Conseil de
l'Union européenne

Bruxelles, le 16 mai 2017
(OR. fr)

9135/17

GENVAL 56
CYBER 74

NOTE DE TRANSMISSION

Origine:	Délégation française
Destinataire:	Délégations
Nº doc. préc.:	7588/2/15 REV 2 DCL 1
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" - Suivi du rapport sur la France

Chaque État-membre, à la suite de chaque cycle d'évaluations mutuelles, doit informer le Secrétariat Général du Conseil du suivi donné ou des actions implémentées par rapport aux recommandations mentionnées dans le rapport d'évaluation concerné. Ce suivi doit être soumis dans les 18 mois après l'adoption du rapport.

Les délégations trouveront ci-joint le suivi du rapport d'évaluation sur la France concernant les recommandations qui ont été mentionnées dans le rapport 7588/2/15 REV 2 DCL 1.

NOTE DES AUTORITÉS FRANÇAISES

Objet : Septième Cycle 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"* – Suivi des onze recommandations adressées à la France.

Réf. : ST 7588/2/15 REV 2

P. J. : un tableau de suivi sur l'état de mise en œuvre des onze recommandations adressées à la France (tableau de 14 pages).

L'objectif européen de prévention et de lutte contre la cybercriminalité a amené les États membres à se doter de moyens au niveau national dont la mise en œuvre a été appréciée dans le cadre du 7éme cycle 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 ».

À cette fin, le rapport d'évaluation sur la France a été adopté le 24 juin 2015 (ST 7588/2/15 REV 2), portant notamment des préconisations et orientations afin de satisfaire aux objectifs fixés au niveau de l'Union.

Ce rapport, ainsi que le document 15538/4/15, donnent lieu à un suivi dans un délai de 18 mois afin d'apprécier l'avancement dans la mise en œuvre de ces préconisations au moyen de l'édiction et de la transmission au Secrétariat Général du Conseil (SGC) d'un rapport de suivi. Tel est notamment l'objet du tableau annexé à la présente correspondance. À titre liminaire, et afin de faciliter la lisibilité du tableau annexé, les autorités françaises souhaitent faire part au SGC de plusieurs remarques introductives.

En premier lieu il semble opportun d'apprécier la mise en œuvre des recommandations en prenant en considération une mise en œuvre différenciée, dans le temps, suivant la nature des mesures à mettre en œuvre : ainsi certaines recommandations sont en cours. La période de suivi n'est ainsi pas suffisamment étendue pour permettre de constater à ce jour une avancée totale sur l'intégralité des recommandations.

Par ailleurs, certaines des thématiques ayant une très forte actualité dans les travaux actuellement menés au niveau européen (notamment sur le point du chiffrement), il est important de noter que la mise en œuvre au niveau national des recommandations y afférant est tributaire de l'avancée réalisée ou non au niveau supra-étatique.

Enfin, concernant la forme du tableau en tant que tel, les autorités françaises tiennent à préciser que le libellé de la première recommandation étant particulièrement large, le suivi de cette recommandation est dilué dans le suivi des dix autres. Ainsi, certains points qui pourraient y être exposés n'y sont qu'évoqués, pour faire l'objet de plus amples développements plus loin.

Pour une meilleure appréhension des informations, le suivi est organisé sous la forme d'un tableau que vous trouverez en annexe et faisant état des mesures institutionnelles, légales et administratives ainsi que des mesures d'ordre pratique et logistique prises ou envisagées afin de satisfaire aux recommandations proposées par l'équipe d'évaluation.

Septième Cycle 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 » Tableau de suivi : État de mise en œuvre des onze recommandations adressées à la France		
Les recommandations adressées à la France – la France devrait :	**Mesures institutionnelles, légales et administratives**	**Mesures d'ordre pratique et logistique, dispositifs en place ou en cours**
1. Étudier et faire part des suites données au rapport du groupe interministériel sur la cybercriminalité présidée par le Procureur Marc ROBERT		**S'agissant du Ministère de la Justice :** • **2015 : création de l'instance spécialisée de la « mission de prévention et de lutte contre la corruption et la Cybercriminalité » au sein de la DACG en février 2015.** Objectifs généraux : coordonner les actions de prévention et de lutte conduites par la direction dans le domaine de la cybercriminalité, l'élaboration des instructions de politique pénale adressées aux procureurs généraux et leur évaluation ainsi que la contribution de la direction aux travaux des instances européennes et internationales Bilan - Analyse détaillée des rapports d'activité 2015 des ministères publics sur le traitement de la cybercriminalité. - Participation active aux travaux internationaux et européens du recueil de la preuve numérique (point de contact de l'European Judicial Cybercrime Network) dont le chiffrement offline et online. - Réunion de travail avec la HADOPI avec pour objectif d'actualiser à moyen terme le mécanisme de « riposte graduée ». - Édiction de guides méthodologiques par la DACG, comme celui sur les faux ordres de virement particulièrement apprécié, avec notamment des avis systématiques aux juridictions interrégionales spécialisées (JIRS), ainsi que sur le recueil de la preuve numérique. - Suivi de la compétence nationale concurrente du parquet de Paris.

		Difficultés et obstacles : - Les cyber-référents sont une pratique aléatoire, réservée aux plus grands parquets. Du fait du lien entre cyber-infractions et préoccupations financières, les référents sont souvent des magistrats davantage spécialisés en droit pénal économique et financier. - La taille réduite de certains parquets n'est pas toujours propice à la spécialisation des magistrats. Les référents sont donc bien souvent les chefs de parquet, voire le procureur général. Perspectives : - Janvier 2017 : création d'une **« instance de coordination sur la stratégie numérique** » au sein de la DACG, déclinée en 7 groupes de travail. **S'agissant du Ministère de l'Intérieur :** Les questions 2 à 11 amenant à développer plus précisément certaines mesures relevant en réalité de la question1, les réponses sont intégrées directement dans les questions 2 à 11.

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 cyber sécurité.		**Stratégie nationale pour la sécurité du numérique** Une stratégie nationale pour la sécurité du numérique a été diffusée en octobre 2015 : elle a été élaborée avec l'ensemble des ministères et a été soumise par le secrétaire général de la défense et de la sécurité nationale à l'approbation du Premier ministre en application du 7° de l'article R*1132-3 du code de la défense. Il n'existe pas de structure spécifiquement dédiée à un objectif de coordination de la mise en œuvre de cette stratégie compte tenu de la diversité des infractions cyber qui rend impossible la centralisation du traitement de cette question. La coordination se fait donc par thématique, au sein des ministères selon les compétences qui leur sont attribuées, et non en interministériel. Chaque ministère est donc responsable de la stratégie ministérielle qui décline et met en œuvre, en ce qui le concerne, la stratégie nationale. **Mesures prises par le Ministère de l'Intérieur et ses services :** Institution d'une **délégation ministérielle aux industries de sécurité et à la lutte contre les cyber-menaces (DMISC)** au sein du Ministère de l'Intérieur par décret n° 2017-58 en date du 23 janvier 2017. Son objectif est de mettre en œuvre la stratégie nationale de sécurité du numérique. La stratégie de lutte contre les cybermenaces du Ministère de l'Intérieur décline les 5 objectifs de la stratégie nationale pour la sécurité du numérique au travers de 16 enjeux. Au sein de chacun de ces pôles sera mis en place un comité de pilotage. Nota : compte de la diversité des menaces liées à la cybercriminalité, les efforts consentis et les effets des mesures doivent être appréciés sur le moyen terme. Bilan : - Coordination des travaux relatifs à **l'actualisation de la stratégie de lutte contre les cyber-menaces du Ministère de l'intérieur**. - Mise en place d'un groupe de travail composé des services du ministère chargés de la lutte contre la cybercriminalité (DGPN/DCPJ/OCLCTIC, DGGN/C3N, PP, DGSI). - Fusion entre la délégation ministérielle aux industries de sécurité et la délégation de lutte contre les cyber-menaces.

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".		**Travaux en cours au sein du Ministère de l'Intérieur :** Les travaux sont toujours en cours, avec néanmoins trois avancées à noter : - Production de statistiques par un service dédié en matière d'atteintes aux STAD sur la base des préconisations du rapport Robert. Ce service spécifique (Service Statistique ministériel de la sécurité intérieure) rattaché au Secrétariat Général, a été créé en 2014 au sein du Ministère de l'Intérieur et représente un progrès important. Il a notamment pour vocation de produire un rapport annuel sur l'état de la menace afin d'actualiser le renseignement en matière de cybercriminalité. - Projets THÉSÉE et PERCEVAL, concernant respectivement les escroqueries en ligne et les usages frauduleux des moyens de paiement, devant permettre une meilleure connaissance de ces infractions. À noter : ces plateformes permettent une connaissance quasiment en temps réel des infractions de ce type, ce qui représente là encore un progrès notable. Ces deux plateformes seront développées plus en avant dans la question 7. **Travaux en cours au sein du Ministère de la Justice :** Amorce d'une réflexion destinée à faire évoluer les possibilités du logiciel CASSIOPEE. Il parait plus opportun de mentionner l'intérêt des Projets THESEE et PERCEVAL pour cette question, notamment au vu des données statistiques que ces plateformes pourront fournir.

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.	**Mesures législatives :** • 13 novembre 2014 : pénalisation des actes d'apologie du terrorisme (alors régis par la loi sur la presse, aménageant un délai de prescription de 3 mois) ; les affaires judiciaires traitées dans ce domaine sont désormais traitées en comparution immédiate devant les tribunaux correctionnels (400 décisions rendues, dont la majorité a donné lieu à des peines d'emprisonnement ferme) ; • Concernant les nouveautés procédurales issues de **la loi du 3 juin 2016,** l'on peut d'abord citer le **nouveau critère de compétence de la victime de cybercriminalité**.	**Structures judiciaires existantes :** • Il existe des structures judiciaires spécialisées au niveau de la région parisienne qui concourent à l'efficacité de traitement des affaires, notamment la section du Parquet de Paris, comportant deux magistrats, ainsi que des magistrats « référents cyber » dans les départements limitrophes. À noter : certains Parquets auront accès aux plateformes susnommées, ce qui leur permettra à la fois de recouper les affaires présentant des liens de connexité et de régler les questions relatives à la juridiction compétente. - Stratégie **:** En Janvier 2017 : création d'une « instance de coordination sur la stratégie numérique » au sein de la DACG. Cette dernière s'est déclinée en 7 groupes de travail chargés de traiter la question de manière complète. **Pistes à étudier pour le Ministère de la Justice :** Comme suggéré dans l'analyse des rapports d'activités, **un effort de formation des magistrats**, notamment des **cyber-référents** est une piste à étudier. Il convient de noter que l'ENM offre plusieurs formations continues de sensibilisation à la cybercriminalité, et que l'université de Montpellier propose un diplôme universitaire portant la mention « Cybercriminalité : Droit, Sécurité de l'information & Investigation numérique légale ».

	⇨ Insertion de l'article 113-2-1 nouveau du code pénal: lorsque des faits de crimes et délits sont tentés ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République par voie de réseaux de communication électronique, ils sont réputés commis sur le territoire de la République. Cette nouvelle disposition n'impose pas de plainte préalable. En outre, les dispositions relatives à la compétence du procureur de la République, du juge d'instruction et du tribunal correctionnel ont été corrélativement modifiées (articles 43, 52 et 382 du code de procédure pénale).	La cybercriminalité étant protéiforme, il est délicat de dégager des priorités globales dans la politique pénale. Une approche sectorielle paraît davantage pertinente. **Une réflexion est en cours en ce moment sur le traitement optimisé des « rançongiciels »**. À cet effet, une consultation approfondie est actuellement en cours au sein de la DACG afin de déterminer une politique pénale optimale en la matière. Par ailleurs, il faut également prendre note de l'importance croissante du contentieux en matière de **faux ordres de virement**, qui devient là aussi une priorité pour les services concernés. Sur cette question, l'instance de coordination stratégique de la DACG est chargée d'assurer des missions de veille globale, d'analyse et d'anticipation des enjeux liés à la révolution numérique en matière pénale, notamment dans le domaine de la preuve. Ses axes de travail concernent l'amélioration du recueil de la preuve numérique, de son traitement, et les perspectives en matière de lutte contre la cybercriminalité. Un premier état des travaux est attendu pour fin mars 2017.

	• Article 28 de la loi du 3 juin 2016 : modification des dispositions pénales relatives aux **atteintes aux systèmes de traitement automatisé de données** (articles 323-1 à 323-4-1 du code pénal), des articles 706-72 et suivants du code de procédure et création d'une **compétence concurrente des juridictions parisiennes** (du procureur de la République, du pôle de l'instruction, du tribunal correctionnel et de la cour d'assises de Paris et des juridictions des mineurs) pour ces infractions (art. 706-72-1 du code de procédure pénale). À noter : cette réorganisation des champs de compétence ne concerne pas que les atteintes en bande organisée aux STAD mis en œuvre par l'État, mais également les techniques spéciales d'enquête (enquête sous pseudonyme, notamment).	

5. Renforcer les capacités nationales de protection des systèmes d'information au profit des petites et moyennes entreprises ainsi que des particuliers.	.	**Mesures d'ordre pratique au sein du Ministère de l'Intérieur :** Bilan de l'action du ministère et des services concernés : - Participation au forum de la prévention et de la sensibilisation de la cybercriminalité piloté par EUROPOL. - Opérations de sensibilisation à l'attention de divers publics : magistrats, experts-comptables, juristes de banques, responsables de la sécurité des systèmes d'information, directeurs de sûreté, risk-managers, avocats, TPE/PME voire monde académique. - Contacts entre la DACG et l'ANSSI devant permettre de pousser la réflexion relative à l'amélioration de l'information des autorités judiciaires en cas de cyberattaques dénoncées à l'ANSSI, mais un travail de pédagogie à l'encontre des acteurs privés est requis. En effet, le risque de cyber sécurité devient de plus en plus un risque judiciaire (action contre un sous-traitant à la politique en matière de sécurité inadaptée, par exemple). Dès lors, il faut encourager l'entreprise victime de tels agissements à alerter les autorités judiciaires à la moindre alerte. En outre, les débats autour du chiffrement online et offline vont se poursuivre. - Conférences de sensibilisation des entreprises par la DGSI. À noter : développement de la formation des référents sûreté des autres directions générales, qui interviennent de plus en plus dans ce genre d'activités. - Édiction d'un guide pratique « Comment réagir à une attaque informatique » par la DCPJ à l'attention des TPE/PME.

		Dispositif national d'assistance aux victimes d'actes de cyber-malveillance (ACYMA). **Arrêté du 3 mars 2017 portant approbation de la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance (ACYMA) publié au Journal officiel de la République française le 5 mars 2017.** Après l'expérimentation menée conjointement par le Ministère de l'intérieur et l'ANSSI, dans la Région des Hauts-de- France pendant 2 mois à l'été 2017, le déploiement national est prévu **en octobre 2017**. Le co-pilotage est assuré par ces deux services. Objectifs : - Accompagner les victimes éventuelles en déterminant si elles sont bien touchées par un acte de cyber malveillance et, le cas échéant, les rediriger vers un professionnel répertorié qui saura prendre en charge leur problème. - Mener des actions et campagnes de sensibilisation pour améliorer la prévention de cette menace. - Être un observatoire du risque numérique, avec la coopération des professionnels répertoriés qui transmettront, à chaque acte de cyber malveillance, les informations utiles à l'édiction de statistiques en la matière. Cela permettra notamment d'affiner la connaissance de cette menace et le nombre de ces incidents. - **orientation et aide aux victimes en vue de la judiciarisation de leur dossier avec, en particulier, le souci de la préservation des preuves,** - **échanges d'expériences avec tant les services du ministère de l'intérieur que les magistrats spécialisés.**

		Fonctionnement : - Plate-forme numérique à vocation préventive, comportant également des services tels que la mise en relation avec une assistance technique de proximité. - Développement de structures et partenariats : création d'un CSIRT (computer security incident response team), responsable national de la lutte contre les malwares. Par ailleurs, dans le cadre de ses activités de sensibilisation, l'ANSSI a publié en janvier 2017, en coordination avec la CGPME, un « Guide des bonnes pratiques de l'informatique » à destination des PME. Ce guide détaille 12 règles essentielles à la sécurisation des équipements numériques d'une PME, indique les organisations à contacter pour obtenir plus d'information ainsi que les réactions à adopter en cas d'incident.

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 cyber-menaces 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).		**Ministère de l'Intérieur et du Ministère de la Justice :** Renforcement progressif du dialogue entre la mission de prévention et de lutte contre la cybercriminalité du Ministère de la Justice et les acteurs publics *(ANSSI, CNIL, HADOPI…).* **ANSSI** Comme indiqué lors de l'évaluation, l'ANSSI informe et encourage systématiquement les victimes de leur faculté à saisir l'autorité judiciaire. En tant que de besoin, les victimes bénéficient de conseils et sont orientées vers les services compétents si elles décident de judiciariser leur dossier. Cette mission d'information est facilitée par la présence au sein de l'ANSSI d'un officier de police judiciaire détaché par le ministère de l'intérieur qui est également chargé de favoriser le partage d'informations et la coopération au niveau opérationnel entre le centre opérationnel de l'ANSSI et les services compétents du ministère de l'intérieur. Depuis la réalisation de l'évaluation, un magistrat a également rejoint le cabinet du directeur général de l'ANSSI. Ce magistrat est en lien avec ses homologues dans le cadre d'actions de sensibilisation à destination de magistrats judiciaires et apporte une expertise juridique sur les sujets opérationnels.

		Enfin, une dérogation explicite à l'article 40 du code de procédure pénale a été introduite à l'article 47 de la loi n° 2016-1321 du 7 octobre 2016 pour une République numérique. Désormais l'article L. 2321-4 du code de la défense précise que « pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données. L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

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.		**Projets qui seront mis en œuvre prochainement au sein du Ministère de l'Intérieur et du Ministère de la Justice:** • **Thésée (mise en œuvre prévue pour début 2018)** Objectif : Faciliter la plainte en ligne contre les faits d'escroquerie sur internet. • **Perceval (mise en œuvre prévue pour juin 2017)** Objectif : Permettre aux particuliers de signaler les usages frauduleux de cartes bancaires et à la Gendarmerie d'analyser les signalements faits par cette voie. Dans les deux cas, ces systèmes ont pour vocation de faciliter le traitement et l'élucidation d'affaires relatives à ces infractions, et bénéficient tant aux services de Police qu'à la Gendarmerie. Ici, l'avancée est notable dans la mesure où elle met en œuvre un véritable dispositif de plainte en ligne en matière de cyber criminalité, allant encore plus loin que le mécanisme déjà satisfaisant de la pré-plainte en ligne (utilisable en matière d'atteintes aux biens). Cette bonification d'un système préexistant permet, au-delà de la visibilité statistique du phénomène, d'optimiser le traitement de ces infractions en les recoupant en vue d'éviter les actes d'investigation redondants.

		À noter : ces systèmes, une fois opérationnels, permettront de recenser et recouper les affaires potentiellement connexes en centralisant l'information (contentieux, plaintes). Par ailleurs, ils faciliteront la remontée d'affaires relative à des infractions de cyber escroquerie. Perspectives : - Échanges de données et de signalements avec les acteurs économiques pour enrichir la base de données. - Réfléchir sur l'amélioration de l'information des autorités judiciaires en cas de cyberattaques rapportées à l'ANSSI. En ce sens, des contacts sur les questions de chiffrement ont été initiées entre la DACG et l'ANSSI.

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.	**S'agissant du Ministère de la Justice :** - Adoption d'un régime juridique en matière de captation de données informatiques sur la base de l'article 706-102-1 du code de procédure pénale. - Création d'une section intitulée «Des interceptions de correspondances émises par la voie des communications électroniques et du recueil des données techniques de connexion» dans le Code de Procédure Pénale, par la loi n°2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale.	**Au sein du Ministère de l'Intérieur, sur un plan pratique, différentes démarches ont été initiées :** - Constitution d'un groupe de contact permanent animé par la DMISC, à destination des opérateurs étrangers avec l'objectif de faire face à leur absence d'obligation de réponse ou à leur réactivité inégale. 9 réunions sont à dénombrer. Il est compoté d'acteurs américains de l'internet (Apple, Facebook, Google, Microsoft et Twitter), et des services concernés du Ministère de la Justice et du Ministère de l'Intérieur. Bilan : mise en place de demandes harmonisées à destination de ces opérateurs afin d'obtenir de meilleures réponses dans les enquêtes et définition de modèles harmonisés. Ces avancées significatives ont permis d'obtenir des réponses satisfaisantes dans des délais acceptables dans un grand nombre de cas. - Participations aux travaux relatifs à la mise en œuvre des procédures spéciales d'enquête (captation des données dans un cadre judiciaire, par exemple) par la DMISC et les autres services concernés du Ministère de l'Intérieur. - Mise en place d'une formation sur les aspects juridiques de l'infiltration et de l'enquête sous pseudonyme. - Mise en place d'un module de formation continue relatif au recueil de la preuve numérique à l'attention des officiers de police judiciaire par l'ENM. - À noter : il s'agit de thèmes chronophages comparativement à la cybercriminalité (concernent une grande majorité des enquêtes pénales). Ainsi, la forte actualité sur la question n'a pas permis de remplir l'intégralité des objectifs assignés.

	Désormais, ce dispositif n’est utilisable que dans le cadre d'une enquête portant sur des infractions définies et par les agents de services figurant sur une liste précise. À noter : L'« IMSI-catcher » ne peut être mis en œuvre pour une finalité autre que celles de la recherche et de la constatation des infractions pour lesquelles il a été autorisé. Les règles procédurales entourant de tels dispositifs est strictement encadré par le code de procédure pénale. Enfin, un suivi attentif est tout particulièrement accordé aux travaux européens en cours sur l’e-evidence, le chiffrement et sur l’évolution des problématiques de conservation des données de trafic, de contenus et leur localisation.	

	Piste de réflexion : La création d'un régime procédural adapté à la preuve numérique est à l'étude dans le cadre de plusieurs groupes de travail au sein de la direction des affaires criminelles et des grâces (DACG). Sur ce point, l'arrêt récent de la Cour de Justice de l'Union européenne TELE2 nécessite une réflexion approfondie. Dans le même ordre d'idées, un suivi attentif est accordé aux travaux européens en cours relatifs à l'e-evidence, au chiffrement, et sur l'évolution des problématiques de conservation des données de trafic, de contenus, ainsi que leur localisation. À noter : De nombreux échanges entre la DACG et le Ministère de l'intérieur ont lieu sur ces problématiques, de même qu'avec l'ANSSI.	

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.		• **DGPN** - Renforcement des structures de la SDLC et du dispositif territorial de lutte contre la cybercriminalité (RH, budget, formation, doctrine d'emploi commune, sécurisation juridique des pratiques). - Renforcement des effectifs de la SDLC, portés à 120. - Implantation de 12 laboratoires d'investigation opérationnelle du numérique (LIONs) dans les structures régionales et dont l'utilisation sera élargie aux services territoriaux de la sécurité publique. À noter : ces nouvelles structures sont dotées d'investigateurs en cybercriminalité et équipées des matériels nécessaires à l'accomplissement de ces missions. Ils sont les relais territoriaux pour le développement des dossiers judiciaires cyber et l'assistance au recueil et à l'exploitation de la preuve numérique en « situation opérationnelle » et en laboratoire. - Renforcement de structures de la SDLC dans l'optique de lutter contre le terrorisme : section de l'internet et plateforme PHAROS, unité de blocage administratif des contenus d'apologie et d'incitation aux actes de terrorismes et de pédopornographie, cellule « droit de la presse » (traite des contenus en ligne discriminatoires, xénophobes, antisémites), création d'une unité en charge d'une veille en sources ouvertes pour l'anticipation des phénomènes majeurs sur internet et l'environnement internet lié à des affaires judiciaires en cours.

		• **DGGN** - Renforcement du budget pour les dotations matérielles pour les unités de terrain (1 million d'euros, avec le soutien du FSI). - Renforcement des capacités d'enquête des groupes cyber des sections de recherche JIRS et de certaines unités (outre-mer, offices centraux…). À noter : montée en puissance des cellules d'identification criminelle et numériques au niveau départemental. - Amélioration de l'équipement du centre de lutte contre les criminalités numériques (C3N) par un investissement de plusieurs centaines de milliers d'euros en logiciels lourds innovants destinés à suivre les activités sur les réseaux sociaux, le darkweb, et les flux de bitcoins. - 1er octobre 2016 : transformation des « cellules d'identification criminelle » en « cellules d'identification criminelle et numérique » au niveau départemental.

		À noter : les capacités criminalistiques départementales sont regroupées au sein d'une même structure dans l'optique de préparer la future accréditation des plateaux techniques NTECH conformément aux standards européens. En outre, ce regroupement est en phase avec la logique de dissociation de la chaîne criminalistique numérique de celle de l'investigation criminelle, issue de l'optimisation du dispositif de lutte contre la cybercriminalité engagé en juillet 2014. Objectif : favoriser le contrôle des actes techniques ainsi que l'engagement de la démarche d'assurance qualité. - Formation de 20 nouveaux NTECH (investigateurs de haut niveau) chaque année. - Allongement de la formation C-NTECH et rénovation de la mallette pédagogique au niveau des enquêteurs de brigade territoriale. Mise en place de référents cyber de proximité capables de traiter des plaintes simples et de prendre les premières mesures de sauvegarde des supports et des données. - Définition du nouveau parcours « enquêteur sur internet ». Il reprend 3 modules de formation préexistants. Objectif : mettre à la disposition des commandants territoriaux de nouveaux enquêteurs cyber sans avoir recours à la formation NTECH, technique, longue et centrée sur les opérations de criminalistique numérique. - Sensibilisation sur la matière cyber des élèves-gendarmes, par la voie de la formation à distance avec objectif d'une formation en présentiel à terme.

		• **Direction de la coopération internationale** - Spécialisation accrue en 2014, au moyen d'un officier référent pour assurer une interface dédiée au traitement international des dossiers cyber suivis par cette direction. - Développement d'une action spécifique concernant la formation spécifique des personnels de police et de gendarmerie en poste à l'étranger. À noter : le réseau DCI compte 290 personnels déployés dans 74 représentations. Une large partie de ces représentants a vocation à intervenir en soutien aux acteurs opérationnels du Ministère de l'Intérieur, notamment sur la problématique cyber (relais de commissions rogatoires internationales, assistance aux coopérations techniques, signalement d'événements cyber, information sur les phénomènes, contacts avec les services locaux). - Sensibilisation des personnels par trois approches : Création d'un module cyber lors du stage de préparation à l'expatriation (présentation de 30 minutes sur les enjeux et missions de la direction) ; rappel des grandes tendances et priorités à l'occasion du colloque annuel de direction avec les chefs de poste du réseau DCI ; diffusion de documentations et informations spécialisées à l'occasion du colloque et par courriel. • **DGSI** Doublement des effectifs chargés de l'analyse et de l'enquête judiciaire. Leur objectif est de mieux lutter contre les phénomènes cybercriminels relevant de sa compétence. Au plan judiciaire, cela se traduit par la prise en charge des enquêtes relatives aux attaques sur les administrations et les opérateurs d'importance vitale.

		• **Préfecture de police** - Création fin 2014 au Cabinet du Préfet de Police d'un chargé de mission dédié aux questions liées à la cybercriminalité pour harmoniser les actions des et pour les services de son ressort. - Élaboration de mesures visant à adapter son dispositif dans le cadre de son plan de modernisation, notamment en terme de recrutement de personnels à moyen terme compte tenu des contingences budgétaires, de formation et des délais de mise en œuvre. - Développement, depuis 2014, d'un logiciel de traitement de big data permettant à la fois la supervision et l'analyse des traces des serveurs de la PP, mais aussi le traitement par les divers services de renseignement et judiciaires de leur data techniques. Mise en œuvre mutualisée en 2016, intéressante et efficace. - Poursuite de formations dispensés par la BEFTI, de niveau inférieur à celle dispensée aux investigateurs en cybercriminalité, tout en participant aux formations "Premier intervenant en cyber criminalité" (PICC) au profit notamment des agents de la Direction de la Sécurité de Proximité et d'Agglomération Parisienne (DSPAP), qui seront dispensées en mars 2017. Objectifs : permettre aux services locaux non spécialisés d'être plus performants en matière d'investigations liées à l'utilisation des nouvelles technologies, tout en constituant un vivier de recrutement pour la BEFTI. Pour information : dans ce contexte, les capacités de la Préfecture de police pourront être maintenues sous condition d'augmentation des possibilités de formation au niveau national ou européen offertes par EUROPOL, CIVIPOL et l'ECTEG et de renforcement du partage de connaissances avec les autres acteurs compétents.

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.		**Travaux en cours au sein du Ministère de l'Intérieur sur le référentiel commun :** **Actuellement, il n'existe aucun référentiel commun de formation.** Cependant, des avancées notables allant dans le sens d'une meilleure interopérabilité des services de Police et de Gendarmerie sont à souligner : • **Police nationale** - Augmentation du plan de formation annuel des ICC par la SDLC, qui a **doublé son nombre de formations annuelles** pour en dispenser 4 qui forment chaque année 80 ICC qualifiés et équipés. - Élargissement du **plan national de formation de la Police nationale en matière de lutte contre la cybercriminalité** avec le soutien de la DRCPN. À cet effet, des formations sont dispensées au moyen de deux modules pour des catégories plus larges d'enquêteurs : ⇨ **Module EIRS**, destiné à former les enquêteurs sur internet et les réseaux sociaux. Fournit un tronc commun de connaissances de bases des techniques d'enquête dans ces milieux. Ce module est développé par la Commission nationale et est suivi par la gendarmerie nationale. ⇨ **Module PICC**, débutant en 2017 et destiné à la formation des « primo-intervenant en cybercriminalité » ayant vocation à être affectés dans les services territoriaux, capables de préserver une scène de crime numérique et prendre en compte les supports informatiques et en effectuer la première lecture grâce à une « boite à outils » adaptée. - Élaboration d'une **doctrine d'emploi** destinée à sécuriser juridiquement les usages des enquêteurs, promouvoir des pratiques uniformisées et préserver une capacité d'adaptation dans un domaine numérique très évolutif caractérisé par une volatilité des données recherchées.

		• **Gendarmerie nationale** - Élaboration du **manuel des opérations NTECH** par le pôle judiciaire, diffusé fin 2015 et mis à disposition du DGPN, de la Préfecture de police et de la DGSI au premier trimestre 2016. - 4 stages de différents niveaux figurent au plan de formation de la Gendarmerie nationale : stage NTECH (investigateurs de haut niveau), stage « enquêteur sur internet », stage correspondant technologie numérique (C-NTECH) et module de sensibilisation cyber pour les élèves-gendarmes.

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.		**S'agissant du Ministère de l'Intérieur :** - En l'absence d'une homogénéisation de ce type de documentation, la DMISC assure une **veille juridique spécialisée**, avec la direction des libertés publiques et des affaires juridiques, une veille juridique spécialisée à l'attention des services du ministère donnant lieu) une **lettre de présentation unifiée de la législation et de la jurisprudence** paraissant régulièrement à l'attention de l'ensemble des services opérationnels. - Police et Gendarmerie assurent **une large diffusion des notes et documents** produits en matière cyber : ⇨ Élaboration par la DGGN d'un **manuel des opérations NTECH** diffusé fin 2015 à l'attention du DGPN, de la Préfecture de police et de la DGSI. ⇨ **Mise en place de l'intranet CyberAIDE par la DGGN** regroupant plus de 8000 fiches pratiques à l'attention de l'ensemble des fonctionnaires de la Préfecture de police et de la Police nationale. ⇨ Diffusion régulière de **guides pratiques** (guide darkweb, guide bitcoin) et **notes d'alertes/analyse** élaborées par le C3N à l'attention du réseau des enquêteurs cyber gendarmerie et des chefs d'unités spécialisées cyber (DCPJ, PP, DGSI, Cyberdouane, etc.). **S'agissant du Ministère de la Justice,** Des fiches techniques inter-bureaux sont également élaborées et diffusées régulièrement. À noter qu'elles touchent davantage la thématique de la preuve numérique que celle du cyber.