui s'est poursuivie sur le premier semestre 2014. Celles-ci sont davantage mises en avant du fait de l'obligation de déclaration en cas de divulgation.
Depuis 2011, l'ANSSI a traité une centaine d'attaques informatiques de grande envergure visant des systèmes d'information de l'Etat ou des opérateurs d'importance vitale essentiellement à des fins d'espionnage.

6.1.2 Mécanisme de réaction aux cyberattaques

La loi 2013-1168 du 18 décembre 2013 donne à l'ANSSI la capacité d'imposer aux opérateurs d'importance vitale les mesures techniques nécessaires à la réponse à une cyberattaque majeure. L'organisation de crise est testée régulièrement au travers des *exercices Piranet*, ce plan gouvernemental fait actuellement l'objet d'une actualisation sous la conduite du SGDSN et devrait en particulier intégrer l'organisation territoriale de l'État. Ces travaux devraient s'achever fin 2015.

Parallèlement et comme déjà indiqué, l'OCLCTIC dispose d'un rôle de coordination des enquêtes judiciaires diligentées en matière de cyber criminalité.

Lorsque les suspects identifiés demeurent à l'étranger et lorsqu'une dimension internationale des faits est constatée, les parquets procèdent généralement à l'ouverture d'une information judiciaire, afin notamment de pouvoir utiliser les instruments d'entraide judiciaire dans le cadre des commissions rogatoires.

Le recours à l'entraide pénale internationale, par le parquet et par les magistrats instructeurs, est un outil utilisé dans les procédures relatives à la cybercriminalité. La Convention de Budapest est le principal fondement visé dans ces demandes, outre les conventions d'entraide bilatérales ou multilatérales (Convention des Nations-Unies contre la criminalité transnationale organisée).

La procédure de gel de données prévue par le protocole de Budapest est employée régulièrement, tant à l'intérieur de l'UE que vers des pays extérieurs à celle-ci.

Les données font en général l'objet d'une transmission après réception de la demande d'entraide pénale internationale, soit plusieurs mois après la demande de gel. Les données découvertes lors des analyses post mortem des systèmes présentent alors en général un intérêt finalement assez limité.

6.2 Actions contre la pédopornographie et les abus sexuels en ligne

6.2.1 Banques de données identifiant les victimes et mesures destinées à éviter une revictimisation

En France il existe une base nationale de contenus pédopornographiques dénommée CALIOPE ; elle est détenue par le Centre national d'analyse des images de pédopornographie (CNAIP). Composé de gendarmes travaillant en appui des unités de gendarmerie et des services de police les missions du CNAIP sont :

- d'administrer CALIOPE à partir des contenus (images et vidéos) découverts au cours d'enquêtes de gendarmerie ou de police, ainsi que de tous les éléments pertinents liés à ces enquêtes (photos d'anthropométrie, photos d'arrière-plans, caractéristiques techniques des matériels de réalisation de contenus découverts, références des affaires, identités des protagonistes, origine des contenus …) ;

- d'analyser les contenus en vue d'identifier les victimes et les auteurs, principalement au moyen de logiciels de rapprochement d'images ou de métadonnées ;
- de fournir les contenus traçables utilisés lors des enquêtes sous pseudonyme, ainsi que les empreintes numériques utiles aux recherches criminalistiques ; sur ce second point, le CNAIP est relayé en gendarmerie par des moyens spécifiques à l'échelon régional et des moyens standards au niveau départemental ;
- d'assurer une parfaite complémentarité avec la base internationale de contenus pédo-pornographiques (ICSE) détenue par INTERPOL.

Lorsqu'une infraction est constatée, l'accès à l'image ou la représentation du mineur présentant un caractère pornographique est supprimé et les images concernées sont supprimées.

Par ailleurs, les infractions relatives aux images ou vidéos pédopornographiques sont conçues, en droit français, par rapport à l'auteur des faits. Ainsi, une personne peut être poursuivie pour avoir fixé, enregistré, transmis, offert, rendu disponible, diffusé ou consulté une image ou représentation d'un mineur présentant un caractère pornographique, quelle que soit l'image ou représentation en cause, et même si cette image ou représentation a déjà servi de fondement aux poursuites diligentées à l'encontre d'une autre personne.

Les images sont intégrées dans les bases d'images nationales et internationales (notamment la base Interpol), et les internautes qui détiennent, échangent et diffusent ces images sont poursuivis pénalement. Dans le cadre de ces poursuites, les supports numériques sont saisis.

La plate-forme PHAROS s'efforce de faire supprimer les contenus pédopornographiques qui lui sont signalés. Quand ils sont hébergés sur des serveurs informatiques français, les hébergeurs en sont informés, à charge pour eux d'appliquer l'article 6 de la loi du 21 juin 2004 sur la confiance dans l'économie numérique, qui leur enjoint de supprimer les contenus manifestement illicites portés à leur connaissance. Quand ils sont hébergés sur des serveurs étrangers, un message est adressé aux services de police du pays concernés via le réseau INTERPOL.

6.2.2 Mesures de lutte contre l'exploitation et les abus sexuels en ligne, le sextage et la cyberintimidation

Concernant les abus sexuels/l'exploitation sexuelle en ligne : la mise en relation de l'auteur des infractions sexuelles avec la victime par le biais d'un moyen de communication électronique est une circonstance aggravante de la majorité des infractions sexuelles commises au préjudice des mineurs (notamment corruption de mineur, recours à la prostitution de mineurs, viol et agression sexuelle, atteinte sexuelle, proxénétisme et traite des êtres humains).

Concernant la cyberintimidation, la loi n° 2011-267 du 14 mars 2011 a introduit dans le code pénal l'article 226-4-1 réprimant d'un an d'emprisonnement et de 15 000 € d'amende le fait « d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération ». Cette disposition a pour objet de permettre une répression des usurpations d'identité d'un tiers, mais également l'usage de toute donnée permettant de l'identifier (telles que adresse électronique, numéro de téléphone, pseudonyme). Cet article permet également de réprimer le fait de troubler la tranquillité d'autrui ou de porter atteinte à son honneur ou à sa considération. Le fait par exemple de participer à un forum internet en diffusant le numéro de téléphone d'une personne et en incitant les autres participants à contacter ce numéro sera constitutif de ce délit, tout comme le fait d'utiliser l'adresse électronique d'une autre personne et de lui faire tenir par ce biais des propos de nature à porter atteinte à son honneur.

Par ailleurs, la loi n°2014-873 du 4 août 2014 pour l'égalité réelle entre les femmes et les hommes a créé une nouvelle infraction de harcèlement moral définie ainsi : « Le fait de harceler une personne par des propos ou comportements répétés ayant pour objet ou pour effet une dégradation de ses conditions de vie se traduisant par une altération de sa santé physique ou mentale".

Concernant le sextage, ces faits sont réprimés par les dispositions générales sur les images pédopornographiques (article 227-23 du code pénal).

Ces phénomènes criminels sont pris en compte par la plateforme PHAROS au travers de signalements qui lui sont adressés par des victimes, des particuliers non directement victimes ou par des fournisseurs de services en ligne (réseaux sociaux, etc...)

Ils se classent dans trois catégories principales :

- **Les faits commis par des proches qui profitent de la possession de photographies intimes pour harceler leurs victimes**. Ces faits sont parfois précédés d'usurpations d'identités et/ou de piratages de comptes sur des réseaux sociaux. Les auteurs étant généralement dans l'entourage des victimes, ces faits relèvent de la compétence des services territoriaux de police et de gendarmerie.

- **Le chantage à des fins sexuelles**, commis par des individus inconnus des victimes. Classiquement, ils abordent leurs victimes sur internet, gagnent leur confiance, obtiennent d'elles des photos intimes puis menacent de les diffuser si elles ne se livrent pas à des actes d'exhibitionnisme plus poussés.

- **L'extorsion de fonds** : des individus généralement basés à l'étranger utilisent le mode opératoire ci-dessus pour obtenir de l'argent.

Dans tous les cas, la plateforme PHAROS contacte les victimes et les assiste pour prendre des mesures de conservation des preuves avant de les orienter vers des services d'enquête territoriaux. A l'occasion de ces contacts, PHAROS prodigue aux victimes les conseils afin qu'elles soient en mesure d'apporter aux services territoriaux tous les éléments de preuve nécessaires. Lorsque les auteurs sont inconnus des victimes, PHAROS recense les identifiants numériques des suspects (adresse e-mail, profil, etc.) pour faire des recoupements. Ces identifiants numériques conservés et recoupés par PHAROS sont des données publiques contenues dans les signalements (par exemple, l'URL du profil Facebook de l'auteur d'une infraction).

Au sein de la Préfecture de police de Paris, la Brigade de Protection des Mineurs participe à la lutte contre les phénomènes d'abus sexuels ayant une composante internet. En revanche, les menaces, chantages sur internet ou les réseaux sociaux ne ressortent pas de ses compétences d'attribution. Cette lutte prend la forme de trois champs d'action complémentaires :

- conduite d'enquêtes sur les faits relevant de sa compétence (exploitation et abus sexuels) portés à sa connaissance par le biais de plaintes et de signalements, rassemblant les preuves pour permettre des poursuites pénales par l'autorité judiciaire,
- travail d'initiative (enquête sous pseudonyme et cybersurveillance) sur les réseaux sociaux ou sites d'échanges d'images ou de vidéos les plus utilisés par les amateurs de pédopornographie afin de les identifier,
- travail d'analyse technique des vidéos pédopornographiques découvertes au cours des enquêtes aux fins d'identification des éléments vocaux permettant d'en localiser l'origine et de transmission aux services compétents pour poursuite des investigations et identification de la victime (l'OCRVP pour les vidéos françaises et INTERPOL pour les vidéos étrangères).

6.2.3 Prévention du tourisme sexuel, des spectacles pornographiques impliquant la participation d'enfants et autres

Toute publicité relative aux possibilités de commettre des abus sexuels et au tourisme sexuel impliquant des enfants est interdite aux termes de la législation française.
Cette législation réprime depuis de nombreuses années le tourisme sexuel commis à l'encontre de personnes mineures et afin d'améliorer la répression de toutes les formes de tourisme sexuel la loi française a été rendue applicable pour l'ensemble des crimes ou délits sexuels commis contre des mineurs à l'étranger par des Français ou des personnes résidant habituellement sur le territoire français, et ce sans condition de dénonciation ou de plainte préalable et de réciprocité d'incrimination.

Par ailleurs, l'article 2-3 du code de procédure pénale déclare recevable la constitution de partie civile de toute association déclarée depuis au moins cinq ans et dont l'objet statutaire comporte la défense ou l'assistance de l'enfant en danger, même en l'absence de poursuites ou de plainte de la victime.

En outre, le recours à la prostitution de mineurs est réprimé par le code pénal d'une peine de 5 ans d'emprisonnement, portée à 7 ans lorsque l'infraction est commise de façon habituelle ou à l'égard de plusieurs mineurs ou lorsque la victime a été mise en relation avec l'auteur des faits grâce à l'utilisation d'un réseau de communications électroniques.

Bonnes pratiques

L'Office central pour la répression des violences aux personnes (OCRVP) met en place des **partenariats avec les ONG** et notamment avec ECPAT France : élaboration d'un manuel de signalements des comportements de tourisme sexuel en milieu hôtelier, transmission à l'OCRVP des signalements afférents à des cas de tourisme sexuel, participation à des campagnes publiques d'information et de sensibilisation

Le Ministère de l'éducation nationale a diffusé une **campagne de sensibilisation aux dangers du cyberharcèlement** à l'école et a mis en place, dans ce cadre, un numéro d'appel gratuit et un site internet dédié.

Les services de poursuite prennent localement des initiatives de sensibilisation, avec les enquêteurs spécialisés, sur ces nouvelles infractions, tant à destination des responsables éducatifs des établissements scolaires que des mineurs eux-mêmes.

La section mineur du parquet de Saint-Malo a pris l'initiative, courant 2012, de proposer la tenue d'un forum sur les infractions liées aux réseaux numériques au cours duquel le magistrat du parquet est intervenu aux côtés de techniciens informatiques de la gendarmerie et de militaires de la brigade de prévention de la délinquance juvénile et de la brigade de recherche de Saint-Malo. Le parquet de Cherbourg a été associé à une action de formation en milieu scolaire autour des risques d'internet.

Des interventions sont menées par le parquet de Valence dans les établissements scolaires pour débattre auprès des collégiens et des lycéens des risques liés aux multimédias (Facebook, « happy-slapping », l'atteinte à la vie privée, le droit à l'image). Le parquet de Mulhouse a mis en œuvre un projet multi-partenarial de prévention pour améliorer le traitement de procédures pénales diligentées de chefs d'infractions sexuelles commises sur et par des mineurs ; le parquet des mineurs de Mulhouse ayant constaté que beaucoup de dossiers ne relèvent pas du champ d'application du code pénal - faute de défaut de consentement des plaignants ou plaignantes réellement caractérisé - mais traduisent une réalité sociologique alarmante : l'entrée dans la sexualité d'adolescents de plus en plus jeunes, parfois avec des pratiques sexuelles violentes liée à la pratique des nouveaux moyens de télécommunication et à l'utilisation massive d'internet qui augmentent les facteurs de risque de passages à l'acte sexuel problématiques. Ce projet a pour but de sensibiliser les adolescents aux situations à risques et de faire comprendre aux adolescents en quoi les réseaux sociaux et les nouveaux moyens de télécommunication multiplient les situations à risques et les faire réfléchir sur les moyens d'éviter ces dernières sans renoncer aux premiers. Dans le cadre de cette action les adolescents sont amenés à créer eux-mêmes une campagne de sensibilisation destinée à être diffusée auprès de leurs pairs.

Le **Service National d'Accueil Téléphonique de l'Enfance en Danger** (S.N.A.T.E.D.), plus communément appelé « 119-Allô enfance en danger » a deux missions :

- une mission de prévention et de protection : accueillir les appels d'enfants en danger ou en risque de l'être et de toute personne confrontée à ce type de situations, pour aider à leur dépistage et faciliter la protection du mineur en danger ;
- une mission de transmission : transmettre les informations préoccupantes concernant ces enfants aux services départementaux compétents en la matière : les cellules de recueil des informations préoccupantes (C.R.I.P.)

Le **numéro national d'aide aux victimes**, le 08 VICTIMES (08 842 846 27) qui a pour missions :

- L'écoute, pour mieux comprendre la demande de la victime
- L'information, qui permet à chacun de trouver des repères (comment porter plainte ? comment se faire indemniser ?)
- L'orientation vers les associations ou services d'aide aux victimes conventionnés par le Ministère de la Justice, les plus proches du domicile de la victime. Cette orientation peut, pour les infractions les plus graves, et pour les victimes qui le souhaitent, prendre la forme d'une transmission des coordonnées de la victime à l'association compétente géographiquement, qui prendra l'initiative d'un nouveau contact avec la victime.

Il existe en France **un grand nombre de sites internet informatifs à destination des enfants et des parents**. Parmi eux, le portail officiel "www.internet-signalement.gouv.fr" de la plateforme PHAROS contient des rubriques « conseils aux jeunes », « conseils aux parents », « internet prudent », « protéger son ordinateur », ainsi que des liens en direction d'autres sites gouvernementaux, notamment celui de la CNIL.

La gendarmerie nationale a créé le "**Permis internet", initiative destinée aux élèves de l'école primair**e visant à proposer aux enseignants un programme « clé en main » de prévention sur les dangers de l'internet et de présentation de bonnes pratiques pour son utilisation, avec la participation des forces de sécurité. Les matériels pédagogiques nécessaires ont pu être réalisés grâce à un partenariat public-privé. Depuis décembre 2013, 600 actions "Permis internet" ont été menées dans 550 écoles, dont 70 à l'étranger. Ce sont ainsi plus de 15.000 élèves qui sont désormais sensibilisés aux dangers d'internet. La police nationale va également mettre en œuvre cette opération".

Par ailleurs des associations spécialisées, agréées par le Ministère de l'Education nationale, telles que « e-enfance », « Internet sans crainte » et « Droit @ L'Enfance » interviennent dans les écoles pour informer les jeunes. Elles disposent d'un matériel pédagogique idoine.

6.2.4 Acteurs de la lutte contre les sites contenant ou diffusant de la pédopornographie et mesures prises

La loi française précise qu'il n'existe pas, pour les fournisseurs d'accès et d'hébergement, d'obligation générale de surveillance «des informations qu'ils transmettent ou stockent », ni «d'obligation générale de rechercher des faits ou des circonstances révélant des activités illicites ». Une activité de surveillance ciblée et temporaire peut leur être demandée par l'autorité judiciaire. Les fournisseurs d'accès et d'hébergement doivent aussi déférer aux décisions de Justice destinées à faire cesser ou à prévenir un dommage et la neutralisation de certains sites est prévue par la loi. Le blocage ou la neutralisation peut être ordonnée par l'autorité judiciaire ou résulter d'une mesure de police administrative.

La loi du 21 juin 2004 pour la confiance dans l'économie numérique a été la première à prévoir un dispositif de lutte contre les contenus illicites. La personne lésée s'est vue reconnaître le droit de requérir de l'hébergeur implanté en France le retrait de données manifestement illicites et de faire appel à l'autorité judiciaire pour y parvenir.

La loi impose aux fournisseurs d'accès et d'hébergement de « mettre en place un dispositif facilement accessible et visible permettant à toute personne de porter à leur connaissance ce type de données ».

En matière de lutte contre les contenus pédopornographiques et partant du constat que la grande majorité des images en question sont diffusées par des sites hébergés à l'étranger, le législateur français a instauré en 2011 un dispositif de protection des internautes contre les images de mineurs à caractère pornographique en prévoyant un système de filtrage des sites internet contenant des images pédopornographiques.

Il fait peser, non plus sur les hébergeurs, mais sur les fournisseurs d'accès, l'obligation de mettre obstacle aux contenus illicites pédopornographiques dont les adresses électroniques seraient désignées par le ministre de l'Intérieur, sous peine de sanctions pénales. Ce dispositif repose sur la mise à jour en temps réel d'une liste d'adresses. Implantée sur les serveurs des fournisseurs d'accès à internet (FAI), cette liste doit empêcher les internautes d'accéder aux sites répertoriés ou du moins, gêner l'accès à ces sites, en affichant à la place une page d'information officielle.

Le Conseil constitutionnel français a estimé conforme à la Constitution une telle procédure administrative de blocage, compte-tenu de son caractère proportionné et de la nature de son objet. Le décret 2015-125 du 5 février 2015 permet désormais la mise en œuvre de cette loi en confiant à l'O.C.L.C.T.I.C la charge de l'établissement et de la transmission des listes d'adresses électroniques dont l'accès doit être interdit sous le contrôle d'une personnalité qualifiée désignée en son sein par la commission nationale de l'informatique et des libertés.

La loi fait aussi obligation aux fournisseurs d'accès à internet de mettre à disposition de leurs abonnés un logiciel de contrôle parental afin de leur permettre de restreindre l'accès à certains services ou de les sélectionner.

Lorsqu'un serveur est hébergé à l'étranger, divers mécanismes de coopération policière dont ceux de l'UE sont utilisés. Il peut s'agir de demandes visant à préserver les données contenues sur ce serveur dans le cadre d'enquêtes menées au sein d'un service français, dans l'attente de la production d'une commission rogatoire internationale. Le réseau 24/7 est alors privilégié pour la rapidité de sa mise en œuvre. Sont utilisés indifféremment le réseau 24/7 du Conseil de l'Europe ou celui mis en place par le G8. Le canal BCN Interpol est utilisé dans les autres cas.

Des demandes de coopération visant des serveurs hébergés au sein d'Etats membres de l'UE sont adressées via le système sécurisé d'échange d'information SIENA. Il s'agit de messages visant à informer les Etats que des serveurs hébergeant des contenus illicites existent dans leur pays (Ce type de messages fait suite aux signalements effectués via la plateforme PHAROS au sein de l'OCLCTIC ou à des enquêtes menées par tout service d'investigation spécialisé). Il peut également s'agir de messages à visée opérationnelle (demandes de renseignements par exemple). Le canal BCN est utilisé si le pays hébergeur n'est pas membre de l'UE.

L'Office Central pour la Répression des Violences aux Personnes (OCRVP) est le bureau central national d'INTERPOL et le point d'entrée national pour les questions de pédopornographie. Ce service a également une compétence nationale. Il compte dix enquêteurs affectés au groupe central des mineurs victimes, dotés d'un niveau d'expertise élevé qui traitent des affaires liées à la pédopornographie et au tourisme sexuel impliquant des mineurs. Cette unité compte notamment des investigateurs en cybercriminalité chargés des exploitations des supports numériques.

Les unités régionales et locales de police traitent des infractions liées à la pédopornographie mais peu souvent d'initiative. Ces services sont saisis des dossiers initiés par l'OCRVP via les magistrats des tribunaux territorialement compétents. Localement, des enquêteurs investigateurs en cybercriminalité sont mis à contribution pour mettre à profit leur compétence sur ce type d'infractions.

Le département des activités illicites sur internet est une unité de gendarmerie qui comprend la section des atteintes aux mineurs et violences aux personnes (SAMVP) assurant la surveillance des réseaux, la conduite d'initiative et la coordination en gendarmerie des enquêtes sous pseudonyme, la formation à ces dernières, la direction d'enquêtes particulières et la coordination d'opérations de dimension importante et l'assistance aux unités territoriales.

La brigade de protection des mineurs de PARIS réalise des opérations de formation ou de sensibilisation ponctuelle sur des sollicitations diverses (associations, éducation nationale, établissements hospitaliers...) prenant la forme d'interventions à des colloques, des tables rondes. Elle est appelée à formuler régulièrement des propositions d'évolution législative, d'actions de sensibilisation ou de formation, dans son domaine de compétence propre (cf. Groupe de travail interministériel sur la lutte contre la cybercriminalité).

Le renforcement de ses capacités tant humaines que techniques est une préoccupation majeure pour lui permettre de maintenir son efficacité à la hauteur des enjeux et des évolutions de la cybercriminalité. En termes d'effectif, une politique volontariste de recrutement va permettre au Groupe de passer de 6 à 9 enquêteurs d'ici la fin de l'année 2014. Les moyens techniques alloués sont très satisfaisants suite aux efforts budgétaires consentis. Ils ont d'ailleurs permis au groupe d'être précurseur d'évolutions ensuite partagées au niveau national (constitution d'une salle informatique SARE, adoption du logiciel LACE..). Ces efforts doivent d'être maintenus sur le long terme, notamment pour répondre aux évolutions extrêmement rapides des nouvelles technologies. Par ailleurs, pour maintenir un niveau de connaissance suffisant eu égard aux évolutions, il est recouru parfois à des formations privées.

6.3 Fraude en ligne aux cartes de paiement

Si les victimes ne déposent pas toujours plainte en cas de fraude en ligne aux cartes de paiement, elles ont la faculté de signaler les faits grâce à un dispositif de signalement.

Si à l'occasion des plaintes ou signalements relatifs à certaines escroqueries, les services d'enquête ont connaissance de ce type de fraudes, la majorité des victimes ne dépose plus plainte compte-tenu des mécanismes d'indemnisation en vigueur résultant du code monétaire et financier : en cas d'opération de paiement non autorisée signalée par l'utilisateur dans les conditions prévues par la loi le prestataire de services de paiement du payeur rembourse immédiatement au payeur le montant de l'opération non autorisée et, le cas échéant, rétablit le compte débité dans son état antérieur.

Cette obligation de remboursement s'applique aussi lorsque le titulaire n'a pas été dépossédé de sa carte bancaire et comprend les frais bancaires supportés.

L'application de ces dispositions n'est pas conditionnée à l'existence d'une plainte.

La facilitation des signalements sur internet. Lorsqu'un particulier découvre un site lui laissant suspecter la commission d'une infraction sur internet, il peut le signaler sur le site de la plateforme PHAROS à l'adresse suivante : https://www.internet-signalement.gouv.fr/.

Les signalements sont traités par l'OCLCTIC et peuvent constituer le point de départ d'une enquête pénale.

En 2013, PHAROS a reçu 123.987 signalements (contre 119.788 en 2012 et 101.171 en 2011), soit une moyenne de 2.384 signalements par semaine. Dans leur grande majorité, ces signalements se classent dans trois catégories :

- escroqueries et extorsions : 56 % (stable)
- atteintes aux mineurs (pédopornographie, prédation sexuelle, etc.) : 12% (stable)
- xénophobie et discriminations : 10% (contre 8% en 2012)

Sur 123.987 signalements adressés à PHAROS, 7.698 ont fait l'objet de transmissions à une autorité compétente, (soit 6% environ), dont 1.488 pour enquête à des services d'enquête français.

Pour le moment, il n'existe pas en France de dispositif adapté au traitement de ce contentieux de masse. Ce point fait partie des recommandations du groupe de travail interministériel sur la cybercriminalité. Un projet est en cours pour créer un système de plainte en ligne permettant de recueillir toutes les données pertinentes à partir desquelles pourraient être effectués des rapprochements.

6.4 Conclusions

- L'arsenal mis en œuvre aux fins de prévenir et réduire les risques liés aux cyberattaques semble davantage orienté vers la protection de la réputation et de l'étanchéité des infrastructures que vers la protection des futures victimes potentielles contre la cybercriminalité.

- De manière générale l'absence d'une synergie articulée entre les différents corps de police impliqués dans les différents aspects opérationnels peut conduire à une disparité dans les stratégies de l'action publique et une déperdition des ressources. Deux initiatives démontrent qu'une approche commune ou collaborative apporte une efficience à la hauteur des défis : l'enquête sous pseudonyme et la plate-forme PHAROS.

- L'enquête sous pseudonyme, notamment telle qu'elle est mise en œuvre par les services de police spécialisés dans la protection des mineurs contre les infractions sexuelles est un outil de travail apprécié et particulièrement efficace. La pratique française présente à cet égard un fort intérêt pour les autres Etats membres.

- Une autre expérience très encourageante est celle de PHAROS, plateforme de signalement des contenus illicites sur internet, dont l'originalité et le succès mérite d'être soulignés ; PHAROS, composée de policiers et de gendarmes spécialement formés, permet l'analyse des signalements effectués par les internautes, par les associations et par les opérateurs du net et assure le suivi répressif le cas échéant.

7 COOPERATION INTERNATIONALE

7.1 Coopération avec les agences de l'UE

7.1.1 Exigences formelles pour la coopération avec Europol/EC3, Eurojust, ENISA

Il n'y a pas d'exigences formelles ni de procédures spécifiques pour la coopération entre les autorités nationales et Europol/EC3, Eurojust et l'ENISA en matière de lutte contre la cybercriminalité.

7.1.2 Évaluation de la coopération avec Europol/EC3, Eurojust, ENISA

La France est membre du Focal Point CYBORG. La coopération avec les services de l'OCLCTIC et les services de Gendarmerie est effective. A noter, à cet égard, l'opération Mousetrap (qui fait l'objet d'une OAP dans la sous-priorité "EMPACT Cybercrime", et l'opération Price en matière d'ingénierie sociale.

Les autorités françaises se sont montrées très satisfaites de la coopération avec les agences susmentionnées et en particulier avec Europol/EC3. Elles ont répondu comme suit au questionnaire GENVAL.

Europol/EC3.
La création d'EC3 correspond à un réel besoin de disposer au niveau européen d'un service spécialisé dans la lutte contre la cybercriminalité qui puisse :

- procéder à une analyse de l'ensemble du phénomène, à l'aide notamment des fichiers spécialisés de travail Focal Points comme TERMINAL pour les cartes bancaires,
- coordonner l'action des différents acteurs engagés.

Même si sa création est encore trop récente pour procéder à une véritable évaluation, il est clair que les capacités d'analyse d'EC3 s'avèrent très utiles aux enquêtes en cours dans plusieurs pays à la fois.

En matière de lutte contre la pédopornographie, le soutien apporté par le FP TWINS d'Europol permet de bénéficier de l'analyse des données, de la constitution de dossiers d'objectifs et d'une coordination opérationnelle.

Eurojust. Les autorités françaises ont évoqué pour se féliciter des résultats atteints, une affaire suivie par les JIRS de Rennes et de Paris faisant suite à un renseignement opérationnel du FBI selon lequel une enquête était diligentée aux Etats-Unis dans le but d'identifier et d'interpeller les concepteurs et les utilisateurs américains d'un malware (logiciel malveillant "**Blackshades"**), lequel permet la prise de contrôle à distance d'autres ordinateurs et notamment l'accès à toutes les données contenues sur l'ordinateur infecté.

Sous l'égide d'EUROJUST et avec la participation d'EUROPOL une action coordonnée des Etats-Unis et des neuf pays européens saisis (France, Autriche, Belgique, Estonie, Finlande, Allemagne, Pays-Bas, Roumanie, Grande-Bretagne) a été menée, une enquête préliminaire étant confiée à l'OCLCTIC aux fins d'identifier les auteurs d'infractions sur le territoire français. A cet effet, le FBI a pu communiquer officiellement à l'OCLCTIC une liste d'adresses IP d'acheteurs français du logiciel, associées à des informations déclaratives (nom, adresse postale, adresse mai, téléphone). EUROPOL a aussi contribué à la coordination de cette action qui a conduit à l'interpellation de plus de 70 personnes en France dont 20 par la BEFTI co-saisie sur son ressort territorial avec l'OCLCTIC et à la détection d'une vingtaine de dossiers intéressants.

La coopération entre la France et plusieurs pays membres a aussi été mise en place au sein d'Europol et Eurojust dans plusieurs procédures portant sur des escroqueries par faux ordre de virement international ou sur des infractions dites de contenu commises au moyen de sites internet hébergés en France, notamment aux fins d'exécution concertée et simultanée des commissions rogatoires internationales.

Selon l'équipe d'évaluation, Eurojust pourrait également soutenir la création d'un réseau européen de magistrats spécialisés en matière de cybercriminalité. Un tel réseau favoriserait l'échange de bonnes pratiques, faciliterait la coopération transfrontalière et permettrait la diffusion d'informations actualisées sur l'état de la cybercriminalité dans l'UE et sur l'évolution des technologies de l'information et des menaces qu'elles induisent.

ENISA.L'ANSSI représente la France au Conseil d'administration de l'ENISA et coopère avec celle-ci dans le cadre de ses activités en matière de sécurité des systèmes d'information.
La France fait observer que l'ENISA n'a pas pour mission première de lutter contre la cybercriminalité mais de relever le niveau global de sécurité des systèmes d'information (SSI) en Europe. Toutefois la SSI joue un rôle important dans la prévention de la cybercriminalité. L'ENISA organise par conséquent chaque année une conférence réunissant les communautés SSI et de maintien de l'ordre et a récemment signé un accord de coopération avec Europol (EC3). La France est satisfaite de cette coopération qui devrait à la fois permettre aux deux agences d'échanger sur leurs domaines d'expertise respectifs, tout en s'assurant de l'absence de redondance entre leurs activités.
À la question de savoir **quelles recommandations pourraient être faites pour une utilisation plus efficace des agences de l'UE** susmentionnées, **les autorités françaises ont répondu comme suit**.

- Il est essentiel d'éviter toute redondance entre les activités d'Europol et de l'ENISA. Si l'EC3 a vocation à lutter contre la cybercriminalité, l'ENISA s'intéresse au renforcement de la sécurité technique des systèmes d'information. A titre d'exemple, la prévention de la menace cyber sur les infrastructures critiques – traitée au niveau national par les agences de cybersécurité – relève pleinement du domaine de compétence de l'ENISA et non de celle d'Europol.

- Une formation européenne (au besoin organisée de manière régionale pour tenir compte des barrières linguistiques) sur l'utilisation d'EUROPOL/EC3 pourrait être dispensée à des enquêteurs spécialisés et expérimentés de chaque état-membre afin de leur permettre de maîtriser les dispositifs de coopération européenne et d'en faire une ressource apte à armer des équipes communes d'enquête.

- L'utilisation d'EUROJUST serait plus efficace si chaque Etat Membre disposait d'une juridiction nationale spécialisée dont les magistrats bénéficieraient d'une formation à la coopération européenne.

7.1.3 Résultats opérationnels des ECE et des cyberpatrouilles

La France n'a pas encore d'expérience concrète à partager dans ce domaine.

7.2 Coopération entre les autorités françaises et Interpol

Les échanges via Interpol se font par le biais de la messagerie dédiée hébergée au sein des points de contact nationaux d'Interpol (BCN).
L'OCLCTIC et la gendarmerie participent également aux groupes de travail, réunions et conférence organisés par INTERPOL. Par ailleurs, il existe une interaction opérationnelle entre la base internationale ICSE et la base nationale CALIOPE en matière de contenus pédopornographiques.

7.3 Coopération avec des pays tiers

La politique de coopération s'appuie en priorité sur les outils existants de lutte contre la cybercriminalité, en premier lieu la Convention de Budapest. L'OCLCTIC a participé à titre d'expert à divers projets mis en œuvre par le Conseil de l'Europe (cybercrime@IPA, GLACY…) visant à aider des pays tiers (Balkans, Maroc, Sénégal, etc..) à mettre en place des outils de lutte contre la cybercriminalité tels que des points de contact 24/7, une législation adaptée, ou des unités de lutte.

Depuis 2008, L'OCLCTIC dispense de façon régulière des formations à destination de pays d'Afrique de l'ouest (Sénégal, Côte d'Ivoire, Burkina Faso, Bénin, Togo) afin de qualifier des enquêteurs spécialisés en cybercriminalité. Ces actions ont permis, grâce à une volonté politique forte des pays concernés, la mise en place d'outils de lutte comme une plate-forme de signalement en Côte d'Ivoire au sein d'une Direction de l'Informatique et des Traces Technologiques du Ministère de l'Intérieur. Le Sénégal quant à lui est engagé dans le processus de ratification de la Convention de Budapest.

La gendarmerie nationale mène également des actions de formation à l'étranger et notamment à destination des pays africains et a participé au Sénégal au projet GLACY du Conseil de l'Europe.
La BEFTI est impliquée également comme expert en prenant des stagiaires sur des périodes de 15 jours à deux mois (Côte d'ivoire, Algérie...) et en dispensant des formations à l'étranger avec la BFMP ou l'OCLCTIC (Maroc, États arabes unis, Madagascar...).

Le canal des points de contact 24h/24 et 7j/7 est fréquemment utilisé car il permet un échange facilité. Enfin, le réseau des Attachés de sécurité Intérieure, ou des officiers de liaison revêt une grande importance car il offre la possibilité d'échanges directs et simplifiés avec des interlocuteurs identifiés.

7.4 Coopération avec le secteur privé

La coopération avec le secteur privé national a déjà été décrite plus haut.
La coopération avec les entreprises étrangères pose principalement le problème de la reconnaissance du droit français. Certains partenaires privés, notamment les acteurs majeurs de l'internet s'y soumettent difficilement, tant pour des raisons d'organisation que de culture. Néanmoins, ces entreprises, lorsqu'elles sont destinataires de réquisitions judiciaires font preuve d'un niveau de coopération inégal mais de plus en plus satisfaisant. Elles ont reconnu le principe du traitement direct des réquisitions judiciaires sans exiger des autorités judiciaires françaises la délivrance de commission rogatoires internationales. Toutefois, des progrès sont attendus et notamment, la mise en place d'une représentation française mandatée pour les obligations légales, afin de pouvoir disposer d'un relais (s'agissant de Facebook et Twitter) ainsi que sur la garantie de la confidentialité des demandes adressées par les enquêteurs. La non application de la loi française aux prestataires techniques étrangers exerçant une activité économique sur le territoire français est un des problèmes majeurs de la coopération internationale impliquant le secteur privé. Cette difficulté a été notamment soulignée par le groupe de travail interministériel sur la lutte contre la cybercriminalité présidé par le procureur général Marc Robert sur la lutte contre la cybercriminalité.

Les autorités répressives coopèrent régulièrement avec les succursales locales de sociétés privées ayant leur siège dans un Etat tiers, en particulier aux États-Unis. Il peut arriver que les réponses soient partielles ou faibles mais la procédure n'est pas affectée puisque le juge est seul à pouvoir décider de la recevabilité de la preuve. Les moyens employés pour solliciter les succursales voire les pays à l'étranger n'étant pas coercitifs, les réponses obtenues sont admissible à titre de preuve.

7.5 Instruments de la coopération internationale

7.5.1 Entraide judiciaire

Il n'y a pas de fondement juridique spécifique à l'entraide pénale en matière de cybercriminalité. En conséquence les dispositions du code de procédure pénale relatives à l'entraide pénale s'appliqueront par défaut, s'il n'y a pas d'instrument conventionnel contraire. Suivant le stade procédural auquel la demande d'entraide interviendra, l'autorité compétente pour émettre une telle demande sera le procureur de la République, le juge d'instruction ou la juridiction de jugement. En ce qui concerne l'exécution des demandes d'entraide entrantes, le procureur de la République ou le juge d'instruction sera compétent selon les actes de procédures à effectuer, conformément au droit national.

Les canaux de transmission sont ceux prévus par les Conventions, et à défaut par le code de procédure pénale. En l'absence de toute Convention applicable, le code de procédure pénale prévoit qu'en cas d'urgence la transmission des demandes peut se faire directement entre autorités judiciaires compétentes pour les exécuter (art. 694).

Lorsque les dispositions de la Convention de Budapest ont vocation à être appliquées, en l'absence de traité d'entraide notamment, la France a déclaré que, même en cas d'urgence, les demandes d'entraide émanant des autorités judiciaires françaises et destinées aux autorités judiciaires étrangères sont transmises par l'intermédiaire du Ministère de la justice et les demandes d'entraide émanant des autorités judiciaires étrangères et destinées aux autorités judiciaires françaises sont transmises par la voie diplomatique. Il peut cependant être fait application des dispositions de la Convention prévoyant (art.29) le gel des données à travers le réseau H24.

Une proportion importante des dossiers d'entraide étant traitées par voie de transmission directe entre les autorités judiciaires compétentes, le Ministère de la justice (Bureau de l'entraide pénale internationale) ne dispose pas de statistiques à leur sujet ni d'informations précises sur leur déroulement concret et leurs résultats.

Les acteurs rencontrés ont souligné la nécessité de raccourcir les délais de réponse aux demandes d'entraide internationale, et suggéré que cela pourrait être facilité par le développement de formulaires et procédures allégés pour certains types de demandes - en distinguant, par exemple, les données de trafic des données de contenu, dans le respect des principes fondamentaux du droit, nécessité de simplifier au niveau européen, afin d'obtenir en temps utile des informations de base (ex : identification d'une adresse IP, d'une adresse mail, numéro de téléphone ou de compte bancaire).

Sur le territoire européen ou une partie de celui-ci et pour des catégories d'infractions à l'instar du mandat d'arrêt européen, pourrait être défini un espace au sein duquel (non limitatif) :

- l'échange de renseignements et de constatations (y compris sous pseudonyme) se ferait librement ;
- les réquisitions auraient partout un caractère opposable ;
- l'accès total à un système informatique distant à partir d'un système initial, tous deux situés dans cet espace, serait autorisé au cours d'une perquisition ou depuis un local de service (dépassement du cadre de l'art. 32 de la convention de Budapest).

7.5.2 Instruments de la reconnaissance mutuelle

En ce qui concerne la mise en œuvre des instruments de reconnaissance mutuelle, et pour les raisons indiquées ci-dessus (transmission directe entre autorités compétentes), le Ministère de la Justice n'a pas d'information détaillée à fournir.

7.5.3 Remise/Extradition

Mandat d'arrêt européen. La catégorie "cybercriminalité" à laquelle se réfère la décision-cadre sur le mandat d'arrêt européen n'étant pas définie en droit français, Il appartient à l'autorité émettrice du mandat d'apprécier si l'infraction visée entre dans cette catégorie. Il existe des infractions correspondant directement à cette catégorie (infractions aux STAD) et d'autres qui peuvent aussi correspondre à une autre catégorie, telle celle '"d'escroquerie". 15 remises ont été effectuées entre la France et un autre Etat-membre dans le cadre de cette procédure de remise, correspondant à la catégorie "cybercriminalité".

Extradition. Les infractions entrant dans le champ de l'extradition ne sont pas définies en fonction de leur nature mais en fonction de la peine encourue, dont le quantum varie selon l'instrument conventionnel applicable. Les autorités françaises ne sont donc pas en mesure d'en fournir une liste.

En matière de cybercriminalité, comme pour les autres catégories d'infractions, les autorités compétentes pour recevoir/envoyer des demandes de remise/extradition et pour statuer sur ces demandes sont les mêmes que pour les autres infractions et elles varient selon le fondement juridique conventionnel de la demande. Au sein de l'Union européenne, la transmission des demandes se fait directement entre autorités judiciaires compétentes lorsque le mécanisme du mandat d'arrêt européen est mis en œuvre.

7.6 Conclusions

- Les services de police français coopèrent étroitement avec Europol/EC3 et le support fourni par ceux-ci a fait l'objet de retours d'expériences très positif de la part des services d'enquêtes rencontrées sur place. De manière générale la France est très impliquée dans le fonctionnement du dispositif européen mis en place pour renforcer la prévention et la lutte contre la cybercriminalité ; les priorités définies au niveau européen se reflètent dans l'action des autorités policières françaises.

- Selon les éléments recueillis lors de la visite sur place, les possibilités offertes par Eurojust semblent moins bien connues ou utilisées pour faciliter la coordination judiciaire et la coopération avec les Etats tiers dans le domaine de la cybercriminalité.

- La convention de Budapest est considérée par les praticiens français comme l'instrument de référence en matière de coopération internationale dans le domaine de la cybercriminalité, notamment grâce à la possibilité de solliciter en urgence, par le biais de points de contact nationaux, la préservation immédiate des données numériques pour une durée minimale de 60 jours dans l'attente d'une demande d'entraide judiciaire. Toutefois, la durée est variable selon les pays.

- La lenteur des procédures d'entraide judiciaire internationale empêche notamment les interceptions rapides des serveurs informatiques impliqués dans les cyber-attaques. Cette situation pourrait être nettement améliorée, au niveau européen au moins, par l'instauration de procédures allégées ou de la faculté de réquisition en particulier pour des informations cruciales parmi les données de trafic (ex. adresse IP).

- La coopération entre les autorités françaises et Interpol (ISCE) est bonne ; les canaux G8 et G 20 sont bien utilisés.

8 FORMATION, SENSIBILISATION ET PREVENTION

8.1 Formation spécifique

Les élèves des écoles de police, de gendarmerie et de la magistrature bénéficient évidemment d'une formation initiale (quelques heures) consacrées à la cybercriminalité. Les cours peuvent être complétés, selon les années, par des conférences ou des ateliers de police scientifique et technique.

1. Formation des magistrats

Chaque année l'Ecole Nationale de la Magistrature propose deux types de formation continue ouverte aux magistrats :

a/ -Une session de formation de 5 jours sur la cybercriminalité, dont l'objectif est de sensibiliser aux enjeux de ce phénomène et à sa dimension internationale, aux évolutions législatives récentes, aux particularités des investigations numériques, au traitement judiciaire de cette délinquance. Cette session est pluridisciplinaire dans son public et ses intervenants (90 magistrats français et étrangers, policiers, gendarmes, douaniers etc.).

b/- Une formation universitaire diplômante en cybercriminalité, en partenariat avec l'université de Montpellier, dont l'objectif est d'appréhender les différentes infractions et responsabilités liées à la sécurité des systèmes d'information en général et à l'utilisation frauduleuse des réseaux numériques en particulier. Cette formation ouverte à une quinzaine de participants, se décompose en plusieurs modules répartis sur une durée de 6 mois, et s'achève par des examens venant valider l'acquisition des connaissances et savoirs enseignés. Seuls quelques magistrats, qui s'y inscrivent sur la base du volontariat, suivent ou ont suivi ce cursus.

En outre, une fois par an, l'OCLCTIC organise une **formation « approche de la cybercriminalité »** à destination des magistrats français. Pendant une semaine les intéressés sont sensibilisés aux aspects juridiques spécifiques en matière de cybercriminalité, aux moyens de lutte engagés et aux techniques particulières d'enquête.

Bien que l'Ecole de la Magistrature ait ainsi introduit quelques modules sur la cybercriminalité dans son offre de formation à l'attention des magistrats, ces formations ne sont pas rendues systématiques ni obligatoires, y compris pour les "référents". Les connaissances des praticiens susceptibles de traiter de dossiers de cybercriminalité restent insuffisamment développées, dans un domaine de technicité élevé où les avocats sont très souvent spécialisés.

2. Formation des policiers et des gendarmes

- Au sein de la police nationale, dans le cadre de la création de la Sous-direction de la Lutte contre la Cybercriminalité (SDLC), une section dédiée à la formation vient d'être créée. Elle est en charge de l'organisation des stages ICC ci-dessous, d'un stage "approche de la cybercriminalité" destiné aux magistrats mais également de différents projets de formation de primo-intervenants (800 prévus sur 5 ans).

La **formation « primo-intervenants »** est destinée aux policiers confrontés aux actes courants d'enquêtes en milieu numérique. Ils doivent être capables de procéder au recueil de la preuve dans des conditions garantissant sa validité juridique et de procéder à une première lecture des supports numériques. Ils sont également rompus à la spécificité de la prise de plainte en cybercriminalité et aux premiers actes d'enquêtes que sont les perquisitions et réquisitions. La durée prévue de ce stage est de deux semaines, la première en « distanciel », la deuxième en « présentiel » pour la partie pratique.

La **formation des investigateurs en cybercriminalité** (ICC) est assurée par l'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC). Elle se déroule sur 8 semaines. Deux sessions de 18 auditeurs sont organisées annuellement et permettent ainsi la formation de 36 ICC chaque année. 377 ICC sont déjà en activité. A l'issue de la formation, l'ICC est capable d'analyser et de catégoriser les infractions pénales spécifiques ou liées à la cybercriminalité, de réaliser des copies et des analyses de supports numériques dans le respect de la préservation de l'intégrité de la preuve, de procéder à des constatations techniques et de diligenter des enquêtes dans le domaine des technologies de l'information et de la communication. La formation des ICC est sanctionnée par un examen théorique et pratique ainsi que par une reconnaissance d'équivalence universitaire de niveau II (Bachelor/Master). Cette certification est conditionnée à trois années de pratique et à l'étude d'un dossier technique par un jury de professionnels.

L'OCLCTIC est présent aux réunions du Européan cybercrime training and education group (ECTEG) et participe activement à la création de contenu de formations.

En plus du stage ICC, une formation à la fraude à la carte bancaire est organisée annuellement au bénéfice des enquêteurs de la police judiciaire. Il s'adresse à 15 stagiaires, pour une durée de 4 jours. Son coût est évalué à 2.500 euros.

- Au sein de la préfecture de police de Paris, outre le stage ICC, la BEFTI suit certaines formations dans le privé et propose deux stages agréés au catalogue des formations professionnelles (FD06 et FD15) ouverts également aux magistrats et aux douaniers. Le premier, d'une semaine en immersion au service, est destiné à apprécier l'appétence ou non du stagiaire et à permettre de construire un vivier. Le second, d'une journée pleine, est relatif aux investigations policières numériques : prise de plainte, premières investigations et environnement technique, ou investigations approfondies et numériques, pour être autonome dans l'enquête simple. Par ailleurs, tous les sachant partagent leurs connaissances pour élever le niveau technique à moindre coût. Au sein de la BEFTI, les praticiens adaptent et délivrent la formation en fonction de l'évolution des enquêtes et de la technologie sans délai. Il y a ainsi des restitutions de nouveaux savoirs en délivrant une formation continue sur le site de la BEFTI au sein de la communauté des ICC et prochainement pour tous les ICC de la Préfecture de police de Paris tel qu'il est prévu dans le programme d'adaptation de la Préfecture de police de Paris à la lutte contre la cybercriminalité.

- Au sein de la gendarmerie nationale, dans la lignée des travaux d'harmonisation conduits au niveau européen par le European Cybercrime Training and Education Group (ECTEG) et du groupe de travail interministériel sur la cybercriminalité le dispositif suivant a été adopté :

- niveau 1 : sensibilisation de tous ses militaires et ceux des unités généralistes ou judiciaires locales en particulier par une formation de quelques heures en ligne de premiers intervenants en technologies numériques (P-NTECH) ; son contenu (support développé avec la police nationale dans le cadre du projet européen 2CENTRE) : définition et visages de la cybercriminalité, dispositifs et acteurs de la lutte, arsenal juridique, recueil d'une plainte, identifications et réquisition des prestataires techniques, recherches en sources ouvertes, participation à une perquisition en environnement numérique, activités d'auto-évaluation ;
- niveau 2 : formation en régions de quelques jours en présentiel de correspondants en technologies numériques (C-NTECH) dans les unités généralistes ou judiciaires locales ; son contenu : enseignements essentiellement pratiques permettant de prolonger l'action des P-NTECH avec la réalisation d'examens criminalistiques simples (téléphonie mobile en particulier) et d'investigations en sources ouvertes ;
- niveau 3 : formation d'enquêteurs en technologies numériques (NTECH) exclusivement affectés aux examens criminalistiques complexes ou aux investigations sur les réseaux dans des unités judiciaires départementales, régionales ou centrales ; formation dispensée au format d'une licence professionnelle répartie sur quatorze mois, avec dix semaines de présentiel partagées entre le centre de formation de police judiciaire de la gendarmerie et l'université de technologie de Troyes, des travaux à distance, des travaux pratiques en tutorat et un mémoire technique ; son contenu : aspect légaux et cadre opérationnel, technologies et architectures, systèmes d'exploitation, internet et réseaux, recherche d'information, outils criminalistiques, sécurité des systèmes d'information, partenaires industriels, pédagogie, témoignage devant une juridiction en Anglais, etc. La licence professionnelle NTECH est un diplôme validé par le ministère de l'enseignement supérieur et de la recherche.
- niveaux experts : formations ad-hoc pour experts en criminalistique numérique ou en investigation des réseaux des unités judiciaires centrales.

Aspect budgétaires. Le budget alloué à la formation nationale des investigateurs en cybercriminalité (ICC) organisée par l'OCLCTIC est d'environ 100 000 euros par an (transport, hébergement, salle de cours, repas…) hors matériel de formation et rémunération des formateurs. A ce budget s'ajoute les coûts de l'e-learning, qui a représenté en 2011 un investissement d'environ 60 000 euros.

Au sein de la gendarmerie, les coûts de formation sont, selon le niveau, quasi-nul au niveau 1 (P-NTECH), relativement bas au niveau 2 (C-NTECH) et significatifs (69.200 € pour 16 stagiaires annuels, répartis en 44.800 € de frais pédagogiques et 24.400 de frais de déplacement) au niveau 3 (NTECH), voire très élevés en incluant pour ce dernier niveau le prix des équipements individuels (720 K€ au total pour une promotion).

8.2 Sensibilisation

Les actions de sensibilisation organisées en France sont nombreuses, en provenance de tous les services compétents et à destination de tous les publics. Elles ont été largement décrites au cours du présent rapport.

Il convient cependant de relever la duplication, par les différents services de police, d'actions similaires de sensibilisation à destination des premiers intervenants, et l'absence de traduction en français du matériel conçu par Europol/EC3 (*Cyberbits*). Le contenu de la sensibilisation faite en direction des praticiens étant un processus évolutif mis à jour en fonction de l'évolution des technologies, les efforts réalisés en parallèle en sont d'autant plus redondants.

8.3 Prévention

8.3.1 Législation/politique national et autres mesures

En France les actions de prévention en matière de cybercriminalité sont nombreuses, qu'elles soient le fait d'administrations, d'organismes professionnels ou d'associations. Ces actions sont souvent menées en partenariat.

- Le ministère de l'intérieur, par sa présence dans les territoires, peut en effet contribuer significativement à rehausser le niveau de vigilance des particuliers, des acteurs économiques et des collectivités territoriales. L'axe 3 de son plan d'action stratégique **est relatif à l'amélioration du niveau de sensibilisation et de prévention contre les cyber menaces des particuliers, des acteurs économiques et des collectivités :**

- impulser une politique de prévention et de sensibilisation à la cybersécurité, organisation de campagnes de communication et de sensibilisation associant les professionnels du net et les associations ayant passé des conventions de partenariat avec les services du ministère de l'intérieur (notamment la plate-forme PHAROS) ;
- contribuer au renforcement du dispositif interministériel des observatoires zonaux de la sécurité des systèmes d'information. Leurs actions de sensibilisation et d'alerte doivent pouvoir être conduites pleinement auprès des acteurs économiques et des collectivités territoriales ;
- renforcer les compétences en sensibilisation à la cybersécurité des « réseaux d'intelligence économique » et « référents sûreté » de la gendarmerie et de la police nationales, contribuer à la sensibilisation dans l'enseignement secondaire et universitaire, lancer une opération de sensibilisation à destinations des collectivités territoriales ;
- poursuivre le développement des actions de sensibilisation à destination des acteurs économiques par une convention de partenariat avec la chambre de commerce et d'industrie France (CCI-France).
- promouvoir le dispositif « Permis Internet » déjà cité, à destination des élèves du primaire.

L'expérimentation lancée par la gendarmerie va être généralisée en septembre 2014 et son extension à la police est à l'étude ;

- participer à la consolidation des réseaux régionaux de la réserve citoyenne de cyberdéfense déployés au cours de l'année 2013-2014. Ces réservistes d'horizons divers, particulièrement impliqués dans la diffusion de l'esprit de cyberdéfense, constituent d'excellents relais pour diffuser les bonnes pratiques.

Le groupe de travail interministériel sur la lutte contre la cybercriminalité présidé par le procureur général Marc ROBERT a lui-même identifié la prévention comme une priorité et a émis quelques recommandations, qu'il s'agisse de protéger les internautes par une approche humaine, ou d'éviter la commission des infractions par une approche technique:

- impliquer davantage l'État en terme d'impulsion, de synergie, de définition des objectifs, de pilotage à long terme dans la politique de prévention de la cybercriminalité, par des campagnes de sensibilisation destinées au grand public (protection des données, vigilance contre les escroqueries) ou à des publics plus restreints (pôles de compétences), l'harmonisation et la généralisation des différents supports préventifs utilisés, la création d'un numéro public d'urgence de l'internet, la réalisation systématique d'études de risque des nouveaux services réglementés ;
- faire de l'internaute le premier acteur de sa propre sécurité, par l'éducation au numérique à l'école en lien avec les professionnels, le développement d'espaces d'information en ligne ou par téléphone, la mise en ligne d'un moteur de recherche facilitant la détection des cyber-infractions, une meilleure association des structures d'aide aux victimes ou de consommateurs ;
- mobiliser les professionnels en assurant une meilleure cohérence des actions de sensibilisation, en instaurant un cahier des charges d'obligations préventives à respecter par les établissements publics ou privés ouvrant sur l'internet (commerce en ligne, fournisseurs d'accès, plates-formes de téléchargement, vendeurs d'appareils numériques...), en préconisant un plan de prévention pour les grandes entreprises et en incitant à la création de CERT pour répondre aux attentes des petites et moyennes entreprises ;
- mobiliser la recherche et l'industrie françaises et européennes pour la détermination de réponses techniques et technologiques appropriées.

Les actions de prévention conduites par les services de police et de gendarmerie ont été déjà abordées.

De plus en plus de services de poursuite locaux s'impliquent dans la prévention. Plusieurs organisent des réunions de sensibilisation souvent en coopération avec les enquêteurs spécialisés, tant à destination des responsables éducatifs des établissements scolaires que des enfants et des jeunes.

Ainsi le parquet de Versailles a lancé en 2014 un plan d'action de lutte contre la cybercriminalité en raison du développement du nombre des infractions relevant de la cybercriminalité, et de la technicité des contentieux dans ce domaine. Il s'agit dans un premier temps de dresser un état de la délinquance dans ce domaine, et de rappeler les dispositifs législatifs et techniques à disposition des parquets. Ce plan d'action comprendra :

- d'une part l'organisation d'une **rencontre des procureurs et de leurs substituts avec les directeurs des offices centraux compétents**. Une politique volontariste doit en effet être définie en lien avec les services d'enquête spécialisés, qui peuvent aider les parquets à mieux cibler les objectifs, à leur fournir des clés de compréhension du phénomène, et des éléments pratiques en termes de recherche et de recueil de la preuve numérique.

- d'autre part l'organisation d'une **journée de formation,** dans le cadre de la formation continue déconcentrée de la cour d'appel de Versailles, qui permettra de fournir une base technique et juridique actualisée, et **d'échanger sur les bonnes pratiques,** afin d'aider les parquets à faire face aux difficultés (textes applicables, compétence territoriale, problématiques liées aux éléments d'extranéité) .

Autre excellente initiative locale, le parquet de Lons-le-Saunier a en projet, à titre de mesure alternative aux poursuites, la création de stages de prévention sur les violences sexuelles commises par les mineurs, afin de faire prendre conscience aux auteurs le respect du corps d'autrui, mais également, les dangers des réseaux sociaux et d'internet qui banalisent certains comportements sexuels inadaptés.

Enfin, la section des mineurs du parquet de Paris a pour objectif de créer un stage de soins à l'encontre des auteurs de faits liés, notamment, à la détention d'images pédopornographiques. Ce stage, ordonné comme alternative aux poursuites, serait essentiellement fondé sur un partenariat avec une association dans le cadre d'un protocole. Il se composerait d'un suivi médical et psychologique très rigoureux et prolongé dans le temps. L'objectif est en effet d'imposer au mis en cause une véritable réflexion, doublé d'un suivi, sur les faits commis, plus long et contraignant.

8.3.2 Partenariat public/privé (PPP)

Les exemples de partenariat public-privé pour la prévention et la lutte contre la cybercriminalité sont nombreux et un certain nombre ont été évoqués ci-dessus au point 4.3.

Le centre expert contre la cybercriminalité français (CECyF), parmi les premières actions proposées à ses membres, a réalisé ou projette de réaliser :

- une étude des besoins en formation et une cartographie des formations disponibles ainsi qu'un processus de labellisation de ces formations ;
- la contribution à la création de supports de sensibilisation ex : réalisation avec son membre Signal Spam et Paypal d'une plaquette de sensibilisation sur les escroqueries aux petites annonces ;

le lancement avec Signal Spam d'un site d'information (prévention, détection, nettoyage) sur les botnets, dans le cadre du projet européen ACDC : www.antibot.fr ;

- le développement de formations à distance, pour les services d'investigation comme pour les entreprises ou les collectivités territoriales ;
- une étude des besoins en recherche et développement ainsi qu'un processus de labellisation de projets de R&D ;
- le développement d'outils en sources ouvertes d'investigation numérique ;
- la participation à des conférences, pour dynamiser les échanges entre les communautés sur les différents aspects de la prévention et de la lutte contre la cybercriminalité ;
- l'organisation d'une conférence francophone sur la réponse aux à incidents et l'investigation numérique (CoRI&IN, Lille, janvier 2015) et le soutien officiel d'autres événements ;
- des contributions aux revues spécialisées ;
- une publication scientifique gratuite sur des sujets techniques, juridiques, criminologiques : « Le Journal de la Cybercriminalité et des Investigations Numériques (CybIN ; journal.cecyf.fr) ;
- des ateliers pour l'identification et la construction des nouveaux projets.

8.4 Conclusions

- L'offre de formation aux services d'enquête est abondante, ce qui représente indéniablement un point très positif. Toutefois, en raison du compartimentage important des différents services d'enquêtes, cette offre est aussi fort diversifiée, au point de créer un risque de double emploi et une disparité des méthodes d'enquête qui pourrait freiner l'efficacité globale des poursuites. Si police et gendarmerie doivent pouvoir conserver le modèle de formations multi-niveaux adapté à chacune de leurs organisations, l'harmonisation des contenus et méthodes peut cependant être recherché au moyen de référentiels communs servant à construire ces formations.

- La spécialisation de certains magistrats dans le domaine de la cybercriminalité repose sur une pratique empirique et ne résulte pas d'une politique ou d'une stratégie. Les magistrats "référents en cybercriminalité" sont désignés sans condition de formation certifiée, celle-ci n'étant pas obligatoire.

- Les autorités françaises multiplient les bonnes initiatives dans le domaine de la sensibilisation du public et la prévention de la cybercriminalité (voir, entre autres, l'exemple du CECyF ci-dessus).
- Un dialogue entre les opérateurs privés, et les autorités devrait se développer, notamment aux fins de renforcer les mécanismes d'identification des contenus litigieux (pédopornographie, incitation au terrorisme), ainsi que les modalités de leur retrait à chaque fois que cela s'avère nécessaire.

9 REMARQUES FINALES ET RECOMMANDATIONS

9.1. Suggestions de la France

La prévention et la lutte contre la cybercriminalité pourrait se trouver renforcée par la définition d'une stratégie interministérielle globale en la matière afin de mettre en cohérence l'action des différents acteurs et le renforcement des actions de formations et de prévention.

En ce qui concerne la prévention et la réponse aux attaques informatiques, la mise en œuvre par les Etats membres de dispositions similaires à celles prises dans le cadre de la loi adoptée en France en 2013 permettrait de traiter le cas fréquent de systèmes d'information déployés dans plusieurs pays. C'est le sens du projet de directive Network & Information Security proposée par la Commission le 7 février 2013 et votée par le Parlement en mars 2014.

Les attentats terroristes du début d'année 2015 en Europe sont venus rappeler l'enjeu que représente l'espace numérique pour la lutte contre le terrorisme. Compte tenu des similitudes des enjeux identifiés pour la prévention et la répression, dans l'espace numérique, des infractions liées au terrorisme et celles liées à la criminalité de droit commun, les autorités françaises proposent que ce volet fasse l'objet de deux recommandations spécifiques mettant en relief les besoins de dialogue avec les grands opérateurs d'Internet et de garanties afin que les capacités de chiffrement ne constituent pas un obstacle technique insurmontable pour les services compétents en matière de prévention, détection et poursuite des infractions pénales, en particulier en matière de lutte contre les infractions les plus graves, dont le terrorisme.

9.2 Recommandations

Pour ce qui est de la mise en œuvre et du fonctionnement pratique de la décision-cadre et des directives, l'équipe d'experts qui a participé à l'évaluation de la France a pu examiner le système français dans des conditions satisfaisantes.

La France devrait procéder à un suivi des recommandations figurant dans le présent rapport 18 mois après l'évaluation et rendre compte des progrès effectués au groupe "Questions générales, y compris l'évaluation" (GENVAL).

L'équipe d'évaluation a jugé opportun d'adresser un certain nombre de suggestions aux autorités françaises. Elle a en outre présenté, sur la base des différentes bonnes pratiques, des recommandations à l'UE, à ses institutions et agences, et notamment à Europol.

9.2.1 Recommandations à la France

La France devrait :

1. Etudier et faire part des suites données au rapport du groupe interministériel sur la cybercriminalité présidé par le procureur général Marc ROBERT (cf. notamment 3.2, 3.3, 3.5, 4.6, 5.2, 8.3) ;

2. Renforcer la coordination de l'action de tous les acteurs concernés en la confiant au besoin à une entité nationale chargée de mettre en œuvre la stratégie d'ensemble dans tous ses aspects et en synergie avec les autorités de cyberdéfense et cybersécurité. (voir, par exemple, les développements du rapport ROBERT en la matière) (cf. 3.2.2, 4.5, 4.6) ;

3. Construire un outil national de mesure qualitative et quantitative du phénomène cybercriminel utilisant une classification et un lexique standardisés, pour appréhender sa dimension réelle et réduire d'autant le "chiffre noir" (cf. 3.3.2, 3.5) ;

4. Favoriser la mise en œuvre par les autorités compétentes d'orientations judiciaires stratégiques en matière de cybercriminalité susceptibles d'améliorer le suivi de ce contentieux et de l'action publique, et de réactualiser une politique pénale incluant la définition de priorités, la prise en compte de l'existence de juridictions spécialisées et l'élaboration d'outils pédagogiques à destination des magistrats (cf. 3.2.2, 3.5, 4.1, 7.1, 8.3, 8.4) ;

5. Renforcer les capacités nationales de protection des systèmes d'information au profit des petites et moyennes entreprises ainsi que des particuliers (cf. 3.2.1, 3.5) ;

6. Analyser les conditions dans lesquelles des entités publiques exerçant des missions dans le secteur de l'internet signalent aux autorités répressives que des faits portés à leur connaissance paraissent constituer une infraction pénale ; en effet la définition d'une politique globale de lutte contre les cybermenaces ne peut être réalisée qu'à condition que les infractions constatées soient portées le plus largement possible à la connaissance des autorités répressives, auxquelles il appartient de définir la réponse pénale appropriée (y compris le classement sans suite) (cf. 3.1, 3.3.2, 3.5) ;

7. Instaurer, à la charge des opérateurs économiques, une obligation de dénonciation des fraudes aux moyens de paiement électroniques s'appuyant sur un système qui permettrait de recueillir et d'exploiter les données indispensables et propres à ce contentieux de masse, et serait de nature à réduire le chiffre noir de la cybercriminalité (cf. 3.3.2, 3.5) ;

8. Remédier aux difficultés concrètes que rencontrent les praticiens en matière de recherche et d'obtention des preuves de l'infraction cybercriminelle, face à la multiplicité et l'ambigüité des textes de procédure actuellement applicables ; envisager la création d'un régime procédural propre au recueil de la preuve numérique, cohérent, complet et d'un usage adapté aux besoins des enquêtes judiciaires, en alliant efficacité et respect des droits fondamentaux (cf. 4.1.2, 5.2.3, 5.5) ;

9. Poursuivre les efforts de dotation en ressources humaines, en matériels et en formation qui sont consentis aux services d'enquête spécialisés et généralistes, sans lesquels les excellents résultats atteints par ces services ne pourraient être maintenus et permettant d'élever leur niveau de compétence et d'accroître la qualité de réponse aux victimes (cf. 3.2.2, 4.2, 4.6, 6.2);

10. Envisager la création de référentiels communs de formation pour les enquêteurs en cybercriminalité appartenant aux différents services de police judiciaire, dans le but d'assurer l'homogénéisation des profils et la création d'un réseau d'expertise interservices, au profit de l'efficience des enquêtes et de l'accroissement de l'expertise nationale (cf. 8.1, 8.4) ;

11. Homogénéiser la documentation relative à la lutte contre la cybercriminalité qui est mise à la disposition des différents corps d'enquêteurs, en développant une approche commune et en s'appuyant, notamment, sur les ressources conçues et diffusées par Europol (voir également les recommandations n°15 et 23) (cf. 8.2, 8.4) ;

9.2.2 Recommandations à l'Union européenne, à ses Institutions et aux autres États membres

L'Union européenne devrait :

12. Envisager, en impliquant Eurojust et Europol dans cette réflexion, des solutions permettant, dans le respect des droits fondamentaux, de surmonter les obstacles et lenteurs liés à l'échange entre les services répressifs des Etats membres d'informations numériques même élémentaires, dont l'obtention rapide peut constituer un enjeu crucial pour la résolution d'affaires cybercriminelles ; réfléchir à la définition d'un dispositif de coopération pénale simplifiée en matière de cybercriminalité entre Etats-membres de l'UE tant pour l'obtention des données que pour la mise en œuvre des décisions de nature à mettre fin aux activités illégales (sorte de « Schengen » du numérique) (cf. 5.2.3, 5.4.4, 5.5, 7.5.1, 7.6) ;

13. Suite à l'annulation de la directive 2006/24/CE du 15 mars 2006, réfléchir à la manière adéquate de combler le manque d'harmonisation des législations nationales en matière de conservation des données de trafic électronique, dans le respect de la jurisprudence de la Cour de justice de l'UE en matière de protection des droits fondamentaux (cf. 5.2.3, 5.5) ;

14. Inviter les Etats-membres, et le cas échéant des Etats tiers, qui ne l'ont pas encore fait à ratifier la Convention de Budapest sur la Cybercriminalité du Conseil de l'Europe et inciter à la poursuite des réflexions dans le cadre du Conseil de l'Europe sur la façon d'adapter la Convention de Budapest aux nécessités des enquêtes transfrontalières, par le biais de l'adoption d'un éventuel protocole; en particulier, la soumission des personnes morales étrangères aux obligations légales domestiques des pays dans lesquels elles ont une activité économique officielle est le problème majeur de la coopération internationale impliquant le secteur privé. Cette difficulté a été soulignée par le groupe de travail Robert sur la lutte contre la cybercriminalité (cf. 6.1.2, 7.3, 7.4, 7.6) ;

15. Soutenir un processus d'homogénéisation des formations dispensées aux praticiens (magistrats, policiers et gendarmes) en se référant à des profils définis, par exemple le *Training Competency Framework* mis au point par Europol/EC3 en partenariat avec le CEPOL, ECTEG et Eurojust ; faciliter la reconnaissance de ces formations au sein des Etats membres par la mise en place d'un système européen de certification (cf. 8.1, 8.2, 8.4) ;

16. Un dialogue avec les grands opérateurs d'Internet, hébergeurs, fournisseurs d'accès et/ou de services de l'internet, doit être rapidement structuré tant au niveau européen qu'au niveau international afin de renforcer leur coopération dans le cadre des investigations judiciaires et redéfinir un cadre global adapté aux obligations de ces prestataires. La mise en œuvre de l'agenda européen de sécurité pourrait être l'occasion de porter certaines initiatives en ce sens (cf. 9.1);

17. Des solutions d'ordre technique ou juridique devraient être mise en place au niveau de l'Union pour empêcher que le recours de plus en plus systématisé au chiffrement par les opérateurs, en particulier sur internet, ne devienne un obstacle à l'exercice par les services compétents de leurs pouvoirs d'enquête mis en œuvre conformément à la loi (cf. 9.1);

Les Etats membres devraient :

18. Faciliter, en s'appuyant sur Eurojust, la création d'un réseau européen de magistrats spécialisés dans la lutte contre la cybercriminalité visant à améliorer et faciliter la coopération judiciaire dans ce domaine (voir aussi la recommandation n° 20), (cf. 7.1, 7.6) ;

19. Engager, en s'inspirant du modèle français, une réflexion impliquant l'ensemble des acteurs institutionnels, économiques et associatifs concernés en vue de l'établissement d'une stratégie nationale de lutte contre la cybercriminalité (cf. 3.2, 3.5) ;

20. S'inspirer, dans le respect des droits fondamentaux, des bonnes pratiques françaises suivantes, susceptibles d'offrir d'excellents résultats :
- l'enquête sous pseudonyme, particulièrement utile dans le domaine de la protection des mineurs contre les atteintes sexuelles,
- la faculté pour les enquêteurs, dans des conditions bien encadrées par la loi, d'intrusion dans les systèmes d'information et de captation à distance au moyen d'un logiciel espion,
- le centre expert contre la cybercriminalité français (CECyF), l'une des réalisations du projet européen 2CENTRE financé par la Commission européenne visant à établir en Europe des centres d'excellence en matière de cybercriminalité,
- la plateforme policière PHAROS qui recueille les signalements de contenus illicites sur internet, dont l'originalité et le succès méritent d'être soulignés,
- la base nationale de données d'images pédopornographiques CALIOPE, qui fonctionne en lien avec Interpol,
- l'Observatoire de la sécurité des cartes de paiement établi auprès de la Banque de France, qui a pour mission d'améliorer la sécurité lors de l'utilisation de ce moyen de paiement ;

9.2.3 Recommandations à Eurojust/Europol/ENISA

Eurojust devrait :

21. Améliorer la sensibilisation des autorités répressives aux possibilités offertes par Eurojust pour faciliter et accélérer la coopération avec les autorités compétentes des Etats membre et des Etats tiers dans le domaine de la cybercriminalité (cf.7.1.2, 7.6) ;

22. Favoriser les échanges entre magistrats spécialisés dans le domaine de la cybercriminalité dans le but d'identifier les meilleures pratiques et faire progresser la coopération judiciaire (cf. 7.1, 7.6) ;

Europol devrait :

23. Poursuivre et renforcer le soutien offert aux Etats membres pour implémenter, dans la culture juridique et opérationnelle de chaque Etat, les formations et le matériel de sensibilisation que cette agence conçoit à l'attention des acteurs de terrain (cf. 8.1, 8.2, 8.4) ;

24. Assurer une meilleure diffusion des produits et des services opérationnels aux services enquêteurs ; assurer une meilleure diffusion des informations relatives aux projets européens, tel que le projet "Freetools", qui peuvent soutenir l'action des services spécialisés et de répondre à leurs besoins (cf. 7.1) ;

25. Tirer meilleur profit du déploiement du système SIENA dans les services d'enquête en vue d'encourager l'échange d'informations opérationnelles (cf. 6.2.4) ;

26. Améliorer la visibilités des sous-priorités EMPACT en dressant une cartographie des actions engagées en lien avec les opérations initiées par les « Focal Points »TERMINAL, CYBORG TWINS et le J-CAT (cf. 7.1.2).

ANNEXE A: PROGRAMME DE LA VISITE SUR PLACE

Mardi 28 octobre 2014

Secrétariat général des affaires européennes (SGAE), Paris

09h15 à 10h15 : accueil au SGAE – Salle Lisbonne
Mme Isabelle JEGOUZO, Secrétaire générale adjointe / SGAE
M. Frédéric MOLLARD, chef du secteur sécurité de l'espace européen du SGAE

10h30 : Secrétariat général de la défense et de la sécurité nationale / Agence nationale de sécurité des systèmes d'information (ANSSI), Paris

- introduction du Directeur Général adjoint
- présentation générale du contexte politico-stratégique et de l'historique du développement des capacités cyber en France
- présentation de l'ANSSI
- présentation du Centre opérationnel de la sécurité des systèmes d'information (COSSI) avec illustration autour d'un exemple de traitement d'incident
- présentation de la coopération entre les services opérationnels de l'Etat par M. Laurent Verdier.

12h00 : déjeuner à l'ANSSI

14h15 : Police nationale - Direction centrale de la police judiciaire, Nanterre

- présentation de la Sous-Direction de lutte contre la Cybercriminalité et notamment de sa composante opérationnelle au travers des groupes d'enquête
- focus sur la section de l'Internet comprenant la plateforme de signalement PHAROS, le dispositif Info-escroqueries et le nouveau bureau de l'Internet

- présentation de la coopération internationale autour de trois points essentiels :
- la conservation des données techniques,
- l'échange de données numériques,
- la présentation des points de contact 24/7 et leurs enjeux stratégiques dans la coopération internationale
- présentation de l'office central de répression de la violence aux personnes (OCRVP) compétent en matière de lutte contre la pédopornographie sur Internet.

Mercredi 29 octobre

9h30 : Commission nationale de l'informatique et des libertés (CNIL), Paris

- accueil par le Secrétaire Général de la CNIL, M. Edouard GEFFRAY, présentation générale des principales missions de la CNIL
- présentation des pouvoirs de contrôle a priori et en particulier de la mise en œuvre des traitements relevant du secteur police-justice
- présentation des pouvoirs de contrôle de la CNIL et illustration des pouvoirs de sanction par la présentation de cas concrets

13h00 : déjeuner au Pôle judiciaire de la gendarmerie nationale (PJGN)

14h30: **Gendarmerie nationale – Sous-direction de la police judiciaire / Pôle judiciaire de la gendarmerie nationale (PJGN), Rosny-sous-bois**

- présentation générale du dispositif général de la gendarmerie, puis du plateau d'investigation cyber-analyse numérique (PI CyAN) au sein du PJGN / SCRC+IRCGN
- visite département informatique électronique (INL) de l'IRCGN / démonstrations pratiques
- Division lutte contre la cybercriminalité : atteintes aux mineurs (veille, opérations coordonnées) et centre national d'analyse des images pornographique (CNAIP)
- Division lutte contre la cybercriminalité : présentation du département des investigations sur internet (D2I)
- Division lutte contre la cybercriminalité : présentation Guichet unique des technologies de l'information (GUTI)

Jeudi 30 octobre

9h00 : Ministère de la Justice – Direction des Affaires criminelles et des Grâces, Paris

- Le bureau de la politique d'action publique générale (BPAPG)
- Le bureau de la police judiciaire (BPJ)
- Le bureau du droit économique et financier (BEFI)
- Le bureau de la lutte contre la criminalité organisée, le terrorisme et le blanchiment (BULCO)
- Le bureau de l'entraide pénale internationale (BEPI)

12h00 : déjeuner

14h30 : **Préfecture de Police / Direction de la police judiciaire / Sous-direction des affaires économiques et financières, Paris**

- présentation du dispositif de police judiciaire spécialisé au niveau régional et ses liens avec le niveau national:
- la spécificité parisienne et son articulation avec les structures nationales (Police nationale-gendarmerie nationale)
- la brigade d'enquête des fraudes aux technologies de l'information (BEFTI) et ses missions : les atteintes aux systèmes de traitement automatisé des données, aux données à caractère personnel, contrefaçons de logiciels
- la brigade des fraudes aux moyens de paiement (BFMP) et les escroqueries aux cartes bancaires, faux ordres de virement, e-commerce et la brigade de répression de la délinquance astucieuse (BRDA) : escroqueries via internet
- la brigade de protection des mineurs et la pédopornographie
- visite du plateau BEFTI

- postes et matériels reliés au système d'analyse et de recherche électronique et dispositif d'extraction universel d'investigation numérique et d'analyse
- listage des matériels et logiciels
- bonnes pratiques : un minimum pour l'administration de la preuve (loyauté et intégrité) dans le système de l'intime conviction français.

18h30 : Ministère des affaires étrangères et du développement international (MAEDI), Paris

Réunion avec Mme Michèle RAMIS, Ambassadrice chargée de la lutte contre la criminalité organisée

<u>Vendredi 31 octobre 2014</u> :

09h15 à 11h30 - Réunion de clôture au Secrétariat général des affaires européennes, Paris

M. Frédéric MOLLARD, Chef du secteur sécurité de l'espace européen du SGAE

en présence de quelques représentants des Ministères concernés par l'évaluation.

ANNEXE B: PERSONNES RENCONTRÉES

Réunions/Meetings 28 Octobre/October 2014

Venue: Secrétariat Général des Affaires européennes (SGAE)

Personne interviewée/rencontrée **Person interviewed/met**	**Organisation représentée** **Organisation represented**
Mme Isabelle JEGOUZO	SGAE
M. Frédéric MOLLARD	SGAE
Mme Faiza ABDELOUAHAB	SGAE

Venue: Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Personne interviewée/rencontrée **Person interviewed/met**	**Organisation représentée** **Organisation represented**
M. Dominique RIBAN	directeur général adjoint ANSSI
M. Christian Daviot	chargé de mission stratégie ANSSI
M. Laurent VERDIER	ANSSI

Venue: Direction Centrale de la Police Judiciaire (DCPJ)

Personne interviewée/rencontrée **Person interviewed/met**	**Organisation représentée** **Organisation represented**
Maldonado Valérie Commissaire Divisionnaire Adjoint au Chef de SLDC et chef OCLCTIC	SDLC/OCLCTIC
Delphine GAY Commandant	OCLCTIC
Pierre Yves LEBEAU Commandant	OCLCTIC
CERF Mathilde Commissaire adjoint Chef OCRVP	OCRVP
ZARLOWSKI Chantal Commandant	OCRVP

Réunions/Meetings 29 Octobre/October 2014

Venue: Commission Nationale de l'Informatique et des Libertés (CNIL)

Personne interviewée/rencontrée **Person interviewed/met**	**Organisation représentée** **Organisation represented**
M.Edouard GEFFRAY	CNIL

Réunions/Meetings 30 Octobre/October 2014

Venue: Direction des Affaires criminelles et des Grâces (DACG)

Personne interviewée/rencontrée **Person interviewed/met**	**Organisation représentée** **Organisation represented**
Frédérique Dalle	Mission négociation - DACG
Claire Vuillet	BPPG - DACG
Clément Incerti	BPJ - DACG
Aurélien Letocart	BULCO - DACG
Vincent Filhol	BEFI - DACG
Amélie Rodrigues	BEPI - DACG

Venue: Ministère des Affaires Etrangères et du Développement International

Personne interviewée/rencontrée **Person interviewed/met**	**Organisation représentée** **Organisation represented**
Mme l'Ambassadrice Michèle RAMIS	Ministère des affaires étrangères et du développement international
Mr Léonard ROLLAND	Direction des affaires stratégiques, de sécurité et du désarmement
Mme Anne LEBOURGEOIS	Direction de l'Union européenne

ANNEXE C: LISTE DES ABRÉVIATIONS/GLOSSAIRE DES TERMES UTILISÉS

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	FULL NAME IN FRENCH OR IN ORIGINAL LANGUAGE	ENGLISH
ANSSI	*ANSSI*	*Agence Nationale de la Sécurité des Systèmes d'information*	The French Agency for cyberdefence and cybersecurity
BEFTI	*BEFTI*	*Brigade d'Enquête des Fraudes aux Technologies de l'Information (Préfecture de police de Paris)*	Brigade for the Investigation of Information Technology Fraud (Préfecture de police of Paris)
BFMP	*BFMP*	*Brigade des Fraudes aux Moyens de Paiement (Préfecture de police de Paris)*	Brigade for Means of Payment Fraud (Préfecture de police of Paris)
BPM	*BPM*	*Brigade de Protection des Mineurs (Préfecture de police de Paris)*	Brigade for pProtection of Minors (Préfecture de police of Paris)
CERT			Computer Emergency Response Team
COSSI	*COSSI*	*Centre Opérationnel de la Sécurité des systèmes d'Information*	Operational Center of ANSSI
CNAIP	*CNAIP*	*Centre National d'Analyse des Images Pornographiques*	National Analysis Center of Pornography Images
CNIL	*CNIL*	*Commission Nationale de l'Informatique et des Libertés*	The French data protection Authority
DACG	*DACG*	*Direction des Affaires Criminelles et des grâces (Ministère de la Justice)*	Directorate for Criminal Affaires and Pardons (Ministry of Justice)
DCPJ	*DCPJ*	*Direction Centrale de la Police Judiciaire (Ministère de l'Intérieur)*	Central Directorate of the Judicial Police (Ministry of Interior)
DGGN	*DGGN*	*Direction Générale de la Gendarmerie Nationale*	General Directorate of the National Marechaussee (Ministry of Interior)

LIST OF ACRONYMS, ABBREVIATIONS AND TERMS	FRENCH OR ACRONYM IN ORIGINAL LANGUAGE	FULL NAME IN FRENCH OR IN ORIGINAL LANGUAGE	ENGLISH
DGSI	*DGSI*	*Direction Générale de la Sécurité Intérieure (Ministère de l'Intérieur)*	The French counter-intelligence service (Ministry of Interior)
ENISA	*ENISA*	-	European Union Agency for Network and Information Security
GENVAL	*GENVAL*	*Groupe de travail "Questions Générales y compris l'Evaluation"*	Working Party "General Questions including Evaluation"
GUTI	*GUTI*	*Guichet Unique des Technologies de l'information*	"One Stop Shop" interface between the French Marechaussee and the IT operators
IP	-	-	Internet Protocol
JIRS	*JIRS*	*Juridictions interrégionales spécialisées*	Specialised interregional courts
OCLCTIC	*OCLCTIC*	*Office Central de Lutte contre les infractions liées aux technologies de l'information et de la communication*	Central Office for Combating Crime linked to Information and Communication Technologies
OCRVP	*OCRVP*	*Office Central de Répression de la Violence aux Personnes*	Central Office for Combating Violence against Persons
OSCP	*OSCP*	*Observatoire de la sécurité des cartes de paiement*	Observatory for Card Payment Security
PI-Cyan	*PI-Cyan*	*Plateau d'Investigation Cyber-Analyse Numérique (Gendarmerie Nationale)*	Cyber-analysis Investigation Center of the French Marechaussee
PJGN	*PJGN*	*Pôle Judiciaire de la Gendarmerie Nationale*	Judicial pole of the French Marechaussee
SGAE	*SGAE*	Secrétariat Général des Affaires Européennes (Premier ministre)	General Secretariat for European Affairs (a Prime Minister service)
STAD	*STAD*	Système de Traitement Automatisé de Données	Automated data processing system
VOIP	-	-	Voice Over IP