Conseil de
l'Union européenne

Bruxelles, le 9 juin 2017
(OR. en)

9986/17

GENVAL 63
CYBER 92

NOTE

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
Objet:	Septième série d'évaluations mutuelles sur la mise en œuvre pratique et le fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci - Projet de rapport final

Conformément à l'article 2 de l'action commune 97/827/JAI du 5 décembre 1997[1], le groupe "Questions générales, y compris l'évaluation" (GENVAL) a décidé le 3 octobre 2013, que la septième série d'évaluations mutuelles devrait être 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 délégations trouveront en annexe le projet de rapport final sur la septième série d'évaluations mutuelles. Le présent document comprend les conclusions et les recommandations contenues dans les rapports par pays qui ont déjà été préparés.

[1] Action commune 97/827/JAI du 5 décembre 1997 adoptée par le Conseil sur la base de l'article K.3 du traité sur l'Union européenne instaurant un mécanisme d'évaluation de l'application et de la mise en œuvre au plan national des engagements internationaux en matière de lutte contre la criminalité organisée (JO L 344 du 15.12.1997).

Le projet de rapport final, préparé par le Secrétariat général du Conseil, sera présenté au groupe GENVAL lors de sa réunion du 13 juin 2017, en vue d'un premier échange de vues.

Les délégations seront invitées à soumettre par écrit des observations sur le projet de rapport final au Secrétariat général du Conseil (secretariat.mutual-evaluation@consilium.europa.eu et giovanna.giglio@consilium.europa.eu) **au plus tard le 3 juillet 2017**.

La version finale du rapport sera présentée au Coreper et au Conseil pour les informer du résultat de l'évaluation. Il est rappelé que, conformément à la procédure prévue à l'article 8, paragraphe 3, de l'action commune 97/827/JAI, le Conseil peut, lorsqu'il l'estime nécessaire, adresser toute recommandation à l'État membre concerné et inviter celui-ci à lui faire part des progrès accomplis dans les délais qu'il fixe.

Conformément à l'article 8, paragraphe 4, de l'action commune précitée, le rapport final devrait également être transmis au Parlement européen pour information.

ANNEXE

Rapport final sur la septième série d'évaluations mutuelles sur la mise en œuvre pratique et le fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci

TABLE DES MATIÈRES

I- INTRODUCTION

À la suite de l'adoption de l'action commune 97/827/JAI du 5 décembre 1997 instaurant un mécanisme d'évaluation de l'application et de la mise en œuvre au plan national des engagements internationaux en matière de lutte contre la criminalité organisée, le présent rapport s'efforce de résumer les résultats et les recommandations et de tirer des conclusions concernant la septième série d'évaluations mutuelles.

Conformément à l'article 2 de l'action commune précitée, le groupe "Questions générales, y compris l'évaluation" (GENVAL) a décidé le 3 octobre 2013, que la septième série d'évaluations mutuelles devrait être 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 contre des mineurs en ligne et la pédopornographie sur internet, et la fraude en ligne aux cartes de paiement, et devrait comporter 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 2011/92/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) sont particulièrement pertinentes dans ce contexte.

[2] JO L 335 du 17.12.2011, p. 1.
[3] JO L 218 du 14.8.2013, p. 8.

Le questionnaire relatif à la septième série d'évaluations mutuelles a été examiné par le groupe GENVAL le 27 novembre 2013 et le 22 janvier 2014, et a ensuite été adopté par procédure de silence le 31 janvier 2014. L'ordre des visites, sous réserve de certaines modifications, et la composition des équipes d'évaluation en ce qui concerne les observateurs ont été approuvés par le groupe GENVAL le 1er avril 2014.

Conformément à l'article 3 de l'action commune 97/827/JAI, des experts possédant des connaissances pratiques approfondies dans le domaine concerné ont été désignés par les États membres, en réponse à une demande écrite adressée aux délégations par le chef d'unité de la DGD 2B du Secrétariat général du Conseil le 28 janvier 2014. Pour chaque mission, trois experts nationaux ont participé à l'évaluation. D'autres experts de la Commission, d'Eurojust, d'Europol et de l'ENISA ont participé à certaines missions d'évaluation en tant qu'observateurs. Le Secrétariat général du Conseil a coordonné les missions avec un ou deux membres du personnel pour chaque évaluation et y a participé, a préparé le processus et a assisté les experts.

La première mission d'évaluation a été menée en France entre le 28 et le 31 octobre 2014.
La dernière mission d'évaluation a eu lieu en Suède entre le 27 et le 30 septembre 2016.
Les 28 missions d'évaluation ont toutes donné lieu à des rapports détaillés sur les États membres concernés. Ces rapports d'évaluation ont ensuite été examinés et adoptés par le groupe GENVAL[4].
La plupart d'entre eux sont disponibles sur le site internet du Conseil et accessibles au public.

[4] France (7588/2/15 REV 1 DCL 1); Pays-Bas (7587/15 DCL 1); Royaume-Uni (10952/2/15 REV 2 DCL 1); Roumanie (13022/1/15 REV 1 DCL 1); Slovaquie (9761/1/15 REV 1 DCL 1). Estonie (10953/15 DCL 1); Slovénie (14586/1/16 REV 1 DCL 1); Italie (9955/1/16 REV 1 DCL 1); Espagne (6289/1/16 REV 1 DCL 1); Bulgarie (5156/1/16 REV 1 DCL 1); Lituanie (6520/1/16 REV 1 DCL 1); Malte (7696/1/16 REV 1 DCL 1); Grèce (14584/1/16 REV 1 DCL 1); Croatie (5250/1/17 REV 1 DCL 1); Portugal (10905/1/16 REV 1 DCL 1); Chypre (9892/1/16 REV 1 DCL 1); Pologne (14585/1/16 REV 1 DCL 1); République tchèque (13203/1/16 REV 1 DCL 1); Hongrie (14583/1/16 REV 1 DCL 1); Lettonie (5387/1/17 REV 1 DCL 1); Danemark (13204/1/16 REV 1 DCL 1 + COR 1); Belgique (8212/1/17 REV 1); Autriche (8185/1/17 REV 1); Allemagne (7159/1/17 REV 1 DCL 1); Luxembourg (7162/1/17 REV 1 DCL 1); Irlande (7160/1/17 REV 1 DCL 1); Finlande (8178/17); Suède (8188/17 REV 1).

Le présent document rend compte des conclusions et des recommandations contenues dans les rapports par pays qui ont déjà été préparés[5]. Ces évaluations s'étendant toutefois sur le long terme, il y a lieu de noter que les rapports par pays ne correspondent pas toujours à la situation actuelle.

[5] Les rapports par pays ont été produits juste après la visite effectuée dans les États membres. Des changements, par exemple l'achèvement de la mise en œuvre de la législation, pourraient être intervenus par la suite, dont les rapports par pays ne tiennent pas compte. Le suivi des rapports d'évaluation, prévu dix-huit mois après l'adoption, devrait tenir compte des modifications apportées. Au moment de l'examen du rapport par le groupe GENVAL, les États membres ont souvent annoncé des changements (à venir) en vue de donner suite aux recommandations formulées dans le rapport les concernant individuellement.

RÉSUMÉ

- Du fait de l'utilisation plus fréquente de l'internet, la cybercriminalité est un phénomène criminel de plus en plus répandu et de nouvelles tendances, de nouveaux modus operandi et de nouvelles formes de criminalité apparaissent; il s'agit tant d'infractions liées au cyberespace, dont la définition légale met en évidence la dimension cybercriminelle, que d'infractions facilitées par le cyberespace, qui sont des infractions de droit commun commises au moyen des technologies de l'information. Par conséquent, la progression dans la lutte contre la cybercriminalité requiert dans tous les pays un niveau élevé de volonté politique, des efforts budgétaires et un investissement majeur dans les ressources humaines et techniques.

- Il ressort de l'évaluation que tous les États membres prennent la lutte contre la cybercriminalité au sérieux et ont mis en place des structures, des ressources et des mesures à cet effet. Cependant, le degré d'engagement et d'efficacité varie selon les États membres et, dans certains cas, des améliorations seraient possibles en ce qui concerne certains aspects de l'approche globale en matière de lutte contre la cybercriminalité. Dans le même temps, certains problèmes et défis communs ont été identifiés dans la septième série d'évaluations et peuvent être résumés comme suit.

- Au moment de l'évaluation, la majorité des États membres avaient adopté une stratégie nationale de cybersécurité, fournissant un cadre pour l'établissement des priorités nationales ainsi que des structures de coordination essentielles aux niveaux stratégique et opérationnel, afin de lutter contre la cybercriminalité et d'assurer la cyber-résilience, tandis qu'un petit nombre d'États membres étaient en train de le faire. Certains États membres avaient également adopté un plan d'action pour la mise en œuvre de la stratégie nationale de cybersécurité.

- Au moment de l'évaluation, la plupart des États membres avaient signé et ratifié la Convention sur la cybercriminalité du Conseil de l'Europe de 2001 (Convention de Budapest) et son protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques. Les États membres qui ne l'ont pas encore fait ont été invités à signer et à ratifier ces instruments.

- L'une des principales lacunes recensées concerne la collecte de statistiques distinctes sur la cybercriminalité et la cybersécurité, celles qui sont disponibles étant insuffisantes, fragmentées et non comparables dans la plupart des États membres. Des statistiques fiables sont nécessaires pour disposer d'une vue d'ensemble de la cybercriminalité, surveiller et analyser ses tendances et ses évolutions, en vue de prendre des mesures appropriées et d'évaluer l'efficacité du système judiciaire dans la lutte contre cette forme de criminalité. Il a par conséquent été recommandé aux États membres de recueillir des statistiques spécifiques et complètes pour la cybercriminalité aux différents stades de la procédure sur la base d'une approche normalisée.

- En raison de l'évolution rapide des technologies de l'information grâce à des méthodes de plus en plus sophistiquées et de la complexité de la cybercriminalité, un degré élevé de spécialisation des professionnels travaillant dans ce domaine est extrêmement important. Selon les conclusions de l'évaluation, le degré de spécialisation est généralement suffisant ou satisfaisant pour les services répressifs, tandis qu'il laisse à désirer en ce qui concerne le système judiciaire, étant donné que, dans plusieurs États membres, la cybercriminalité est traitée par les parquets généraux et les juridictions pénales. Il a par conséquent été recommandé aux États membres d'accroître le niveau de spécialisation de leur personnel judiciaire traitant des affaires de cybercriminalité.

- Pour les mêmes raisons, l'évaluation a mis en évidence l'importance d'assurer de façon régulière et continue des formations spécialisées sur la cybercriminalité qui s'adressent à la fois aux services répressifs et aux autorités judiciaires, y compris en tirant le meilleur parti des possibilités de formation offertes par les organes de l'UE, tels que l'EC3/Europol, l'ECTEG, Eurojust, l'OLAF et le CEPOL.

- L'évaluation a souligné qu'une coordination et une coopération interinstitutionnelles étroites et efficaces, fondées sur une approche faisant intervenir plusieurs organismes aux niveaux stratégique et opérationnel, entre toutes les parties prenantes concernées des secteurs public et privé associées à la cybercriminalité et à la cybersécurité, constituent des éléments essentiels pour lutter efficacement contre la cybercriminalité et veiller à ce que le système national de cybersécurité présente un bon niveau de résilience face aux menaces informatiques. Dans certains États membres, une telle coopération n'a cependant pas encore été suffisamment développée ou peut être encore améliorée.

- À cette fin, les États membres ont également été encouragés à envisager la mise en place éventuelle d'une entité ou d'un organe central au sein duquel le secteur public et le secteur privé sont tous deux représentés, afin de coordonner les activités dans ce domaine.

- Une étroite coopération entre le secteur public et le secteur privé - les institutions financières/bancaires, les entreprises de télécommunications, les fournisseurs de service internet (FSI), les ONG, le monde universitaire, les entreprises, les associations professionnelles, etc. - est fondamentale dans ce contexte, étant donné que leur expertise apporte une grande valeur ajoutée à la réussite des enquêtes et des actions menées pour résoudre les cyberincidents. Les formes les plus avancées de coopération avec le secteur privé sont institutionnalisées par la création d'institutions/de groupes de travail appropriés. Les partenariats public-privé ont été identifiés par les évaluateurs comme étant un outil important pour une bonne coopération entre les services répressifs et le secteur privé.

- Certains États membres ont des contacts directs avec les FSI situés à l'étranger, en particulier aux États-Unis, mais la coopération avec ces entreprises est assez problématique parce qu'elles ne répondent pas à chaque demande ou exigent une entraide judiciaire/des commissions rogatoires ou un mandat délivré par un tribunal pour fournir les informations demandées; par conséquent, l'évaluation a mis en évidence que l'UE et ses États membres devraient réfléchir à la manière d'améliorer cette coopération.

- L'utilisation croissante du chiffrement à l'aide de techniques de plus en plus sophistiquées pose de plus en plus de problèmes dans l'ensemble des États membres car elle complique ou empêche totalement l'accès à des informations pertinentes concernant la criminalité en ligne ou la cybercriminalité. Le déchiffrement n'est possible qu'en utilisant du matériel et des logiciels spécialisés à fortes capacités et l'évaluation a montré que la lutte contre le chiffrement, en particulier dans les cas les plus complexes, ne rencontre qu'un succès limité. De nombreux États membres utilisent la plateforme de déchiffrement d'Europol, le Centre européen de lutte contre la cybercriminalité (EC3). Selon les conclusions de l'évaluation, les problèmes posés par le chiffrement pourraient être partiellement compensés par l'intensification de la recherche et du développement et l'élaboration de nouvelles méthodes, ainsi que par une bonne coopération entre les différentes autorités concernées. Il a également été recommandé aux États membres et aux institutions de l'UE d'envisager l'élaboration d'une injonction de déchiffrement.

- La nature des preuves électroniques et la facilité avec laquelle elles peuvent être manipulées ou falsifiées peuvent créer des problèmes en ce qui concerne l'admissibilité qui ne se posent pas avec d'autres types de preuves. Pour cette raison, il existe dans certains États membres des exigences spécifiques en ce qui concerne la collecte des preuves électroniques pour qu'elles soient admissibles devant les tribunaux. Cependant, il ressort de l'évaluation que, dans la plupart des États membres, le droit procédural est principalement neutre sur le plan technologique, ce qui signifie que les règles et les principes généraux relatifs au recueil des preuves sont appliqués et que le système procédural ne contient pas de règles de forme spécifiques concernant l'admissibilité et l'évaluation des preuves électroniques.

- Dans certains États membres, la législation nationale permet d'obtenir des informations concernant les abonnés directement auprès de fournisseurs étrangers, tandis que dans d'autres États membres il est nécessaire de suivre les procédures d'entraide judiciaire, qui devraient être plus rapides et plus efficaces. Les États membres ont été invités à veiller à ce que leur législation nationale soit suffisamment souple pour faciliter l'admissibilité des preuves électroniques, y compris lorsqu'elles sont obtenues d'un autre pays.

- L'évaluation a mis en évidence que les actes de cybercriminalité commis dans le "nuage" soulèvent généralement des problèmes pour les enquêtes et les poursuites, étant donné que les informations dans le "nuage" ne sont pas facilement localisables par les services répressifs ni facilement accessibles pour ceux-ci. Selon le type d'acte de cybercriminalité, l'effet peut être ressenti par les juridictions de plusieurs États, y compris à l'extérieur de l'UE. Des conflits de compétence peuvent donc survenir lorsque l'aide d'Eurojust et du réseau judiciaire européen (RJE) peut être sollicitée. L'évaluation a souligné l'importance de relever ces défis au niveau de l'UE.

- L'évaluation a confirmé les préoccupations des États membres concernant l'absence d'un cadre juridique commun sur la conservation des données au niveau de l'UE. Cela a une incidence sur l'efficacité des enquêtes et des poursuites pénales, en particulier en termes de fiabilité et d'admissibilité des preuves devant les tribunaux, fondées sur la collecte de données de communications électroniques, ainsi que sur la coopération judiciaire transfrontière. Un processus de réflexion commune associant les institutions et les États membres de l'UE est en cours pour traiter la question de la conservation des données en vue de trouver des solutions juridiques et pratiques aux problèmes découlant de la jurisprudence de la Cour de justice.

- Les abus sexuels commis contre des enfants sur internet, sous différentes formes, ont considérablement augmenté ces dernières années. Afin de lutter efficacement contre de telles formes de criminalité, un large éventail de mesures tant préventives (notamment des formations et des campagnes d'information à des fins de sensibilisation) que coercitives (blocage d'accès ou suppression des contenus illicites) associant à la fois le secteur public et le secteur privé est mis en œuvre, à des degrés divers, dans les États membres. Il ressort de l'évaluation que seuls quelques États membres disposent d'une base de données nationale consacrée à l'identification des victimes pour lutter contre les abus sexuels à l'encontre des enfants; il a été recommandé aux autres États membres qui utilisent uniquement la base de données internationale sur l'exploitation sexuelle des enfants d'Interpol de mettre en place une telle base de données nationale. Plusieurs États membres ont pris des mesures pour empêcher une nouvelle victimisation, y compris dans certains cas pour protéger les victimes et les témoins d'abus sexuels commis contre des enfants pendant les procédures pénales. Une bonne coopération entre toutes les parties prenantes concernées, à savoir les services répressifs, les lignes directes, les ONG et les FSI, est considérée comme un élément essentiel pour lutter contre ces formes de criminalité.

- En ce qui concerne la cybersécurité, les centres nationaux de réponse aux urgences informatiques (CERT), déjà mis en place par la majorité des États membres, jouent un rôle fondamental pour surveiller les cyberincidents et y répondre. En outre, il a été recommandé aux États membres d'introduire dans leur droit national l'obligation pour le secteur privé de notifier sans délai aux services répressifs les cyberattaques qui ont une incidence significative sur la continuité des services essentiels. Les deux aspects sont prévus par la directive SRI et devront être mis en œuvre d'ici le 9 mai 2018.

- Étant donné que la cybercriminalité, d'autres crimes liés au cyberespace et les enquêtes sur ceux-ci concernent souvent plusieurs États membres, la coopération et l'échange d'informations avec les agences de l'UE, telles que Europol/EC3, Eurojust, le RJE et l'ENISA, sont prioritaires. Pour la même raison, il a été recommandé de recourir davantage aux équipes communes d'enquête (ECE), qui constituent un instrument efficace pour mener des enquêtes transfrontières.

- Internet n'ayant pas de frontières, une coopération internationale harmonieuse et efficace est essentielle pour lutter efficacement contre la cybercriminalité. Toutefois, comme l'évaluation l'a mis en évidence, les procédures d'entraide judiciaire sont au contraire lentes, inefficaces et prennent du temps, ce qui a une incidence négative sur les enquêtes, étant donné que les preuves numériques sont volatiles et doivent être traitées rapidement. Par conséquent, il est nécessaire d'accélérer le traitement des demandes d'entraide judiciaire pour des enquêtes en matière de cybercriminalité. En outre, les États membres ont notamment été encouragés à utiliser plus fréquemment les outils d'Eurojust, du RJE et d'Europol et de développer des contacts informels avec les autorités étrangères compétentes afin d'obtenir plus rapidement des réponses aux demandes d'entraide judiciaire.

III - STRATÉGIE NATIONALE DE CYBERSÉCURITÉ

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- L'ENISA a mis au point un guide pratique sur l'élaboration et l'exécution de stratégies nationales de cybersécurité en 2012. Selon ses conclusions, une stratégie nationale de cybersécurité est un outil visant à améliorer la sécurité et la résilience des infrastructures et des services nationaux.

- En général, l'objectif d'une stratégie nationale de cybersécurité est de fournir un cadre pour établir les priorités nationales ainsi que les structures de coordination essentielles aux niveaux stratégique et opérationnel, afin de lutter contre la cybercriminalité et d'assurer la cyber-résilience.

- Une stratégie nationale de cybersécurité globale devrait être ciblée et comprendre des objectifs spécifiques et mesurables ainsi qu'une délimitation claire des responsabilités, de façon à assurer la coordination des rôles des différentes parties prenantes et de fournir une estimation des coûts pour les actions pertinentes à entreprendre.

- Au moment de l'évaluation, la majorité des États membres avaient adopté une stratégie nationale de cybersécurité, certains d'entre eux ayant également adopté un plan d'action pour sa mise en œuvre, tandis que quelques États membres étaient en train de le faire.

- À la suite de l'élaboration d'une stratégie nationale de cybersécurité et, le cas échéant, d'un plan d'action, il est essentiel d'assurer un suivi approprié et de surveiller de près la mise en œuvre de la stratégie nationale.

- En raison du développement rapide tant des technologies de l'information que de nouveaux types d'infractions liées au cyberespace, il est également nécessaire d'actualiser constamment les mesures et les moyens mis en place pour lutter efficacement contre la cybercriminalité, et dès lors pour garantir, le cas échéant, l'évaluation en temps utile de la stratégie nationale de cybersécurité.

- La mise en place d'un organe unique doté de fonctions de coordination pour la mise en œuvre de la stratégie nationale de cybersécurité, comme cela est le cas dans certains États membres, peut être considérée comme une bonne pratique qui devrait être suivie par d'autres États membres.

- L'adoption d'une stratégie nationale en matière de sécurité des réseaux et des systèmes d'information est prévue dans la directive 2016/1148 (directive SRI) récemment adoptée afin de définir les objectifs stratégiques et les mesures politiques et réglementaires appropriées en vue de parvenir à un niveau élevé de sécurité des réseaux et des systèmes d'information et de le maintenir (article 7).

RECOMMANDATIONS

- ***Les États membres qui n'ont pas encore adopté une stratégie nationale de cybersécurité sont encouragés à le faire dans les meilleurs délais et à envisager également l'adoption d'un plan d'action; ceux qui en ont adopté une devraient assurer sa bonne mise en œuvre et l'attribution éventuelle à un organe/une entité unique doté(e) de fonctions de coordination à cette fin.***

- ***Les États membres devraient mettre à jour leur stratégie nationale de cybersécurité lorsque cela est nécessaire, dans le droit fil des évolutions pertinentes des technologies de l'information ainsi que des tendances dans le domaine de la cybercriminalité.***

IV - CONVENTION DE BUDAPEST

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- La Convention de 2001 sur la cybercriminalité du Conseil de l'Europe (Convention de Budapest) est le premier traité international sur les crimes commis par l'intermédiaire de l'internet et d'autres réseaux informatiques, traitant spécifiquement des atteintes à la propriété intellectuelle, de la fraude informatique, de la pornographie enfantine, des crimes de haine et des violations de la sécurité des réseaux. Elle prévoit également une série de pouvoirs et de procédures, telles que la perquisition de réseaux informatiques et l'interception légale.

- Son principal objectif, énoncé dans le préambule, est de mener une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, en particulier par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale.

- Les articles 16, 17, 29 et 30 de la Convention, en particulier, régissent la conservation rapide de données informatiques stockées et de données relatives au trafic et la divulgation de données relatives au trafic, tandis que l'article 35 établit le réseau international d'urgence 24/7, qui permet le gel des données, facilitant ainsi la conservation des preuves numériques. Ce réseau est un instrument important car il crée une possibilité de conservation rapide des données numériques avant l'envoi d'une demande d'entraide judiciaire.

- La Convention de Budapest s'accompagne d'un protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques, et de la Convention de Lanzarote pour ce qui a trait à la protection des enfants contre l'exploitation et les abus sexuels.
- Au moment de l'évaluation, la plupart des États membres avaient signé et ratifié ces instruments, tandis que quelques États membres ne l'avaient pas encore fait. Dans ses conclusions sur l'amélioration de la justice pénale dans le cyberespace du 9 juin 2016, le Conseil a demandé une nouvelle fois aux États membres de ratifier et d'appliquer intégralement la convention sur la cybercriminalité du 23 novembre 2001.

RECOMMANDATIONS

- ***Les États membres qui ne l'ont pas encore fait sont invités à signer et à ratifier la Convention de 2001 sur la cybercriminalité du Conseil de l'Europe (Convention de Budapest) et son protocole additionnel et à mettre pleinement en œuvre ces instruments.***

V- STATISTIQUES

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- L'analyse de la législation de l'UE met en évidence la réelle nécessité de collecter des statistiques dans le domaine de la cybercriminalité. Aux termes de l'article 14, paragraphe 1, de la directive 2013/40/UE relative aux attaques contre les systèmes d'information, les États membres veillent à mettre en place un système d'enregistrement, de production et de communication de statistiques sur les infractions visées aux articles 3 à 7.

- L'article 14, paragraphe 2, de la même directive dispose que les statistiques visées au paragraphe 1 portent, au minimum, sur les données existantes concernant le nombre d'infractions visées aux articles 3 à 7 enregistrées par les États membres, ainsi que le nombre de personnes poursuivies et condamnées pour les infractions visées aux articles 3 à 7.

- En outre, conformément au considérant 44 de la directive 2011/93/UE relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie, les États membres sont encouragés à mettre en place des mécanismes de collecte de données ou des points d'information, au niveau national ou local et en coopération avec la société civile, permettant l'observation et l'évaluation des phénomènes d'abus sexuels et d'exploitation sexuelle des enfants.

- Par ailleurs, la nécessité de collecter des statistiques au niveau national découle en principe pour les États membres de leur législation ou réglementation nationale.

- Les statistiques sur la cybercriminalité sont extrêmement importantes. D'une part, elles rendent possibles une analyse détaillée et une compréhension de l'ampleur des nouvelles tendances émergentes de cette forme de criminalité en expansion, permettant ainsi d'avoir une vue d'ensemble de ses évolutions et de suivre celles-ci, afin de prendre des mesures appropriées; d'autre part, elles permettent d'évaluer l'efficacité du système juridique et l'adéquation de la législation aux fins de la lutte contre la cybercriminalité et de la protection des intérêts privés des citoyens qui en sont les victimes.

- De surcroît, la collecte de données statistiques facilite le travail des institutions (la Commission) et des agences (Europol, Eurojust ou ENISA) de l'UE concernées par la lutte contre la cybercriminalité. Ces données permettent d'avoir une vision plus complète du problème de la cybercriminalité et de la sécurité des réseaux et des informations au niveau de l'UE, contribuant ainsi à l'élaboration d'une réponse plus efficace.

- Les statistiques sont également importantes pour disposer d'une image réaliste du taux de cybercriminalité, compte tenu du faible taux de signalement aux autorités répressives des infractions liées à celle-ci, y compris les infractions graves, par les victimes, qu'il s'agisse de personnes physiques, de banques ou de sociétés.

- Des statistiques complètes devraient porter sur tous les domaines jugés importants pour ce type de criminalité à tous les stades de la procédure: enquête, poursuites, procès, infraction pénale spécifique et mesure d'enquête spécifique, nombre d'infractions signalées, nombre d'enquêtes menées et décisions de ne pas mener d'enquête sur un certain type de cybercriminalité, nombre de victimes et de plaintes déposées par des victimes, nombre de personnes poursuivies et condamnées pour différentes formes de cybercriminalité, nombre d'affaires transfrontières, résultats des demandes d'entraide judiciaire et durée de la procédure.

- Cependant, l'une des principales lacunes recensées dans la majorité des États membres lors de la septième série d'évaluations concerne la collecte de statistiques distinctes sur la cybercriminalité, la criminalité en ligne (les infractions ordinaires facilitées par l'utilisation des technologies de l'information et de la communication) et les incidents de cybersécurité. Les statistiques disponibles sont insuffisantes, fragmentées et non comparables dans la plupart des États membres.

- En outre, beaucoup d'États membres ne disposent pas d'une définition nationale commune de la cybercriminalité ou de la criminalité en ligne à des fins statistiques. Dans de nombreux États membres, il n'est pas possible de déterminer la part que représente la cybercriminalité par rapport à l'ensemble de la criminalité, tandis que d'autres qui collectent des statistiques sur la cybercriminalité les produisent sous la forme d'un chiffre unique; il n'est donc pas possible de les diviser en catégories ni d'établir une distinction entre les affaires qui concernent des actes de cybercriminalité au sens strict et celles qui concernent des infractions en ligne. Les États membres ne produisent pas tous des rapports statistiques réguliers sur la cybercriminalité.

- Dans la plupart des États membres, les statistiques judiciaires sont séparées des statistiques des services répressifs. Comme les systèmes statistiques varient souvent sensiblement en fonction des autorités compétentes et que chaque autorité collecte des données auprès de diverses sources selon des méthodes différentes et les gère suivant des critères différents et/ou en utilisant des bases de données différentes sans aucune interopérabilité entre elles, la cybercriminalité ne peut pas faire l'objet d'un suivi dans le cadre d'un système statistique unique.

- Dans de nombreux États membres, les chiffres de la cybercriminalité enregistrés dans les différents systèmes sont très faibles, ce qui soulève des questions quant à l'efficacité de la détection des actes de criminalité et des poursuites et sanctions à l'encontre de leurs auteurs et quant à l'exactitude des données statistiques.

- Le partage de statistiques entre autorités répressives et judiciaires pourrait être très précieux pour un mécanisme de suivi ainsi que pour la hiérarchisation des objectifs dans la lutte contre ce phénomène. Il est toutefois fréquent que l'échange de données statistiques entre les différentes autorités nationales engagées dans la lutte contre la cybercriminalité soit inexistant ou insuffisant.

RECOMMANDATIONS

- ***Les États membres confrontés à des problèmes liés à l'absence de définition ou de vision commune de la cybercriminalité sont encouragés à élaborer une définition (ou une vision) nationale cohérente de la cybercriminalité, qui sera utilisée par tous les acteurs intervenant dans la lutte contre la cybercriminalité et aux fins de la compilation de statistiques.***

- ***Les États membres devraient recueillir des statistiques spécifiques sur la cybercriminalité qui permettent à la fois de vérifier les chiffres globaux de la cybercriminalité et de déterminer la part que celle-ci représente dans l'ensemble de la criminalité.***

- ***Les États membres devraient mettre au point une approche normalisée aux fins de la collecte de statistiques complètes aux différents stades de la procédure, ventilées entre les domaines spécifiques de la cybercriminalité, de préférence ceux qui ont été recensés au niveau de l'UE, à savoir les abus sexuels commis contre des enfants via Internet, la fraude en ligne aux cartes de paiement et les cyberattaques.***

- ***Les États membres devraient réfléchir à des solutions permettant l'interopérabilité des différentes bases de données contenant des chiffres relatifs à la cybercriminalité, afin de réaliser rapidement des comparaisons de cas, l'identification des malfaiteurs et la quantification des cas.***

VI - STRUCTURES - LE SYSTÈME JUDICIAIRE

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- La structure et l'organisation du système judiciaire varie selon les États membres, y compris en ce qui concerne l'attribution de la compétence pour traiter les dossiers de cybercriminalité.

- En raison du développement rapide des TIC ainsi que de la complexité et de la sophistication croissante de la cybercriminalité, le succès des enquêtes, des poursuites et des condamnations dans les dossiers de cybercriminalité dépend dans une large mesure du niveau de savoir-faire et d'expérience des autorités chargées des enquêtes. Un bon niveau de compréhension et de connaissance au sein du corps judiciaire et la spécialisation de celui-ci dans ce domaine sont donc de la plus haute importance.

- Cependant, selon les constatations de l'évaluation mutuelle, le degré de spécialisation des procureurs et des juges chargés des questions de cybercriminalité et des infractions qui y sont liées n'est pas toujours satisfaisant.

- Dans un nombre non négligeable d'États membres, la cybercriminalité est traitée par les parquets généraux, et aucun État membre ne possède de juridictions ou de juges spécialisés chargés d'examiner et de juger les affaires de cybercriminalité. En revanche, certains États membres disposent de procureurs ou de structures spécialisés au sein des parquets chargés des infractions liées à cybercriminalité.

- Dans quelques États membres, il existe des parquets/des services dont les compétences portent notamment sur les infractions commises ou ordonnées par des groupes criminels organisés ou sur la criminalité économique et la corruption, y compris les actes de cybercriminalité.

- Selon les pratiques internes d'organisation du pouvoir judiciaire, en fonction des spécialisations des procureurs ou de la concentration des dossiers de cybercriminalité au sein de certains bureaux judiciaires, dans quelques États membres, la responsabilité du traitement de ce type d'infractions incombe de facto à des parquets et à des juges spécialisés, qui ont été formés ou ont une expérience dans le domaine de la cybercriminalité et acquièrent ainsi en pratique un haut degré de spécialisation leur permettant de prêter assistance à leurs collègues.

- Dans certains États membres, il existe des réseaux nationaux de "cyberprocureurs" spécialisés en cybercriminalité, ce qui peut être considéré comme une bonne pratique, car cela permet des échanges de connaissances et d'expériences et favorise la diffusion des bonnes pratiques parmi les praticiens.

- Les évaluateurs avaient recommandé aux États membres de faciliter, avec l'appui d'Eurojust, la création d'un réseau européen de juges se spécialisant dans la lutte contre la cybercriminalité, afin d'améliorer et de faciliter la coopération judiciaire dans ce domaine. Depuis, cet objectif a été réalisé au moyen de l'établissement en juin 2016, sur la base de conclusions du Conseil, du Réseau judiciaire européen en matière de cybercriminalité, qui a déjà commencé à fonctionner.

RECOMMANDATIONS

- ***Les États membres devraient augmenter le niveau de spécialisation de leur corps judiciaire, afin de poursuivre et de sanctionner efficacement les auteurs d'infractions liées au cyberespace et relevant de la criminalité en ligne. Pour ce faire, ils devraient de préférence créer des bureaux ou des structures/unités internes spécialisés et/ou nommer des procureurs et des juges spécialisés possédant un bon niveau de compréhension et de connaissance de la cybercriminalité, pour traiter ces dossiers.***

- ***Les États membres devraient mettre en place des réseaux de procureurs et de juges spécialisés dans la cybercriminalité au niveau national en tant qu'instrument supplémentaire pour améliorer l'efficacité de la lutte contre ce type de criminalité.***

VII - STRUCTURES - LES SERVICES RÉPRESSIFS

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- La structure et l'organisation des services répressifs varient sensiblement selon les États membres, y compris en ce qui concerne l'attribution des compétences en matière de cybercriminalité. Dans certains États membres, des unités spécialisées travaillent sur la base d'une approche en deux volets comprenant la planification stratégique et les activités opérationnelles, alors que dans d'autres, ces fonctions sont exercées séparément par des autorités et des organes différents.

- Une organisation efficiente, l'intégration internationale et les compétences professionnelles des services répressifs intervenant dans les enquêtes sur la cybercriminalité sont des éléments essentiels pour contrer efficacement cette dernière. Un bon niveau de connaissance et de spécialisation des services répressifs, pour les mêmes raisons que celles décrites à propos du corps judiciaire, est également fondamental pour lutter efficacement contre cette forme complexe et sophistiquée de criminalité.

- D'une manière générale, l'évaluation mutuelle a révélé que le degré de spécialisation des services répressifs est plus élevé que celui du corps judiciaire mais que, dans de nombreux cas, il peut être amélioré.

- Dans la plupart des États membres, il existe des structures centralisées spécialisées dans la cybercriminalité au sein du ministère de l'intérieur et/ou de la police, qui sont chargées de prévenir et de combattre la cybercriminalité au niveau national, assurant ainsi la coordination des enquêtes portant sur la cybercriminalité dans tout le pays avec un degré élevé de spécialisation dans ce domaine. Cela facilite également la communication entre la police et les procureurs. Dans plusieurs États membres, il existe aussi des unités spécialisées décentralisées au niveau local ou régional qui s'occupent spécifiquement des enquêtes sur la cybercriminalité.

- Il a été recommandé à certains États membres de procéder à la réorganisation de la police et de prendre des mesures appropriées pour renforcer les ressources humaines, offrir une formation plus efficace et plus intensive aux policiers et prévoir des équipements techniques suffisants pour la lutte contre la cybercriminalité. En outre, il convient de mettre constamment à jour les équipements et les ressources des services répressifs pour faire face à l'évolution et à la diversification incessantes des modes opératoires dans le domaine de la cybercriminalité.

- Les principaux obstacles au succès des enquêtes sur la cybercriminalité sont, entre autres, le développement rapide de la technologie, le professionnalisme et le niveau d'expertise croissants des cyberdélinquants, le fait que la cybercriminalité puisse facilement relever de la compétence de plusieurs pays, la difficulté d'obtenir l'accès aux preuves électroniques en rapport avec la cybercriminalité et les difficultés liées à l'utilisation du chiffrement, du réseau Tor et de l'anonymisation.

- Aucun pays ne dispose actuellement d'un réseau national de policiers spécialisés dans la cybercriminalité.

RECOMMANDATIONS

- ***Les États membres devraient maintenir et, le cas échéant, augmenter le niveau de spécialisation des services répressifs chargés des enquêtes sur la cybercriminalité. Les États membres qui ne l'ont pas encore fait devraient envisager de mettre en place des unités spécialisées au sein des services répressifs pour lutter plus efficacement contre la cybercriminalité également au niveau régional/local.***

- ***Les États membres devraient réfléchir à la création d'un réseau de policiers spécialisés dans la cybercriminalité au niveau national, qui pourrait également aider à maintenir un canal de communication du secteur public et privé vers la police.***

- ***Les États membres devraient envisager de renforcer le personnel policier non technique dans l'ensemble des structures zonales ou régionales et de doter celles-ci d'équipements techniques suffisants pour répondre à leurs besoins.***

VIII - COOPÉRATION ET COORDINATION AU NIVEAU NATIONAL

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- Étant donné que la cybercriminalité a un caractère transversal et que la responsabilité pour la sécurité du cyberespace au niveau national est généralement partagée entre divers acteurs, dont les missions et les capacités diffèrent, qu'ils soient publics ou privés, militaires ou civils, collectifs ou individuels, une approche pluridisciplinaire est un facteur essentiel pour prévenir et combattre efficacement la cybercriminalité et garantir la cyberrésilience.

- Dans ce contexte, afin de coordonner les initiatives et d'améliorer l'échange de données, le soutien technique ainsi que les techniques d'enquête, il est essentiel d'assurer une coordination et une coopération interinstitutionnelles étroites et efficaces entre les différents pouvoirs et organismes publics aux niveaux opérationnel et stratégique, ainsi qu'entre les autorités centrales et locales/régionales.

- Une coopération étroite dans la lutte contre la cybercriminalité n'est pas seulement nécessaire entre la police et le ministère public, mais aussi avec les services nationaux de renseignement, afin de bénéficier d'une aide d'un point de vue technique (interceptions, expertise, etc.) ainsi qu'en ce qui concerne les renseignements utiles aux enquêtes et aux poursuites pénales, notamment pour l'obtention et le traitement numérique des preuves.

- La coopération entre les secteurs public et privé est également essentielle pour mener à bien les enquêtes, poursuites et condamnations dans le domaine de la cybercriminalité et des infractions informatiques, ainsi que pour répondre aux menaces et attaques informatiques (pour plus de détails, voir le chapitre suivant).

- Habituellement, la stratégie nationale en matière de cybersécurité ainsi que le plan d'action pour la mise en œuvre de cette stratégie, s'il existe, en combinaison avec le cadre juridique pour la coopération interagences, fixent le cadre général de la coordination et de la coopération entre l'ensemble des institutions et autorités publiques chargées de la cybersécurité, ainsi qu'avec le secteur privé, le but étant de veiller à délimiter les rôles et les responsabilités de chacun.

- La bonne mise en œuvre de la stratégie nationale en matière de cybersécurité est donc un élément essentiel pour créer des synergies et optimiser la préparation ainsi que les capacités de réaction en vue de lutter contre la cybercriminalité et de renforcer la cybersécurité.

- Selon les résultats des évaluations, les formes, les modalités et les niveaux de la coopération et de la coordination entre les parties prenantes qui luttent contre la cybercriminalité et garantissent la cybersécurité varient d'un État membre à l'autre, certains ayant plus que d'autres développé des formes d'interaction avancées et efficaces, que les différents rapports recensent en tant que bonnes pratiques.

- Le meilleur moyen de garantir le bon fonctionnement du système est un mécanisme structuré, surtout lorsque les fonctions de coordination pour les questions liées à la cybersécurité et aux politiques de lutte contre la cybercriminalité sont confiées à une autorité institutionnelle unique (c'est-à-dire des ministères ou des bureaux faisant partie de la structure organisationnelle des ministères) ou à un organisme ou une entité ad hoc unique. Certains États membres ont déjà établi une telle institution ou un tel organe unique fournissant un cadre institutionnel de coopération au sein duquel sont représentés les acteurs, tant publics que privés, qui luttent contre la cybercriminalité et garantissent la cybersécurité, et, au moment de l'évaluation, d'autres États membres envisageaient de suivre cet exemple.

- Dans quelques États membres, il n'existe pas de cadre juridique pour la coopération interagences dans des affaires liées à la cybercriminalité et les membres des autorités chargées des enquêtes et des poursuites en la matière coopèrent de manière informelle, car ils connaissent leurs homologues au sein des autres autorités et peuvent donc entrer en contact très facilement; ce système fonctionne bien et facilite les contacts et le dialogue sans retards bureaucratiques inutiles.

- Certains États membres dans lesquels des lacunes ont été identifiées dans le cadre de l'évaluation mutuelle s'efforcent de consolider les structures et les procédures existantes de coopération et de coordination en vue de mieux prévenir et combattre la cybercriminalité.

RECOMMANDATIONS

- ***Les États membres devraient accorder la priorité à la coordination et à la coopération institutionnelles entre l'ensemble des acteurs impliqués dans la prévention de la cybercriminalité, dans la lutte contre ce phénomène et dans la cybersécurité, sur la base d'une approche pluridisciplinaire, en vue de créer des synergies ainsi que d'optimiser la préparation et les capacités de réponse.***

- ***En particulier, les États membres sont encouragés à mettre en place ou à renforcer un cadre structuré de coopération et, éventuellement, à établir une entité ou un organe central au sein duquel les acteurs publics et privés concernés par la cybersécurité et la lutte contre la cybercriminalité sont représentés, et qui assume des fonctions de coordination et dispose d'un pouvoir de décision.***

IX - COOPÉRATION ENTRE LES SECTEURS PUBLIC ET PRIVÉ

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- Compte tenu de la complexité de la lutte contre la cybercriminalité, il est essentiel de mettre en place une étroite coopération entre le secteur public et le secteur privé, les services répressifs ne pouvant pas combattre efficacement ce phénomène sans la coopération du secteur privé (établissements financiers/bancaires, compagnies de télécommunication, FSI, ONG, universités, entreprises, associations professionnelles, etc.).

- Une telle coopération pourrait fonctionner à l'avantage des deux secteurs, car elle permettrait d'associer un large éventail d'entités qui travailleraient ensemble et de créer des synergies entre elles, ce qui contribuerait à accroître le niveau de cybersécurité.

- La contribution des acteurs privés, en termes d'expertise, d'assistance technique et d'échange d'informations sur l'évolution des menaces informatiques et de la cybersécurité, présente une forte valeur ajoutée pour le succès des enquêtes engagées et des mesures prises en vue de remédier aux incidents de sécurité informatique. Il est également utile d'associer les procureurs aux contacts avec le secteur privé, afin de garantir que les preuves sont rassemblées dans le respect de la législation en vigueur et sont recevables dans le cadre des procédures judiciaires.

- Selon les conclusions de l'évaluation, le niveau de la coopération entre le secteur public et le secteur privé est variable dans les États membres et, d'une manière générale, la coopération est plus développée et plus efficace lorsqu'elle est plus structurée et qu'il existe un climat de confiance. Dans certains États membres, l'évaluation a permis de recenser de bonnes pratiques, tandis que dans d'autres la nécessité d'améliorer cette coopération a été mise en évidence.

- Certains États membres recourent largement aux partenariats public/privé afin de prévenir et de combattre la cybercriminalité et d'assurer la cybersécurité; dans certains cas, le recours à de tel partenariats est prévu dans la stratégie nationale de cybersécurité, tandis que, dans d'autres, il est limité à certains domaines spécifiques ou pas encore mis en œuvre. Il peut revêtir diverses formes et, notamment, reposer sur des protocoles d'accord ou des accords formels analogues.

- Dans les conclusions de l'évaluation, les évaluateurs ont estimé que les partenariats public/privé étaient des instruments importants pour assurer une bonne coopération entre les services répressifs et le secteur privé, en particulier les fournisseurs de services Internet, ainsi que le secteur financier, notamment les banques, mais aussi les ONG, les CERT et les infrastructures critiques.

- Comme indiqué dans certains rapports individuels, la réglementation du partenariat public/privé au moyen d'un cadre établissant les droits et les règles améliore la circulation et la gestion de l'information, car cela permet de procéder à un traitement informel plutôt que de recourir à des méthodes plus traditionnelles reposant sur un échange officiel de documents à la suite d'une demande formelle présentée par des autorités répressives.

- Les formes les plus avancées de coopération avec le secteur privé ont été observées dans certains États membres dans lesquels cette coopération est institutionnalisée par la mise en place d'institutions/de groupes de travail appropriés pour la coopération entre le secteur privé et l'administration publique/les services répressifs. C'est plus souvent le cas en ce qui concerne la coopération avec le secteur bancaire (voir ci-dessous), mais, comme certains rapports individuels le recommandent, il est utile d'étendre cette forme de coopération à d'autres domaines et acteurs du secteur privé.

- Tous les États membres n'ont toutefois pas créé de cadre formel pour les partenariats public/privé et, dans certains d'entre eux, la coopération, les réunions et l'échange d'informations avec le secteur privé sur les incidents, les tendances et l'évolution de la situation ont lieu de manière informelle, plutôt que sur une base légale ou contractuelle.

- La coopération avec les FSI ainsi que les fournisseurs de services en nuage et de services de communication électronique est extrêmement utile, tant pour bénéficier de leur expertise que pour accéder aux informations des abonnés ayant trait à la cybercriminalité. En procédant à des évaluations des risques, en prenant les mesures de sécurité appropriées et en appliquant une politique structurée en matière de sécurité, les fournisseurs de réseaux et de services de communication électronique peuvent non seulement prévenir certains types d'infractions informatiques mais aussi aider les services répressifs en leur fournissant des éléments de preuve matériels, à condition que ces éléments soient obtenus dans le respect des procédures prescrites par la loi.

- Selon les conclusions de l'évaluation, il faut trouver des solutions en vue d'établir un cadre clair et approprié permettant de réglementer les relations des autorités judiciaires avec les FSI dans l'ensemble de l'UE. Dans cette perspective, une telle coopération pourrait être améliorée grâce à des procédures permettant aux autorités de recevoir des réponses à leurs demandes en temps utile et grâce à la mise en place d'un système de sanctions (amende administrative ou procédurale) en cas de non-respect, de défaut de coopération ou de manquement.

- Certains États membres ont des contacts directs avec des FSI situés à l'étranger, en particulier aux États-Unis, mais la coopération avec de telles entreprises est assez problématique parce qu'elles ne répondent pas à chaque demande ou, très souvent, répondent qu'elles ne peuvent fournir les informations demandées en l'absence d'entraide judiciaire/de commissions rogatoires ou d'un mandat délivré par un tribunal. Ces situations ont une incidence majeure sur les enquêtes et peuvent parfois même conduire au classement de certaines affaires, dans la mesure où le manque d'informations peut compliquer l'identification de l'auteur, du moment et du lieu où l'infraction a été commise ainsi que de l'instrument au moyen duquel elle l'a été.

- Selon les conclusions de l'évaluation, un dialogue avec les principaux opérateurs, hébergeurs et fournisseurs d'accès et/ou de services Internet, à la fois au niveau de l'UE et au niveau international, pourrait renforcer la coopération dans le cadre des enquêtes judiciaires.

- Une coopération efficace entre les services répressifs, d'une part, et les établissements financiers et les banques commerciales, d'autre part, est également essentielle dans la lutte contre la fraude en ligne aux cartes de paiement et d'autres types de fraude liés aux opérations bancaires sur Internet (et d'utilisation de logiciels malveillants), afin de repérer de telles fraudes, d'informer le secteur privé des nouvelles tendances et de répertorier des mesures de précaution.

- Dans certains États membres, une telle coopération est facilitée par des établissements bancaires ou des commissions interbancaires spécialement créées aux fins de la lutte contre la fraude liée aux systèmes et aux moyens de paiement et qui ont tenu régulièrement des réunions, avec la participation de la police. Dans un État membre, les évaluateurs ont estimé que la participation de la police à l'organe consultatif de l'association bancaire nationale constituait une bonne pratique.

- Dans d'autres, la coopération entre les services répressifs et les établissements bancaires et financiers est moins structurée et se limite à des contacts et/ou à des réunions visant à assurer la collaboration ainsi que des échanges d'informations sur des questions liées à la cybercriminalité.

- Dans certains États membres, le secteur privé est tenu de transmettre des informations en matière de cybercriminalité, tandis que dans d'autres, une telle obligation n'existe pas ou est limitée à certaines branches du secteur privé ou à un certain type d'infractions informatiques.

- Dans certains cas, le signalement d'infractions informatiques s'effectue sur une base volontaire. L'évaluation constate toutefois que, dans certains États membres, les établissements financiers et de crédit ainsi que les FSI se montrent réticents à établir des rapports et à contribuer à une procédure pénale visant à déterminer la responsabilité pénale de l'auteur de l'infraction. Leur principale préoccupation est de réparer aussi vite que possible les dégâts que peuvent occasionner la divulgation et la couverture médiatique, qui nuisent à leur crédibilité et à leur réputation.

- Selon certains rapports, lorsque c'est le secteur privé qui est la victime ou la partie lésée, la coopération avec les services répressifs est généralement bonne car elle offre un cadre pour la préservation des éléments de preuve, leur interprétation et leur transmission aux services répressifs.

- Le secteur privé joue également un rôle important dans la protection des enfants ainsi que dans la prévention et la sensibilisation à cet égard; les associations privées et les ONG actives dans ce domaine coopèrent avec les services répressifs participant à la lutte contre l'exploitation sexuelle en ligne et apportent une contribution déterminante en relayant les rapports faisant état d'abus.

- Selon les conclusions de l'évaluation, un dialogue avec le secteur privé allant au-delà de l'obligation de signalement permettrait, en tout état de cause, d'obtenir de meilleurs résultats dans la lutte contre la cybercriminalité.

- Les pouvoirs publics devraient également coopérer, comme c'est le cas dans plusieurs États membres, avec les universités, les établissements d'enseignement, les services sociaux, les milieux d'affaires, les associations professionnelles, les médias et d'autres institutions et entreprises, afin de prévenir la criminalité informatique et la cybercriminalité et d'en neutraliser l'impact négatif sur la sécurité informatique dans le pays. En particulier, la coopération avec le monde universitaire est très importante pour la sensibilisation, la formation et la recherche et développement (R&D).

RECOMMANDATIONS

- ***Les États membres devraient maintenir et renforcer la coopération régulière entre le secteur public et le secteur privé (banques, sociétés de télécommunication et FSI), y compris en associant les procureurs et éventuellement les magistrats, afin de discuter des méthodes permettant de garantir que la collecte de preuves électroniques a lieu dans le respect de la législation en vigueur, de manière à ce que ces preuves soient admissibles dans le cadre des procédures judiciaires.***

- ***Les États membres devraient avoir recours à des partenariats public/privé structurés en vue de mettre en place, pour la coopération entre le secteur public et le secteur privé, un cadre bien défini doté de règles et de tâches clairement établies.***

- ***Les États membres devraient encourager le secteur privé à partager des informations avec les pouvoirs publics et, au besoin, prévoir dans leur droit national une obligation d'information pour le secteur privé en ce qui concerne les infractions liées au cyberespace, notamment pour imposer aux établissements de crédit de signaler sans retard tout incident lié à une cyberattaque ciblant ces établissements de crédit et/ou leurs clients.***

- ***L'Union européenne et ses États membres devraient réfléchir à la manière d'améliorer la coopération entre les services répressifs des États membres et les entreprises internationales de télécommunication ainsi que les fournisseurs internationaux d'accès à Internet et/ou de services Internet, et notamment à la possibilité pour l'UE de conclure des accords avec de grandes entreprises privées étrangères pour faciliter la coopération en matière pénale.***

X - TECHNIQUES D'ENQUÊTE

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- En raison de la grande diversité des actes de cybercriminalité, il ne saurait y avoir de procédures ou de méthodes généralement testées et éprouvées pour enquêter sur ces infractions. Chaque enquête et approche dépend des circonstances particulières, et les procédures et méthodes d'enquête doivent être adaptées à chaque cas d'espèce.

- Dans le domaine de la cybercriminalité, en particulier, le mode opératoire, les logiciels et les outils utilisés évoluent constamment et à brefs intervalles. Les mesures d'enquête doivent donc être continuellement mises à jour (par exemple au moyen de logiciels d'enquête spéciaux), conformément à l'évolution de la cybercriminalité.

- Outre les techniques d'enquête ordinaires, des techniques spéciales sont utilisées pour enquêter sur les affaires de cybercriminalité. Il existe un certain nombre de possibilités: les techniques d'enquête spéciales les plus utilisées, qui constituent des outils de travail particulièrement efficaces pour traiter notamment les affaires impliquant l'exploitation sexuelle d'enfants, sont l'interception de communications, la préservation des données et les enquêtes sous pseudonyme.

- Ces dernières, particulièrement utiles lorsqu'il n'est pas possible de recourir à des moyens techniques, sont réalisées par le déploiement d'agents infiltrés qui enquêtent sur les forums et les plateformes de discussion. Cependant, les enquêtes de ce type ne sont susceptibles de livrer des résultats satisfaisants que lorsqu'elles sont menées sur le long terme.

- D'autres techniques d'enquête spéciales s'appuient sur les nouvelles possibilités techniques en matière de lutte contre la criminalité en ligne, comme la surveillance en ligne, ou sur d'autres techniques telles que les blocs d'accès et les duplicateurs spéciaux de disques durs, la perquisition et la saisie en ligne (par exemple lorsque des services répressifs piratent en ligne un ordinateur suspect au lieu de s'en emparer physiquement), le traçage des adresses IP (par exemple sur Skype et d'autres services de messagerie), les recherches open source sur Internet, la sauvegarde de données à partir de supports de données ou d'Internet (sites web, fichiers journaux). Des techniques spéciales sont également utilisées pour les appareils mobiles (par exemple un dispositif UFED).

- Toutefois, la législation des États membres ne prévoit pas toujours le recours à des techniques d'enquête spéciales. Dans certains États membres, une décision de justice est nécessaire à cette fin.

RECOMMANDATIONS

- ***Les États membres qui ne l'ont pas encore fait sont encouragés à prévoir dans leur législation nationale la possibilité de recourir à des techniques d'enquête spéciales pour faciliter les enquêtes dans les affaires de cybercriminalité.***

XI - CHIFFREMENT

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- La disponibilité et l'utilisation croissantes de technologies de chiffrement sures et fiables garantit la sécurité, la transmission sécurisée et la confidentialité des données informatiques et, par conséquent, la protection de la vie privée des citoyens ainsi que la protection effective des données dans le cyberespace.

- Néanmoins, le recours grandissant au chiffrement aussi bien dans le cadre du stockage des données que des communications sur Internet, au moyen de techniques toujours plus sophistiquées, rend sans cesse plus difficile le déchiffrement, ce qui pose de plus en plus problème dans l'ensemble des États membres.

- Le chiffrement est souvent délibérément utilisé par les malfaiteurs pour protéger le matériel illégal en leur possession et complique la lutte contre la cybercriminalité ainsi que la prévention de ce phénomène. Comme le chiffrement est sélectionné par défaut dans de nombreuses applications et est utilisé dans le cadre d'un large éventail d'infractions, les données chiffrées posent souvent des difficultés aux services répressifs.

- Le chiffrement complique ou empêche totalement l'accès aux informations pertinentes sur la criminalité en ligne ou la cybercriminalité, en particulier pour l'identification des communications ou des données informatiques aux mains des suspects ou des auteurs d'infractions, non seulement dans le cadre des examens criminalistiques, mais également dans tous les autres types d'enquêtes. En outre, l'utilisation du chiffrement de bout en bout par un nombre croissant de fournisseurs de services rend l'interception ou l'interprétation du matériel plus difficile.

- Il n'existe de solution standard ni pour les données chiffrées ni pour les communications chiffrées. Après examen de chaque cas particulier, des mesures ciblées, telles que des mesures spéciales de surveillance des télécommunications ou des mesures de déchiffrement, peuvent être déployées.

- Dans ce contexte, la première difficulté est de détecter le contenu chiffré, qui n'est pas toujours signalé comme tel, et le type de chiffrement au moyen de l'équipement nécessaire. Le principal problème est toutefois le déchiffrement lui-même, qui n'est possible que par l'utilisation de matériel et de logiciels spécialisés hautement performants, nécessitant des investissements importants et des dépenses non négligeables.

- Pour s'attaquer à ces problèmes, il faut être familiarisé avec l'état actuel des technologies de chiffrement et étudier les points faibles des algorithmes et des applications, notamment pour pouvoir exploiter d'éventuelles erreurs.

- L'évaluation a montré que de bons résultats sont généralement obtenus lorsque des formes très simples de chiffrement sont utilisées, et qu'il est possible de déterminer ou de retrouver les saisies de clavier au moyen d'un logiciel approprié (comme PRTK via la plateforme FTK) permettant le déchiffrement. Les mots de passe simples peuvent être "forcés" à l'aide de matériel et d'outils appropriés.

- Les services d'enquête peuvent contribuer de manière significative au succès du forçage du mot de passe s'ils peuvent fournir des informations pertinentes pour le mot de passe lui-même (éventuelles phrase secrètes, fragments de phrase, jeu de caractères, longueur du mot de passe, etc.) et toutes les preuves numériques (dispositifs de stockage) aux experts en criminalistique informatique. Ce n'est cependant pas toujours efficace.

- Selon les constatations de l'évaluation, dans certains cas plus complexes, le chiffrement du contenu a pu être contourné à la suite d'attaques brutales - c'est-à-dire en essayant tous les codes possibles - ou d'attaques déclenchées par mots clés - c'est-à-dire par l'utilisation de termes conçus pour la recherche de mot de passe - ou lorsque le suspect a fourni le mot de passe ou la phrase nécessaire pour contourner le chiffrement, dans la mesure où il accepte de coopérer ou est de bonne foi.

- Toutefois, les personnes concernées ne sont pas toujours disposées à coopérer avec les autorités et il n'existe aucun moyen de les y obliger. Comme indiqué dans un rapport, un moyen d'améliorer l'efficacité des enquêtes pourrait être l'introduction du concept d'ordre de déchiffrement, qui pourrait également être élaboré au niveau européen.

- Cependant, de manière générale, l'évaluation a montré que la recherche de solutions au problème du chiffrement dans tous les domaines, y compris l'accès, les données relatives au contenu et le chiffrement de bout en bout - donne des résultats limités, car les algorithmes utilisés par les malfaiteurs et leur mise en œuvre sont souvent technologiquement solides.

- Les principaux problèmes posés par le chiffrement concernent les fichiers protégés par un chiffrement puissant (archives chiffrées en AES-256) et le chiffrement complet du disque (TrueCrypt, BitLocker, FileVault2, WinRar ou PGP). Dans ces cas, le déchiffrement au moyen d'attaques brutales ou d'attaques déclenchées par mots clés peut prendre beaucoup de temps (des mois ou parfois même des années), nécessite de très importants moyens informatiques (logiciel commercial spécialisé et équipement permettant l'utilisation d'une grappe de réseaux) pour tenter de briser la protection cryptographique, lorsque les auteurs utilisent des mots de passe longs et complexes, afin de trouver la clé de chiffrement.

- Selon les constatations de l'évaluation, il n'est souvent pas possible de résoudre efficacement le problème du chiffrement et les tentatives de déchiffrement ne sont pas toujours couronnées de succès, en particulier si le mot de passe est techniquement avancé et ne peut pas être récupéré dans un délai raisonnable; dans certains cas, le processus de déchiffrement est arrêté.

- Dans certains États membres, le déchiffrement est effectué en coopération avec des sociétés privées, dont l'expertise se révèle particulièrement utile lorsque les méthodes de chiffrement sont très sophistiquées. Dans plusieurs États membres, au contraire, les sociétés privées ne participent pas au déchiffrement dans le cadre des enquêtes pénales, celui-ci étant réservé aux instituts de police scientifique.

- Les ressources et services d'Europol, en particulier le Centre européen de lutte contre la cybercriminalité (EC3), offrent la possibilité d'utiliser sa plateforme de déchiffrement, et certains États membres font usage de cette possibilité.

- Selon les constatations de l'évaluation, il est possible de neutraliser partiellement les difficultés posées par le chiffrement pour que les enquêtes aboutissent à de meilleurs résultats en intensifiant les travaux de recherche et développement et en mettant au point de nouvelles méthodes, y compris en vue d'une analyse plus intelligente du/des mode(s) de création de mots de passe d'un suspect et de l'agrégation dynamique de la puissance de calcul.

- Une bonne coopération entre les différentes autorités concernées, en particulier les services répressifs, les services d'investigation numérique et les procureurs, est également indispensable, notamment parce que chaque service ou autorité ne peut pas se permettre d'acheter le matériel et les logiciels de récupération de mots de passe en raison des coûts qui y sont liés.

- La coopération entre les États membres dans le domaine du déchiffrement s'effectue par le partage de ressources et d'expériences et la participation à des opérations communes. S'il est nécessaire de transmettre des éléments de preuve à d'autres autorités à des fins de déchiffrement, cela peut se faire par l'intermédiaire d'Europol et d'Interpol.

RECOMMANDATIONS

- ***Les États membres devraient investir dans du matériel et des logiciels spécialisés dotés d'une capacité de calcul suffisante, ainsi que dans du personnel adéquatement formé pour permettre également le déchiffrement dans les cas complexes de fichiers et de communications chiffrés.***

- ***Les États membres devraient assurer une coopération entre tous les acteurs concernés, y compris, le cas échéant, avec des sociétés privées, afin d'améliorer les capacités de déchiffrement des autorités compétentes.***

- ***Les États membres devraient intensifier les travaux de recherche et développement en vue de mettre au point de nouvelles méthodes plus efficaces de déchiffrement et utiliser les ressources d'Europol, à savoir la plateforme de déchiffrement du Centre européen de lutte contre la cybercriminalité (EC3), dans les cas de chiffrement plus sophistiqués.***

- ***Les États membres et les institutions de l'UE devraient envisager l'élaboration d'un ordre de déchiffrement.***

XII — PREUVES ÉLECTRONIQUES

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- Un nombre important d'États membres n'ont pas de définition de la notion de preuves électroniques dans leur législation nationale. Les termes utilisés dans la Convention sur la cybercriminalité du Conseil de l'Europe (ci-après dénommée "Convention de Budapest") et dans la directive 2013/40/UE du 12 août 2013 relative aux attaques contre les systèmes d'information servent de références.

- Dans la pratique, on entend généralement par "preuve électronique" toute information produite, stockée ou transmise au moyen d'un équipement électronique et permettant d'établir l'existence ou la non-existence d'une infraction, d'identifier la personne qui a commis l'infraction et de déterminer les circonstances nécessaires au règlement d'une affaire.

- Il peut s'agir, sans que cette liste soit exhaustive, d'informations figurant dans des registres, de l'historique du trafic Internet, de données relatives aux contenus, d'images, d'adresses IP, de courriers électroniques, de documents électroniques, de fichiers vidéos, de fichiers audios et images, de bases de données, de feuilles de calcul, de cookies, de documents imprimés, de comptabilités électroniques, de données de géolocalisation provenant du système GPS ou de journaux des opérations bancaires effectuées.

- La collecte, l'analyse et l'utilisation de preuves électroniques peuvent être pertinentes dans les procédures pénales portant non seulement sur les infractions commises à l'encontre et au moyen d'ordinateurs mais aussi sur toute infraction susceptible d'impliquer des preuves électroniques.

- La nature des preuves électroniques et la facilité avec laquelle elles peuvent être manipulées ou falsifiées peuvent créer des problèmes d'admissibilité qui ne se posent pas avec d'autres types de preuves; des éléments de preuve supplémentaires peuvent par exemple être nécessaires, comme une analyse criminalistique ou un rapport d'expertise réalisé par des enquêteurs de la police scientifique.

- C'est la raison pour laquelle il existe, dans certains États membres, des exigences spécifiques en matière de collecte de preuves électroniques, qui doivent être respectées pour que ces preuves soient admissibles. Ces exigences peuvent prévoir, entre autres, que la collecte soit effectuée par un expert possédant des connaissances techniques afin de préserver l'intégrité des preuves électroniques ou une bonne documentation de la chaîne de conservation, en ce qui concerne la manière dont les preuves ont été initialement obtenues, la personne qui les a traitées et la façon dont elles ont été traitées, et notamment le fait de savoir si elles ont été modifiées d'une quelconque manière.

- Certains États membres suivent, aux fins de la collecte de preuves électroniques, les bonnes pratiques en matière d'investigation numérique établies dans la Convention sur la cybercriminalité du Conseil de l'Europe ou des orientations internationales comme les orientations de l'ACPO, qui s'appliquent également au stockage et au transfert de preuves électroniques.

- Il ressort toutefois de l'évaluation que, dans la plupart des États membres, le droit procédural est généralement neutre sur le plan technologique, ce qui signifie que les règles et principes généraux relatifs à la collecte de preuves sont appliqués et que le système procédural ne contient pas de règles de forme spécifiques en ce qui concerne l'admissibilité et l'évaluation des preuves électroniques; ces dernières sont soumises aux mêmes conditions que tout autre élément de preuve et sont évaluées par les juges conformément aux règles générales de procédure pénale.

- Par conséquent, les preuves électroniques deviennent généralement admissibles dans les procédures pénales si elles sont obtenues légalement et sont pertinentes pour le procès. Cela s'applique aussi aux preuves électroniques collectées en dehors de l'État dans le cadre la coopération avec les États membres ou de l'entraide judiciaire internationale.

- Cependant, comme cela est indiqué dans un rapport, l'absence de réglementation relative à la méthode de collecte et à la présentation des preuves électroniques devant les tribunaux ne devrait en principe pas empêcher que des poursuites effectives soient engagées dans le cadre des affaires de cybercriminalité, puisque l'admissibilité des preuves électroniques relève de la règlementation générale relative aux preuves.

- Dans quelques États membres, les preuves électroniques, comme la plupart des preuves traditionnelles, sont admissibles en justice et sont évaluées par le juge conformément au principe de la libre appréciation des preuves. Cela signifie que tout ce qui peut être utile comme élément de preuve dans une affaire peut, en principe, être présenté devant une juridiction, qui déterminera au cas par cas la valeur qu'il convient de lui attribuer. Selon les conclusions de l'évaluation, cela peut être considéré comme une bonne pratique.

- Si, au contraire, les règles relatives à l'admissibilité des preuves sont plutôt strictes, cela peut créer des obstacles à l'utilisation des preuves électroniques, notamment lorsqu'elles sont obtenues d'un autre pays, au moyen par exemple d'une demande d'entraide judiciaire.

- 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. Si la clarification des faits pertinents pour la procédure pénale nécessite la préservation des données informatiques stockées qui sont destinées à être enregistrées dans les dossiers, y compris les données opérationnelles sauvegardées au moyen du système informatique, ou sur tout support de données (par exemple CD, DVD, téléphones mobiles), les objets en question sont généralement saisis conformément au code de procédure pénale de l'État membre concerné.

- Si des preuves électroniques se trouvent sur Internet, ou si elles appartiennent à des fournisseurs de services électroniques, la coopération avec les fournisseurs de services de la société de l'information ou de services de communications électroniques est essentielle pour obtenir les données nécessaires et prendre des mesures visant à prévenir la destruction ou la modification de données.

- La nature transfrontière du cyberespace crée des difficultés particulières pour les services répressifs et les autorités judiciaires. Les preuves électroniques, qui sont aujourd'hui fondamentales pour les enquêtes et les autorités judiciaires, peuvent être stockées, modifiées et supprimées en quelques secondes à partir de n'importe quel endroit du monde.

- Elles peuvent donc également être déplacées, supprimées et contrôlées ou fragmentées dans plusieurs pays du monde en quelques secondes. Cependant, il n'est pas possible dans tous les États membres d'avoir un accès direct aux preuves électroniques situées dans un autre pays ou dans le "nuage", et il convient alors d'avoir recours aux procédures d'entraide judiciaire.

- Selon les conclusions de l'évaluation, pour remédier à ces problèmes, les procédures actuelles d'entraide judiciaire doivent être plus rapides et plus efficaces, et les autorités chargées des enquêtes doivent pouvoir envoyer très promptement des demandes à de nombreux pays différents.

- Dans certains États membres, la législation nationale permet d'obtenir des informations sur les abonnés directement auprès de fournisseurs étrangers, sous réserve qu'une telle pratique soit également autorisée par le droit de l'État où se trouve le siège du fournisseur. Dans un État membre, certains praticiens ont exprimé le souhait qu'un mécanisme harmonisé soit mis en place pour échanger des données sur les abonnés et que de nouvelles approches soient adoptées au niveau de l'UE en ce qui concerne la détermination de la compétence.

- Les formulaires de mise à disposition des preuves électroniques obtenues en cours d'enquête dans le cadre d'un dossier sous un format qui permette leur examen par les procureurs et les juges, ainsi que les pratiques en la matière, varient selon les États membres.

- La saisie du matériel informatique contenant des preuves électroniques semble ne pas être la meilleure solution, car il peut être difficile pour une victime de cybercriminalité d'accepter de se passer de l'équipement numérique qui a été ainsi saisi pendant la durée de l'enquête.

- Une autre solution pour sécuriser le matériel numérique consiste à copier (dupliquer) les données stockées sur un autre support de stockage (par exemple un DVD, un disque dur) et à les mettre à disposition sous cette forme et/ou, en particulier s'il s'agit de données lisibles (par exemple des messages textes) ou de fichiers images, à les imprimer et à les mettre également à disposition sur papier.

- En règle générale, la même procédure est utilisée pour les preuves électroniques obtenues à l'étranger. Toutefois, si des conditions spéciales sont fixées par le pays qui a aidé à obtenir les preuves, la police et les procureurs devront les respecter.

- Lorsque le procureur ou les juges qui doivent traiter des preuves électroniques dans des procédures judiciaires les reçoivent sous une forme à laquelle on ne peut accéder et qui ne permet une évaluation qu'au moyen d'un équipement informatique, et que des connaissances spécifiques sont dès lors requises, y compris pour analyser l'authenticité des preuves électroniques, un expert de la police scientifique peut être consulté.

- Selon les conclusions de l'évaluation, un matériel et des logiciels spécifiques de haute technologie aux fins d'une meilleure identification et extraction des preuves électroniques permettraient aux autorités des États membres de travailler et coopérer avec des preuves électroniques comparables.

RECOMMANDATIONS

- ***Les États membres devraient disposer d'un matériel et de logiciels de haute technologie adéquats aux fins de l'identification et de l'extraction des preuves électroniques pour permettre à leurs autorités de travailler et coopérer avec des preuves électroniques comparables.***

- ***Les États membres devraient veiller à ce que leur législation procédurale nationale soit suffisamment souple pour faciliter l'admissibilité des preuves électroniques, y compris lorsqu'elles sont obtenues d'un autre pays, par exemple au moyen de demandes d'entraide judiciaire.***

- ***Les États membres devraient envisager de nouer et maintenir un dialogue constant avec le secteur privé et d'examiner des méthodes visant à garantir que la collecte de preuves électroniques se déroule d'une manière qui permette leur admissibilité devant les tribunaux.***

XIII - L'INFORMATIQUE EN NUAGE

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- La cybercriminalité commise dans le "nuage" est considérée par un nombre important d'États membres comme un domaine soulevant des questions problématiques dans le cadre des enquêtes et des poursuites.

- Au moment de l'évaluation, certains États membres n'avaient aucune expérience en matière d'enquête sur ce type de cybercriminalité et la question de la compétence relative au stockage dans le "nuage" n'avait donc pas encore fait l'objet de recours devant leurs juridictions nationales, ce qui pourrait signifier qu'un certain nombre d'actes de cybercriminalité restent en pratique inconnus; il a toutefois été reconnu qu'ils seraient inévitablement confrontés à de telles situations.

- Ce phénomène pourrait entraîner de graves problèmes à l'avenir, car les solutions d'informatique en nuage connaissent une popularité grandissante et le recours au stockage dans le "nuage" et aux services en nuage devient une pratique de plus en plus répandue non seulement parmi les personnes morales et physiques, mais également parmi les malfaiteurs qui souhaitent dissimuler le stockage de contenu illégal; en particulier, les criminels qui commettent des abus sexuels envers des enfants via Internet sont de plus en plus souvent "cachés", car ils recourent davantage au stockage dans le "nuage".

- En raison des technologies utilisées, ainsi que de la capacité de stockage sur les serveurs et des économies d'échelle, les données se déplacent constamment à travers le monde et peuvent être fragmentées pour n'être ensuite réassemblées qu'au moment de leur récupération. Par conséquent, un des problèmes spécifiques qui se posent lors du traitement des infractions en rapport avec le "nuage" est de déterminer le lieu physique exact où l'infraction est effectivement commise, ce qui peut être difficile, très compliqué et long.

- Il n'est donc pas facile pour les services répressifs de localiser les informations et les ordinateurs qui les traitent dans le "nuage", où peuvent être stockées des données importantes dans le cadre d'enquêtes relatives à des infractions pénales, et d'y avoir accès.

- Le manque d'informations peut rendre plus difficile l'identification de l'auteur de l'infraction ainsi que la détermination du moment et du lieu où celle-ci a été commise et de l'instrument au moyen duquel elle a été commise, avec pour résultat que des actes de cybercriminalité restent impunis et que des personnes continuent à en être victimes.

- Les fournisseurs de services de stockage dans le "nuage" peuvent en outre éprouver des difficultés à localiser l'emplacement (géographique) réel des données; même les propriétaires des données ignorent souvent où se trouve cet emplacement.

- Il est généralement possible de relier les infractions commises dans le "nuage" au lieu où se trouvait l'auteur au moment où il a commis l'infraction et où l'effet s'est fait sentir. Selon le type de cybercriminalité, l'effet peut être ressenti sur le territoire de plusieurs États membres ou également en dehors du territoire des autres États membres de l'UE.

- La méthode de l'informatique en nuage crée donc des problèmes en ce qui concerne non seulement le droit national mais aussi la législation internationale, qui est fondée sur la reconnaissance de l'indépendance des États et sur le principe de territorialité.

- Même si le lieu a été déterminé, la législation de certains États membres ne permet pas la compétence extraterritoriale, ou les actes de cybercriminalité commis dans le "nuage" ne peuvent donner lieu à des poursuites que si les données sont accessibles dans les États membres concernés.

- Des conflits de compétence peuvent se poser en ce qui concerne l'émission d'un ordre visant à obtenir des preuves électroniques lorsque deux ou plusieurs États membres sont en mesure d'établir leur compétence à l'égard de l'infraction; dans ce cas, les États membres peuvent recourir aux services d'Eurojust et à des équipes communes d'enquête pour résoudre ces conflits.

- Il existe deux possibilités principales pour obtenir des données stockées dans le "nuage": soit l'accès direct au contenu du profil et aux équipements de stockage est obtenu au moyen du consentement de l'utilisateur/du propriétaire du profil ou du compte, soit l'emplacement des informations doit être déterminé et il convient de recourir à des procédures d'entraide judiciaire, qui sont longues et peu efficaces.

- L'autre solution consistant à ordonner directement aux fournisseurs de livrer les données se révèle souvent très difficile en pratique, car certains fournisseurs ne coopèrent pas avec les services de police étrangers et ne répondent pas à toutes les demandes.

- Pour surmonter ces difficultés, l'évaluation a souligné que des arrangements spéciaux avec les principaux fournisseurs de services en nuage (par exemple Google et Yahoo) pourraient être mis en place afin de réduire les délais et d'obtenir des informations dans des formats qui soient admissibles devant les tribunaux.

- Le Conseil de l'Europe a conclu des accords de droit conventionnel portant sur ces questions (y compris avec des pays tiers comme les États-Unis, le Canada, l'Australie et le Japon). Cependant, en vertu de la Convention sur la cybercriminalité, une action transfrontière n'est possible que dans un nombre très limité de cas, à savoir avec le consentement légal de la personne légalement autorisée à divulguer les données, si le territoire sur lequel elles se trouvent est connu. Si la localisation des données n'est pas connue, ces dispositions sont inadéquates.

- Compte tenu de ce qui précède, il n'a pas encore été possible de trouver une solution appropriée au problème du stockage dans le "nuage". Les diverses possibilités prévues par le droit international pour agir de manière autonome ou dans le cadre d'une coopération mutuelle (entraide judiciaire) ont montré leurs limites pour ce qui est des enquêtes portant sur des actes de cybercriminalité commis via le "nuage".

- Selon les conclusions de l'évaluation, il convient de tenir compte de ces situations et de réfléchir aux moyens d'améliorer la pratique pour garantir l'efficacité des enquêtes et des poursuites, tout en évitant par ailleurs les conflits positifs de compétence.

- À cette fin, il pourrait être utile d'envisager de se pencher sur les cadres juridiques pertinents qui existent actuellement et/ou sur les questions liées aux enquêtes afin de disposer de règles et de procédures claires pour les actes de cybercriminalité commis dans le "nuage".

- La participation des États membres en tant qu'observateurs au sein des enceintes internationales, par exemple le comité de la Convention sur la cybercriminalité, où ces questions sont examinées a également été jugée utile dans le cadre de l'évaluation.

- Un État membre a formulé des suggestions pour accéder aux données détenues dans le "nuage", par exemple prévoir la possibilité d'effectuer des recherches virtuelles dans des centres de données situés dans d'autres pays sans devoir indiquer au préalable l'emplacement physique du serveur et/ou d'ordonner aux fournisseurs de services de données de fournir des mots de passe aux services répressifs pour leur permettre d'avoir accès aux données.

RECOMMANDATIONS

- ***Les États membres devraient envisager de conclure des arrangements spéciaux avec les principaux fournisseurs de services en nuage (par exemple Google et Yahoo) afin de réduire les délais et d'obtenir des informations dans des formats qui soient admissibles devant les tribunaux.***

- ***Les États membres devraient, le cas échéant, envisager de revoir leurs cadres juridiques existants afin de disposer de règles et de procédures claires pour les actes de cybercriminalité commis dans le "nuage", notamment en prévoyant la compétence extraterritoriale pour les infractions correspondantes.***

- ***Les institutions de l'UE devraient réfléchir aux difficultés posées à l'échelle mondiale par l'informatique en nuage afin de trouver des solutions susceptibles d'augmenter la capacité à détecter les actes de cybercriminalité commis dans le "nuage" ainsi qu'à localiser les preuves de responsabilité pénale aux fins des procédures pénales et à y avoir accès.***

XIV - CONSERVATION DES DONNÉES DE COMMUNICATIONS ÉLECTRONIQUES

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- L'invalidation de la directive 2006/24/CE (directive sur la conservation des données) a créé une situation d'insécurité juridique, en particulier concernant le statut juridique de la législation nationale de transposition et la disponibilité des données de communications électroniques collectées à des fins de consultation par les services répressifs ainsi que l'utilisation de ces données en tant qu'éléments de preuve dans le cadre des procédures pénales.

- Les États membres qui ne sont plus tenus, par une obligation découlant d'un instrument juridique spécifique de l'Union, d'instaurer ou de maintenir un régime national de conservation des données imposant aux fournisseurs de conserver les données de communications électroniques ont eu à l'égard de l'arrêt différentes approches, qu'il s'agisse du maintien de la législation de transposition, de sa modification, de son remplacement ou de son abrogation ou encore de son invalidation par le juge national.

- L'évaluation a confirmé que les États membres étaient préoccupés par l'absence de cadre juridique commun au niveau de l'Union en matière de conservation des données et par la fragmentation des régimes de conservation qui en découle et qui crée d'importantes difficultés dans l'Union mais aussi dans le cadre de la coopération internationale avec les pays tiers.

- Plusieurs États membres ont souligné que l'arrêt susmentionné avait nuit à l'efficacité des enquêtes et des poursuites pénales au niveau national, en particulier pour ce qui est de la fiabilité et de l'admissibilité devant les tribunaux des éléments de preuve issus de la collecte de données de communications électroniques, ainsi qu'à la coopération judiciaire transfrontière entre les États membres et au niveau international (les possibilités de fournir et d'obtenir des éléments de preuve s'en trouvant limitées).

- Certaines données n'étant pas conservées ou ne l'étant que pendant une durée limitée, il est difficile, voire impossible, d'obtenir des preuves électroniques dans les États membres en appliquant les procédures uniformes.

- Il a été souligné en particulier que cette évolution avait gravement détérioré la capacité des autorités nationales compétentes à enquêter sur la cybercriminalité et les autres infractions dont les auteurs pourraient être plus facilement identifiés grâce aux preuves électroniques et aux données de télécommunications ou internet, et à engager des poursuites en la matière.

- Plusieurs États membres ont souligné qu'il serait bénéfique de suivre une approche commune au niveau de l'UE, y compris éventuellement un nouveau cadre législatif de nature à harmoniser les conditions et la durée de conservation des données dans les États membres.

- Entre-temps, dans l'arrêt qu'elle a rendu le 21 décembre 2016 dans les affaires jointes C-203/15 et C-698/15 "Tele2 et Watson", la Cour a jugé qu'une législation nationale qui impose la conservation générale et indiscriminée de toutes les données relatives au trafic et à la localisation excède les limites de ce qui est strictement nécessaire et a clarifié les critères et les conditions que doivent remplir les régimes nationaux de conservation des données des États membres.

- Un processus de réflexion commune associant les institutions et les États membres de l'UE est en cours pour examiner la question de la conservation des données en vue de trouver des solutions juridiques et pratiques aux problèmes découlant de la jurisprudence de la Cour de justice.

RECOMMANDATIONS

- ***Les États membres et les institutions de l'UE devraient poursuivre la réflexion commune afin de déterminer des solutions juridiques et pratiques à la question de la conservation des données de communications électroniques au niveau national et à l'échelon de l'UE, en tenant compte des principes consacrés par la récente jurisprudence de la CEJ.***

XV - ACTIONS CONTRE LA PÉDOPORNOGRAPHIE ET LES ABUS SEXUELS COMMIS CONTRE LES ENFANTS VIA INTERNET

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- Au moment où l'évaluation a eu lieu, la majorité des États membres avait transposé la directive 2011/92/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. La situation actuelle concernant la transposition de cette directive en mesures nationales peut être consultée sur la page suivante: http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32011L0093
- En raison des évolutions sociétales et technologiques, qui ont multiplié aussi bien les possibilités de communication et de diffusion d'informations que les possibilités de commettre des actes délictueux en ligne, les abus sexuels commis contre les enfants via internet (pédopiégeage, textopornographie, harcèlement en ligne, etc.) ont connu ces dernières années une augmentation notable. Afin de lutter efficacement contre ces types de délits, les États membres ont mis en œuvre un large éventail de mesures tant préventives que coercitives associant aussi bien le secteur public que le secteur privé.
- Plusieurs États membres ont établi une base de données nationale consacrée à l'identification des victimes aux fins de la lutte contre les abus sexuels commis contre des enfants, ou avaient entrepris de mettre en place une telle base de données au moment où l'évaluation a été menée. Toutefois, la majorité des États membres ne dispose pas d'une telle base de données, ou alors celle-ci n'était pas suffisamment développée au moment où l'évaluation a été menée. Dans ces cas, les autorités répressives utilisent uniquement les bases de données et les outils mis en place au niveau international, en particulier la base de données internationale sur l'exploitation sexuelle des enfants d'Interpol (ICSE-DB) qui s'avère un outil de renseignement et d'enquête puissant permettant d'identifier les victimes et les auteurs en aidant les enquêteurs spécialisés à partager des données dans le monde entier.

- Dans un État membre, lorsqu'elle ne parvient pas à identifier la victime au moyen de la base de données alors qu'elle a de bonnes raisons d'avoir des soupçons concernant l'identité éventuelle d'un enfant, la police diffuse une ou plusieurs photographies auprès des établissements scolaires à des fins d'identification; cette solution peut être considérée comme une bonne pratique.

- Afin d'éviter la revictimisation, les États membres ont mis en place différentes solutions: outre celle consistant à bloquer l'accès au matériel pédopornographique et/ou à le supprimer, les mesures suivantes sont également appliquées: les médias dangereux jugés préjudiciables aux mineurs sont repris dans un index, les contacts avec l'auteur de l'infraction sont limités, des ONG fournissent des conseils et des orientations aux victimes, ou des mesures spécifiques sont prises pour protéger les victimes et les témoins d'abus sexuels concernant des enfants contre des répercussions négatives au cours de la procédure pénale.

- Un petit nombre d'États membres n'ont pris aucune mesure spécifique pour éviter la revictimisation, mais ont établi une coopération à cette fin avec des ONG, avec des organismes et des institutions spécialisés ne relevant pas de la police mais exerçant des responsabilités dans le domaine de la protection des mineurs ou encore avec la sous-priorité "abus commis contre les enfants en ligne" de l'EMPACT dans le domaine de la "cybercriminalité"

- Les États membres ont instauré diverses mesures juridiques, techniques, organisationnelles et d'information pour lutter contre l'exploitation sexuelle/les abus en ligne, la textopornographie, le harcèlement en ligne et le tourisme sexuel impliquant des enfants. Plusieurs d'entre eux se sont dotés d'unités ou d'agents spécialisés travaillant exclusivement sur les abus sexuels commis contre des enfants, avec pour objectif d'identifier les enfants impliqués et les auteurs de faits et d'enquêter sur ces derniers. Un État membre soumet les fonctionnaires de police spécialisés travaillant dans ce domaine à une évaluation préalable lors du recrutement et à des examens psychologiques annuels; cette solution est considérée comme une bonne pratique.

- Tous les États membres ont pris, à des degrés divers, des mesures préventives visant à encourager l'utilisation sûre d'internet par les mineurs, mesures qui sont souvent mises au point sous l'égide des autorités publiques et en coopération avec des unités spécialisées et avec les ONG travaillant auprès des enfants. Certains projets dans ce domaine sont co-financés par l'UE; tel est le cas par exemple du Réseau de centres nationaux de sensibilisation à la sécurité sur l'internet (INSAFE), dans le cadre du programme de la Commission européenne visant à promouvoir une utilisation plus sure d'internet.

- Parmi les mesures préventives figurent notamment des projets de formation et des campagnes d'information visant à sensibiliser et à former les publics cibles (étudiants, parents, éducateurs, entre autres) aux principaux risques auxquels les mineurs sont exposés lorsqu'ils utilisent internet, et à en encourager une utilisation responsable. Un État membre utilise des techniques modernes consistant à associer des enfants à la formation d'autres enfants; cette solution est considérée comme une bonne pratique. Dans certains États membres, la police organise également de telles activités ou y participe.

- L'éducation aux médias est aussi un puissant outil de prévention des abus sexuels concernant les enfants, notamment en ce qui concerne les enfants et les adolescents, et dans certains États membres des informations sur les comportements sûrs que les enfants peuvent adopter en ligne sont publiées sur des sites web spécialisés. D'autres États membres ont élaboré des brochures ou des manuels ou encore des "guides scolaires" pour promouvoir une utilisation sûre et efficace d'internet, lutter contre le harcèlement en ligne, etc.

- La majorité des États membres a instauré une ligne directe qui permet de signaler anonymement des contenus liés aux abus sexuels contre des enfants et qui fait souvent aussi office de service d'assistance pour les enfants, les adolescents et les parents en leur fournissant une assistance anonyme et gratuite par téléphone et en ligne (sites ou plateformes web), entre autres sur la manière de déposer un dossier auprès de la police. Une plateforme européenne en ligne - www.reportchildsextourism.eu - répertorie l'ensemble des numéros d'urgence en Europe.

- Pour la plupart, les États membres appliquent des dispositions pénales sanctionnant le tourisme sexuel impliquant des enfants ou d'autres mesures encore, y compris pour empêcher ou interdire la diffusion de matériel qui fait la publicité des possibilités de commettre des abus concernant des enfants et du tourisme sexuel impliquant des enfants conformément à l'article 21 de la directive 2011/93/UE. Les dispositifs destinés à mieux déceler cette forme particulière de criminalité incluent des systèmes de surveillance ou de notification des déplacement des délinquants sexuels, des actions impliquant les secteurs du tourisme et du voyage ainsi que les services extérieurs, le détachement d'officiers de liaison à l'étranger, la confiscation des passeports des personnes condamnées pour des faits de pédophilie, etc.

- Parmi les mesures générales pour la détection précoce des abus sexuels commis contre des enfants sur internet, on citera notamment les patrouilles internet et les enquêtes discrètes, qui se révèlent constituer un moyen efficace de lutter contre l'exploitation sexuelle des enfants en temps réel sur internet, ainsi que les outils de filtrage, qui ne sont toutefois pas appliqués dans tous les États membres et ne s'imposent pas toujours aux FSI.

- Tous les États membres n'appliquent pas de la même manière les mesures coercitives en cas d'abus sexuels commis contre des enfants en ligne, dont le blocage de l'accès, la suppression de contenus et la fermeture de pages web; des divergences sont notamment observées en termes de procédure pour ce qui est de savoir si une décision de justice est nécessaire ou non pour mettre en œuvre ou confirmer ces mesures lorsqu'elles sont décidées par la police.

- Dans la majorité des États membres, des mesures juridiques et pratiques sont prises pour supprimer définitivement le matériel pédopornographique audiovisuel en ligne. L'approche consistant à supprimer les contenus peut être considérée comme une solution efficace, parce qu'elle permet d'empêcher que des photographies/vidéos de mineurs continuent d'être accessibles sur internet. D'autres États membres recourent également ou exclusivement à l'approche consistant à bloquer l'accès aux sites web contenant du matériel pédopornographique, ce qui rend ce matériel temporairement inaccessible.

- Lorsque le matériel est hébergé sur des serveurs situés à l'étranger, l'État membre concerné utilise généralement les canaux internationaux, à savoir Europol et son système d'échange sécurisé d'informations SIENA, ou Interpol et son initiative de blocage de l'accès; les lignes directes peuvent aussi avertir simultanément INHOPE (l'association internationale des lignes directes internet), qui veille à ce que le matériel pédopornographique dirigé vers un État mais hébergé à l'étranger puisse être supprimé d'internet.

- Dans quelques États membres, les sites web contenant des matériels pédopornographiques sont bloqués et rendus inaccessibles qu'ils soient hébergés dans l'UE ou en dehors; cette solution est considéré comme une bonne pratique.

- Aux fins de la mise en œuvre des mesures coercitives susmentionnées, il est essentiel d'établir une bonne coopération entre tous les intervenants concernés, notamment les services répressifs, les lignes directes, les ONG et les fournisseurs de services internet (FSI). Dans certains États membres, ces derniers ont l'obligation de prendre les mesures nécessaires pour empêcher d'utiliser les matériels en question, en bloquant l'accès ou en supprimant le contenu, alors que dans d'autres États membres, la législation nationale ne prévoit pas une telle obligation, bien que les mesures précitées puissent être décidées dans des cas individuels sur la base d'une décision de justice.

- Dans les États membres, la coopération entre la police et les FSI nationaux est généralement bonne, et ces derniers retirent souvent les contenus illicites pédopornographiques rapidement et volontairement lorsque ces contenus leur sont signalés par la police, même s'ils n'y sont pas tenus. Un instrument utilisé dans un État membre a été cité comme exemple de bonne pratique: il s'agit d'une icône d'interface identique pour tous les fournisseurs et comportant un bouton pouvant être actionné pour signaler qu'un site web particulier contient du matériel pédopornographique.

RECOMMANDATIONS

- ***Les États membres qui ne l'ont pas encore fait devraient mettre au point une base de données nationale consacrée à l'identification des victimes pour lutter contre les abus sexuels à l'encontre des enfants.***

- ***Les États membres qui ne l'ont pas encore fait devraient envisager de mettre au point des mesures spécifiques destinées à éviter la revictimisation, y compris des mesures pour protéger les victimes et les témoins d'abus sexuels concernant des enfants contre les répercussions négatives qu'ils pourraient subir au cours de la procédure pénale.***

- ***Les États membres devraient veiller au bon fonctionnement de la coopération entre l'ensemble des intervenants concernés, y compris les services répressifs, afin de lutter efficacement contre les infractions ciblant les enfants sur internet, et envisager d'imposer aux fournisseurs de services internet de prendre les mesures requises telles que le blocage de l'accès, la suppression de contenus et la fermeture de pages web.***

XVI - MÉCANISME DE RÉACTION AUX CYBERATTAQUES

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- Au moment où l'évaluation a eu lieu, la majorité des États membres avait transposé la directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information. La situation actuelle concernant la transposition de cette directive en mesures nationales peut être consultée sur la page suivante: http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32011L0093.

- Les cyberattaques représentent une menace en constante évolution, les méthodes et les outils utilisés pour mener ces attaques sont de plus en plus sophistiqués et l'éventail de cyberattaques menaçant le cyberespace est très large. L'évaluation a en particulier montré une augmentation notable, dans l'ensemble de l'Union européenne, du nombre d'attaques par rançongiciel - un type de logiciel malveillant qui bloque l'accès aux données jusqu'à ce qu'une rançon soit payée.

- Lorsque des cyberattaques se produisent, il convient de réaliser une évaluation technique (analyse numérique du matériel saisi pendant les opérations, par exemple recherche de virus, récupération des données effacées, etc.), tâche que certains États membres confient au secteur privé car il possède une bonne expertise et travaille avec un meilleur équipement et à moindre coût. Il est en outre nécessaire d'évaluer l'impact d'attaques éventuelles sur les infrastructures, d'avoir une vue d'ensemble de la situation et de faire le point de l'attaque, ycompris des méthodes et outils utilisés.

- Des contre-mesures appropriées, en vue d'assurer la coordination de la réaction d'urgence et le rétablissement ultérieur des systèmes d'information, et des mesures d'atténuation visant à limiter les effets d'une cyberattaque doivent être prises. Afin de garantir un niveau de sécurité approprié du cyberespace, des mesures préventives (coopération systématique et échange d'informations entre tous les acteurs publics et privés du cyberespace mondial, mesures de sensibilisation, participation à la recherche en matière de sécurité, aux analyses techniques et aux rapports de situation) sont aussi extrêmement importantes.

- La responsabilité de l'accomplissement ces tâches au niveau national afin de garantir la sécurité du cyberespace mondial est généralement partagée entre divers acteurs. Par conséquent, un cadre juridique et institutionnel approprié ainsi qu'un mécanisme pluridisciplinaire intégré sont nécessaires afin de veiller à ce que le système national de cybersécurité dispose d'un bon niveau de résilience face aux menaces informatiques; cela suppose une bonne coordination aux niveaux tant stratégique qu'opérationnel (en particulier pour l'infrastructure critique et les secteurs de l'administration publique), y compris la nécessité d'un système de gestion de crise approprié permettant de coordonner la réponse et les opérations de rétablissement.

- Dans certains États membres, une approche structurée faisant intervenir plusieurs organismes existe déjà, parfois sur la base d'un partenariat public-privé, tandis que dans d'autres, une telle approche n'est pas suffisamment développée ou fait défaut et le mécanisme de coordination de la réaction aux cyberattaques fonctionne essentiellement sur la base d'une coopération informelle.

- Au moment où l'évaluation a été menée, la majorité des États membres avaient déjà mis en place un centre national de réponse aux urgences informatiques (CERT) ou étaient en train de le faire, tandis que quelques États membres ne l'avaient pas encore fait.

- Les tâches principales des CERT consistent à surveiller les incidents de sécurité informatique et à y répondre, à émettre des alertes précoces et des alertes, à fournir des analyses des risques et des incidents, ainsi qu'à mettre en place une coopération avec le secteur privé.

- Dans certains États membres, le rôle des CERT nationaux va même au-delà de ces tâches; en effet, ils gèrent des bases de données relatives aux menaces et aux incidents, favorisent l'échange d'informations entre différentes entités, fournissent conseils et assistance pour la protection des systèmes informatiques des secteurs public et privé, mènent des actions proactives destinées à réduire les risques liés à des incidents de sécurité informatique, mènent des activités de sensibilisation et de formation, servent d'intermédiaire entre le secteur privé, le monde universitaire et les services de police, et constituent le point de contact national pour la coopération internationale.

- Les CERT gouvernementaux sont principalement chargés de gérer les crises et de répondre aux menaces et incidents de sécurité informatiques touchant le secteur public mais aussi, dans de nombreux cas, les infrastructures critiques, ainsi que, dans un nombre limité de cas, le domaine privé, ce dernier relevant toutefois habituellement de la compétence d'autres CERT dans le secteur privé.

- Dans certains États membres, les CERT gouvernementaux assument des fonctions de coordination et de supervision pour d'autres parties prenantes, ce qui s'avère être une pratique utile, en particulier dans les États membres où le mécanisme de réaction aux cyberattaques est assez complexe et/ou un nombre important de CERT divers coexistent dans les secteurs tant public que privé.

- Les CERT ne disposent pas des pouvoirs dont jouissent les services répressifs vis-à-vis des particuliers, mais en ce qui concerne les attaques de nature criminelle (tous les incidents de sécurité informatique ne relèvent pas d'actes délictueux), ils jouent un rôle important de soutien aux enquêtes en étant capables d'aider à obtenir des informations et des preuves. À cette fin, une bonne coopération entre les CERT et les services répressifs est donc très importante car il est essentiel, dans le cadre des enquêtes portant sur des cyberattaques, d'obtenir de manière efficace des informations et des preuves concernant ces attaques, compte tenu du fait que les données électroniques sont très dynamiques et peuvent facilement être perdues. Le cas échéant, d'autres entités de renseignement en matière criminelle et/ou services de renseignement pourraient participer aux enquêtes sur les incidents de sécurité informatique.

- Aux termes de la directive UE 2016/1148 (directive SRI), qui doit être transposée en droit national au plus tard le 9 mai 2018, les États membres devraient disposer de CSIRT, également connus sous la dénomination de centres de réponse aux urgences informatiques (CERT), opérationnels et conformes à certaines exigences afin de garantir l'existence de moyens effectifs pour gérer les incidents et les risques et d'assurer une coopération efficace au niveau de l'Union.

- Les pouvoirs publics ne peuvent assurer à eux seuls la résilience numérique; le secteur privé a également un rôle important à jouer, en particulier les opérateurs d'infrastructures critiques, de systèmes d'information et de réseaux, qui sont directement impliqués dans la gestion des risques et garantissent la sécurité de leurs réseaux et services.

- Conformément à la directive SRI, les États membres veillent à ce que les opérateurs de services essentiels assurent la sécurité de leurs réseaux et de leurs systèmes d'information et notifient à l'autorité compétente ou aux CSIRT, sans retard injustifié, tout incident ayant un impact significatif sur la fourniture d'un service. Une fois que la directive SRI sera pleinement mise en œuvre, les entités constituées d'infrastructures critiques seront donc légalement tenues de signaler les cyberattaques.

- Au moment où l'évaluation a eu lieu, dans certains États membres, le secteur privé avait déjà l'obligation de notifier aux services répressifs les incidents liés à des attaques électroniques dans le cyberespace. Dans certains cas, toutefois, cette obligation était limitée à certaines branches du secteur privé ou à certains types d'incidents ou aucune sanction n'était prévue en cas de non-respect de l'obligation de notification.

- Dans certains cas, malgré l'absence d'obligation formelle, la notification s'effectue sur une base volontaire; cependant, comme certains rapports le soulignent, le sous-signalement est fréquent en raison de la réticence qu'inspire aux fournisseurs de services le préjudice que les procédures pénales pourraient faire subir à leur réputation (pour plus de précisions, voir le chapitre sur la coopération). Comme l'a souligné le rapport concernant un pays, les services de police peuvent, afin d'encourager la notification, mettre en évidence le fait que les enquêtes peuvent être menées en toute confidentialité et que de bons résultats peuvent être obtenus sans porter atteinte à leur réputation.

- Il ressort des conclusions de l'évaluation que, en l'absence d'obligation de notification, il existe un risque réel que les autorités ne soient pas informées de la plupart des incidents de sécurité informatique et que, de ce fait, les infractions correspondantes fassent l'objet de poursuites et de sanctions en fonction des intérêts du secteur privé et non de ceux du secteur public.

- Un système de notification obligatoire, en particulier pour les formes graves de criminalité, est important non seulement à des fins répressives, à savoir pour faciliter une évaluation rapide et complète de la situation et une mise en œuvre plus rapide de contre-mesures ciblées, mais aussi pour que les autorités puissent disposer d'une meilleure vue d'ensemble des menaces, que des statistiques complètes sur le nombre d'incidents de sécurité informatique puissent être établies et que les mesures de précaution appropriées puissent être prises. C'est pourquoi les évaluateurs ont estimé que la mise en place d'un cadre juridique plus contraignant en matière de notification des cyberattaques par les sociétés, par exemple en rendant obligatoire cette notification comme c'est le cas dans certains États membres, constituait une bonne pratique.

- Afin d'assurer un niveau élevé de cybersécurité et un comportement soucieux de la sécurité parmi les dirigeants, les concepteurs de systèmes et les utilisateurs, des améliorations de la sécurité sont nécessaires et, pour ce faire, accroître la sensibilisation à tous les niveaux, comme c'est déjà le cas dans certains États membres, constitue un élément important d'une approche efficace en matière de cybersécurité.

- Les menaces et les attaques informatiques ayant parfois une dimension transfrontière, EMPACT se révèle être une plateforme utile en vue d'améliorer la coopération entre les États membres, les institutions et agences compétentes, et les partenaires du secteur privé dans le but de produire et de diffuser des dispositifs de protection contre les logiciels malveillants et de défense contre les attaques réseau visant les infrastructures.

- Il convient de mentionner la coopération étroite qui existe entre les CERT des trois États baltes qui ont signé un protocole d'accord en novembre 2015 par lequel ils s'engagent à intensifier leur coopération en matière de cybersécurité et de protection des systèmes et réseaux informatiques.

- Pour le traitement des cyberattaques en dehors de l'Union, les canaux formels d'entraide judiciaire sont utilisés. Toutefois, étant donné que le temps peut revêtir une importance cruciale dans le cas des crimes liés au cyberespace (en raison de la volatilité des données), une collaboration directe et un échange d'informations entre les services de police eux-mêmes ou en passant par Europol et Interpol sont également pratiqués afin de permettre une coopération plus rapide et plus efficace. Certains États membres utilisent aussi le réseau 24/7 de points de contact du G7.

- La stratégie numérique pour l'Europe encourageait les États membres à mettre en place, pour 2012, un réseau performant de CERT au niveau national et couvrant toute l'Europe. La Commission européenne invitait les États membres à renforcer la coopération entre les CERT nationaux existants et à développer les mécanismes de coopération existants tels que le groupe des CERT gouvernementaux européens.

- Une communication et une coopération existent également au niveau international par le biais des réseaux de CERT qui ont été créés à l'échelle mondiale, comme le Réseau international de veille et d'alerte (IWWN), le forum FIRST, le groupe des CERT gouvernementaux européens et la TF-CSIRT, afin de mener une collaboration dans le cadre des incidents de sécurité informatique, notamment sous forme d'appui mutuel dans la gestion des problèmes et des crises informatiques par la réalisation d'exercices réguliers. Les priorités des réseaux de CERT peuvent être tantôt similaires, dans le cas des CERT gouvernementaux/des autorités par exemple, tantôt différentes, par exemple pour les équipes issues des milieux des affaires, du monde scientifique et des pouvoirs publics.

RECOMMANDATIONS

- ***Afin de garantir un niveau approprié de protection et de sécurité du cyberespace national, les États membres devraient veiller à disposer d'un cadre interinstitutionnel efficace fondé sur une approche faisant intervenir plusieurs organismes et comprenant une coopération harmonieuse entre toutes les parties prenantes concernées par la cybersécurité, notamment du secteur privé.***

- ***Conformément à la directive SRI, les États membres qui ne l'ont pas encore fait devraient mettre en place un CERT national. Afin d'assurer un niveau élevé de cybersécurité, les États membres devraient envisager de conférer aux CERT gouvernementaux des attributions qui leur permettent de jouer le rôle de points centraux de coordination d'autres CERT et parties prenantes participant à la prévention contre les cybermenaces et à la réaction aux incidents de sécurité informatique.***

- ***À cette fin, les États membres devraient également envisager de confier aux CERT gouvernementaux la tâche de collecter et d'analyser des données concernant les incidents de sécurité informatique, de développer leurs capacités à répondre aux menaces et des systèmes logiciels d'alerte rapide, ainsi que de dispenser des formations spécifiques sur la cybercriminalité et la cybersécurité.***

- ***Conformément à la directive SRI, les États membres qui ne l'ont pas encore fait devraient introduire dans leur droit national l'obligation pour l'ensemble du secteur privé de notifier sans délai aux services répressifs les cyberattaques qui ont une incidence significative sur la continuité des services essentiels pour les services répressifs.***

- ***Les États membres sont encouragés à participer à la plateforme EMPACT concernant les cyberattaques ainsi qu'aux réseaux européens et mondiaux de CERT.***

XVII - COOPÉRATION AVEC LES AGENCES DE L'UE

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- Étant donné que la cybercriminalité, les autres infractions liées au cyberespace et les enquêtes y afférentes concernent souvent plusieurs États membres, la coopération et l'échange d'informations avec les agences de l'UE constituent une priorité.

- Europol/EC3, Eurojust, le RJE et l'ENISA jouent un rôle crucial en déployant un large éventail d'activités comprenant la production d'analyses des tendances observées en matière de cybercriminalité, la coordination des enquêtes, l'échange d'informations et de renseignements, l'analyse des données et la formation à l'échelle de l'UE. Leur expertise et leurs ressources permettent une coopération mutuelle entre les États membres et leurs services répressifs et parquets respectifs.

- Eurojust joue un rôle essentiel dans la coordination des enquêtes pénales et l'offre d'une assistance judiciaire dans le cadre de la coopération transfrontière entre les États membres, qui s'avère particulièrement utile dans des cas complexes d'infractions liées au cyberespace. Elle contribue aussi à faciliter et à accélérer la coopération avec les autorités compétentes des États membres et des États tiers dans le domaine de la cybercriminalité.

- Eurojust collecte et diffuse aussi des études de cas et des bonnes pratiques, propose des activités de formation dans le domaine de la cybercriminalité et favorise les échanges d'expériences entre des magistrats spécialisés en matière de cybercriminalité.

- Europol facilite la coopération et l'échange d'informations entre les États membres, fournit des produits et des services opérationnels aux services d'enquête et assure des formations opérationnelles et en criminalistique ainsi que du matériel de sensibilisation. L'EC3 fonctionne comme un service européen spécialisé dans la lutte contre la cybercriminalité, analyse le phénomène de la cybercriminalité dans son ensemble, coordonne les activités de tous les acteurs concernés et s'avère très utile dans le cadre d'enquêtes menées dans plusieurs pays à la fois. Europol dispose de plusieurs outils permettant l'échange de connaissances et de renseignements entre les services répressifs des États membres et avec Europol dans ce domaine, comme l'initiative EMPACT en matière de cybercriminalité, le système SIENA et la J-CAT. L'expérience opérationnelle révèle que tout effort bien pensé de lutte contre la cybercriminalité devrait comprendre des officiers de liaison J-CAT des États membres, qui possèdent l'expertise requise.

- Les États membres se félicitent d'une manière générale de l'appui et du travail de coordination fournis par Europol/EC3, Eurojust et le RJE avec l'aide de ses points de contact et considèrent que ceux-ci ont un rôle essentiel à jouer afin d'accroître la confiance mutuelle entre les autorités chargées des enquêtes et les procureurs et de faciliter la coopération internationale également avec les États tiers.

- Le rôle de l'ENISA dans la collecte des cyberalertes et la transmission de celles-ci par des systèmes automatisés est également capital pour renforcer la sécurité technique des systèmes d'information.

- Toutefois, les attributions d'Eurojust, d'Europol, du RJE et de l'ENISA en matière de cybercriminalité ainsi que les services qu'ils proposent à cet égard ne sont pas toujours très bien connus et leurs produits et services ne sont pas pleinement utilisés par les praticiens concernés dans les États membres.

RECOMMANDATIONS

- ***Les États membres devraient utiliser au mieux les services offerts par Eurojust, le RJE et Europol en ce qui concerne la cybercriminalité et veiller à une coopération étroite entre leurs CERT nationaux et l'ENISA.***

- ***Eurojust, Europol et l'ENISA devraient envisager de faire connaître leurs services et les possibilités existantes en matière de coopération et de formations spécialisées qu'elles proposent dans le domaine de la cybercriminalité et de soutenir activement les événements qui renforcent la coopération internationale dans la lutte contre la cybercriminalité.***

- ***Europol devrait aussi tirer parti du déploiement du système SIENA dans les services d'enquête, améliorer la visibilité des projets EMPACT, examiner la meilleure façon d'utiliser la J-CAT, envisager de proposer aux États membres une approche normalisée quant aux éléments structurels de bases de données contenant des renseignements relatifs à la cybercriminalité et faciliter l'adoption d'une taxonomie commune dans le domaine de la cybercriminalité.***

- ***L'ENISA devrait examiner comment normaliser le concept des cyberalertes collectées et transmises par des systèmes automatisés, ce qui permettrait de rendre comparables et d'harmoniser les statistiques relatives à ces alertes dans l'ensemble des États membres.***

XVIII - ÉQUIPES COMMUNES D'ENQUÊTE (ECE)

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- La cybercriminalité ayant souvent une dimension transfrontière, il peut être utile de participer à des enquêtes coordonnées à l'échelle internationale afin de poursuivre efficacement les auteurs d'infractions liées à la cybercriminalité.

- Dans le cadre de l'UE, les équipes communes d'enquête (ECE) constituent un outil de coopération internationale dans les affaires de criminalité transnationale, qui se fonde sur un accord conclu entre les autorités (tant judiciaires que répressives) compétentes de plusieurs États membres afin d'effectuer conjointement des enquêtes pénales.

- Au moment où l'évaluation a été menée, plusieurs États membres, certains plus fréquemment que d'autres, avaient pris part à des ECE concernant des affaires de cybercriminalité tandis que d'autres encore ne l'avaient jamais fait.

- La participation aux ECE est généralement considérée comme une expérience positive par les États membres participants, qui perçoivent les ECE comme un instrument efficace pour effectuer des enquêtes transfrontières, en ce qu'elles permettent aux enquêteurs d'échanger des informations directement et de croiser la collecte de preuves en temps utile sans avoir à présenter des demandes formelles d'entraide judiciaire distinctes.

- En raison de la longueur des procédures d'entraide judiciaire, le recours aux ECE permet de raccourcir la durée des enquêtes; elles contribuent, en outre, au renforcement de la confiance entre les autorités nationales.

- Bien que la participation d'Europol et d'Eurojust à la constitution et aux activités des ECE ne soit pas obligatoire, comme certains États membres l'ont fait remarquer, ces deux organisations peuvent jouer un rôle important pour assurer l'efficacité et la capacité opérationnelle des ECE. Certains États membres estiment qu'il est crucial que les ECE puissent être financées par Eurojust et Europol.

RECOMMANDATIONS

- ***Les États membres sont encouragés à recourir plus souvent aux ECE dans les affaires de cybercriminalité transfrontière afin de renforcer l'efficacité des enquêtes et, à cette fin, à mieux faire connaître aux praticiens les possibilités et les avantages qu'offrent les ECE.***

- ***Il convient que les institutions européennes, en particulier Eurojust et Europol, continuent de soutenir et de faciliter la constitution d'ECE et mettent à disposition un financement adapté pour aider les États membres à recourir plus fréquemment aux ECE.***

XIX - ENTRAIDE JUDICIAIRE

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- En raison de la nature fréquemment transnationale de la cybercriminalité, les infractions liées à la cybercriminalité et à la criminalité en ligne étant souvent commises par des ressortissants étrangers ou au moyen d'infrastructures informatiques étrangères, une coopération internationale harmonieuse et efficace est essentielle pour lutter efficacement contre la cybercriminalité.

- Il peut être nécessaire de bénéficier de l'entraide judiciaire d'un État étranger à tous les stades des procédures et dans le cadre de toute mesure d'enquête ou de tout acte de procédure, selon le type d'infraction liée à la cybercriminalité qui constitue le comportement illégal.

- Tel qu'il ressort de nombreux rapports, les demandes d'entraide judiciaire les plus fréquemment transmises aux États membres ou formulées par ceux-ci dans ce domaine concernent notamment les infractions liées à Internet, telles que la fraude et la falsification au moyen d'un système informatique, les attaques contre les ordinateurs et les infractions liées aux cartes de crédit. Par conséquent, de nombreuses demandes d'entraide judiciaire relatives à la cybercriminalité visent l'obtention d'éléments de preuve spécifiques détenus par des fournisseurs de service (traçage de télécommunications et identification des utilisateurs d'adresses IP), la perquisition et la saisie de systèmes informatiques ainsi que l'obtention d'informations bancaires.

- Dans aucun des États membres la législation nationale ne contient de disposition spécifique concernant l'entraide judiciaire en matière de cybercriminalité, et les procédures et conditions générales régissant les demandes d'entraide judiciaire s'appliquent donc aux affaires de cybercriminalité.

- L'entraide judiciaire, notamment dans le domaine de la cybercriminalité, peut être régie par des traités multilatéraux, des accords bilatéraux ou sur la base de la réciprocité. Les autorités nationales chargées de recevoir et d'envoyer les demandes d'entraide judiciaires diffèrent en fonction de l'instrument international applicable.

- La plupart des États membres de l'UE sont parties à la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne du 29 mai 2000 (ci-après dénommé la "convention d'entraide judiciaire"), établie conformément à l'article 34 du Traité sur l'Union européenne, et à son protocole additionnel de 2001. La majorité des États membres participe aussi à l'acquis de Schengen et applique celui-ci, qui rend également applicables les dispositions connexes relatives à la coopération judiciaire qui figurent dans la convention de Schengen, ce qui est particulièrement utile aux États membres qui ne sont pas parties à la convention d'entraide judiciaire.

- Ces instruments permettent aux autorités judiciaires (tribunaux et parquets) des différents États membres de communiquer directement, quel que soit le stade auquel la demande est formulée (enquête, poursuite, procès ou exécution des sanctions); ainsi, les demandes d'entraide judiciaire sont envoyées directement par les autorités judiciaires compétentes de l'État membre demandeur à leurs homologues de l'État membre d'exécution, qui est compétent pour décider de la suite à donner aux demandes.

- Entre les États membres qui n'appliquent pas les instruments susmentionnés, ou dans le cas des demandes transmises à des pays tiers ou formulées par ceux-ci, les demandes d'entraide judiciaire sont transmises directement (entre les autorités judiciaires nationales compétentes ou centrales) ou par la voie diplomatique (par l'intermédiaire du ministère des affaires étrangères), en fonction des dispositions des accords bilatéraux ou multilatéraux applicables.

- Lorsque la convention européenne d'entraide judiciaire en matière pénale du 20 avril 1959 et ses protocoles additionnels de 1978 et 2001 s'appliquent, les commissions rogatoires doivent être adressées par le ministère de la justice de l'État demandeur au ministère de la justice de l'État requis et renvoyées par la même voie. Toutefois, au cours des enquêtes, ou en cas d'urgence, une demande peut être transmise directement par l'autorité judiciaire nationale de l'État membre demandeur (entraide judiciaire active) à l'autorité judiciaire nationale de l'État membre d'exécution (entraide judiciaire passive).

- Les demandes d'entraide judiciaire sont généralement précédées de demandes de conservation rapide de données informatiques stockées constituant des preuves numériques, comme prévu à l'article 29 de la convention de Budapest sur la cybercriminalité du 22 novembre 2001.

- En ce qui concerne les États qui ne sont parties ni aux conventions multilatérales susmentionnées, ni à des conventions bilatérales pertinentes, l'entraide judiciaire peut se fonder sur le principe de réciprocité.

- Le délai moyen nécessaire pour répondre à une demande d'entraide judiciaire est habituellement de quelques mois, mais il varie selon que l'entraide est fournie en application d'un accord international ou du principe de réciprocité; dans ce dernier cas, le temps de réponse est encore plus long car il est d'abord nécessaire de recevoir ou d'accorder une assurance de réciprocité.

- En raison de la rapidité qui caractérise le domaine de la cybercriminalité, dans lequel les preuves numériques doivent être traitées rapidement et efficacement, tout retard risquant d'entraîner la perte de données, la longueur des procédures d'entraide judiciaire rend les canaux officiels assez inefficaces, ce qui nuit au déroulement et à la réussite des enquêtes. Par conséquent, il y a lieu dans l'ensemble d'accélérer le traitement des demandes d'entraide judiciaire dans les enquêtes en matière de cybercriminalité. Des demandes d'entraide judiciaire de meilleure qualité pourraient permettre d'accélérer sensiblement leur exécution dans d'autres pays.

- Au lieu des canaux d'entraide judiciaire formels, certains États membres recourent à ceux d'Europol, d'Eurojust et du RJE, tels que le J-CAT auprès de l'EC3, ou à Interpol, au réseau de points de contact du G7, au réseau d'officiers de liaison, ou encore à des contacts bilatéraux afin d'obtenir des réponses plus rapides. Il convient toutefois de tenir compte du fait que la validité des données devrait être vérifiée en cas d'utilisation de ces canaux moins formels.

- Le soutien fourni par Eurojust pour faciliter la communication et accélérer l'exécution des demandes urgentes, non seulement entre les États membres mais également avec des pays tiers, est considéré par plusieurs États membres comme très utile, compte tenu notamment de la présence physique de procureurs de liaison provenant des États-Unis, de Norvège et de Suisse auprès d'Eurojust.

- En ce qui concerne les pays non membres de l'UE, l'entraide judiciaire en matière pénale relative à la cybercriminalité est principalement demandée aux États-Unis et par ceux-ci, avec lesquels une coopération harmonieuse constitue un facteur essentiel, du fait que nombre de fournisseurs de services internet (FSI) sont situés sur le territoire relevant de leur compétence.

- Toutefois, de nombreux États membres rencontrent des obstacles à cet égard, en particulier dans le domaine de la conservation des données et en ce qui concerne la divulgation des adresses IP de détenteurs de comptes sur Facebook et autres réseaux sociaux. Comme les évaluateurs l'ont indiqué dans certains rapports individuels, la question de l'accessibilité des bases de données des réseaux sociaux sur internet originaires des États-Unis est un problème constant qui se pose à tous les États membres.

- Les États-Unis assortissent généralement ces demandes de fortes exigences formelles et liées au contenu, particulièrement en ce qui concerne le lien entre l'infraction pénale et l'élément de preuve spécifique faisant l'objet de la demande de transmission.

- Il ressort des conclusions de l'évaluation qu'il serait utile d'œuvrer à la mise en place de solutions internationales afin d'améliorer les procédures d'entraide judiciaire avec les pays tiers, par exemple, comme c'est le cas dans un État membre, en utilisant un formulaire de demande d'injonction de produire rapide approuvé par les autorités d'exécution d'un État donné, ce qui pourrait être considéré comme faisant partie des meilleures pratiques.

- Conformément au droit des États-Unis applicable pour la recherche d'un lieu ou l'obtention de données de courrier électronique ou de tout contenu d'une communication stockée par un FSI, une ordonnance judiciaire dénommée "*search warrant*" (mandat de perquisition) est requise. Le niveau de preuve nécessaire pour obtenir un mandat de perquisition est appelé "*probable cause*" (motif raisonnable). Ainsi, dans le cadre d'une demande d'entraide judiciaire visant à obtenir la divulgation par un FSI du contenu d'une communication stocké, les autorités des États-Unis exigeront des informations complémentaires. Cette procédure prend beaucoup de temps et, dans de nombreux cas, n'aboutit pas à l'exécution de la demande.

- Les demandes d'entraide judiciaire envoyées aux États-Unis n'ont souvent pas été exécutées, bien que dans certains cas l'importance de l'affaire ait été mise en avant et que la nécessité de disposer des preuves demandées ait été soulignée dans les demandes.

- En ce qui concerne certains États membres, la mise en place de contacts informels et personnels avec les autorités compétentes de pays tiers avant l'envoi d'une demande d'entraide judiciaire s'est révélée utile en vue d'assurer une coopération meilleure et plus rapide dans l'exécution de telles demandes.

- La mise en place d'un système d'enregistrement et d'un système de gestion en matière d'entraide judiciaire, qui permettraient de suivre un dossier de l'enregistrement de la demande à l'envoi de la réponse au pays demandeur, pourrait être considérée comme faisant partie des bonnes pratiques.

RECOMMANDATIONS

- ***Les États membres devraient améliorer la qualité des demandes d'entraide judiciaire qu'ils envoient à d'autres pays, et notamment s'assurer qu'elles contiennent les éléments adéquats, ainsi qu'étudier des méthodes visant à accélérer les réponses apportées aux demandes d'entraide judiciaire et à améliorer la qualité de celles-ci.***

- ***Il est recommandé aux États membres de renforcer l'efficacité du processus de communication avec les autres États membres et les pays tiers en mettant en place un système d'enregistrement et un système de gestion en matière d'entraide judiciaire qui permettraient de suivre un dossier de l'enregistrement de la demande à l'envoi de la réponse au pays demandeur.***

- ***Les États membres sont encouragés à utiliser plus fréquemment les outils d'Eurojust, du RJE et d'Europol et à établir des contacts informels avec les autorités étrangères compétentes afin d'obtenir plus rapidement les réponses des pays tiers aux demandes d'entraide judiciaire.***

- ***Il conviendrait que l'UE envisage de coordonner les efforts consentis en vue d'établir une méthode pour communiquer et exécuter les demandes d'entraide judiciaire formulées par ses États membres à des pays non membres de l'UE, ou en vue d'établir un cadre de coopération directe avec les FSI pertinents situés en dehors du territoire de l'UE***.

- ***L'UE devrait œuvrer à la mise en place de solutions visant à améliorer et accélérer le processus de communication entre les États membres et les pays tiers, notamment les États-Unis, en particulier eu égard à l'échange d'informations opérationnelles ainsi qu'aux demandes d'entraide judiciaire et à leur exécution.***

XX - FORMATION

PRINCIPALES CONSTATATIONS ET CONCLUSIONS

- Compte tenu de la rapidité des avancées technologiques et du caractère évolutif de la cybercriminalité, ainsi que de la nécessité qui en découle de s'adapter aux nouvelles tendances et à des modes opératoires plus sophistiqués, des formations en matière de cybercriminalité et de cybersécurité spécialisées, régulières et continues à l'intention des praticiens à tous les niveaux, y compris au début de leur carrière, revêtent une importance cruciale aux fins de la réussite des enquêtes et des poursuites relatives aux infractions liées à la cybercriminalité et à la criminalité en ligne.

- Dans la plupart des États membres, des efforts importants et des moyens, notamment humains, sont investis dans des formations spécialisées à l'intention des services répressifs dans le domaine de la cybercriminalité, tandis que tous les États membres n'offrent pas le même niveau de formation au corps judiciaire et que les cours dispensés aux magistrats ne sont pas obligatoires dans certains États membres.

- Néanmoins, au vu des spécificités techniques de la cybercriminalité dans le contexte des enquêtes et compte tenu du fait que les auteurs d'actes de cybercriminalité devraient passer devant les tribunaux, il est nécessaire que les magistrats saisis de ces affaires en aient un niveau de compréhension élevé, et il est donc fondamental que les procureurs et les magistrats chargés d'affaires de cybercriminalité reçoivent des formations spécialisées, notamment sur la façon de collecter, analyser et utiliser les preuves électroniques.

- Dans certains États membres, outre la formation fournie par des organismes publics (écoles ou instituts de police ou de magistrature), une formation en matière de cybercriminalité est également dispensée par des entités externes, telles que des universités et des sociétés privées œuvrant dans ce secteur, dont l'expertise s'avère très utile pour assurer la bonne qualité de la formation, ou bien des ONG. Certains États membres ont établis des centres d'excellence hautement spécialisés afin de fournir une formation en matière de cybercriminalité aux secteurs public et privé.

- Dans certains États membres, la formation prend également la forme de sessions d'apprentissage à distance, d'apprentissage en ligne ou bien de podcasts, qui peuvent être considérés comme faisant partie des bonnes pratiques et comme des méthodes de formation efficaces.

- En complément de la formation fournie au niveau national, les organes compétents de l'UE - EC3/Europol, ECTEG (groupe européen de formation et d'enseignement sur la cybercriminalité), Eurojust, OLAF, CEPOL et ENISA - proposent également des formations spécialisées dans le domaine de la cybercriminalité; toutefois, les États membres n'utilisent généralement pas pleinement cette possibilité.

- Certains États membres affectent un budget spécifique à la formation en matière de cybercriminalité. Dans certains États membres, davantage d'efforts devraient être consentis pour améliorer la formation spécialisée en matière de cybercriminalité de toutes les catégories de fonctionnaires traitant des affaires de cybercriminalité.

- Il ressort des conclusions de l'évaluation qu'une approche intégrée en vue de la formation commune des magistrats, procureurs et représentants des services répressifs peut permettre de diffuser les connaissances sur la cybercriminalité et servir de plateforme en vue de partager les expériences et bonnes pratiques en la matière et d'examiner les obstacles relatifs à l'admissibilité des preuves. Toutefois, l'évaluation mutuelle a révélé que seuls quelques États membres offrent déjà des formations conjointes de ce type.

RECOMMANDATIONS

- ***Les États membres devraient offrir un programme de formation complet, portant sur l'ensemble du déroulement des affaires des cybercriminalité, à tous les acteurs et praticiens qui participent à la lutte contre la cybercriminalité, et en particulier dispenser des formations plus régulières au corps judiciaire, et envisager d'affecter un budget spécifique à la formation en matière de cybercriminalité.***

- ***Les États membres devraient envisager d'organiser des formations conjointes en matière de cybercriminalité à l'intention des policiers, des procureurs et des magistrats, et d'utiliser l'approche de l'apprentissage en ligne.***

- ***Les États membres devraient utiliser au mieux les possibilités de formation offertes tant par les organes de l'UE, tels que l'EC3/Europol, l'ECTEG, Eurojust, l'OLAF, le CEPOL et l'ENISA, que par les établissements universitaires et les sociétés privées, et envisager d'établir des centres d'excellence hautement spécialisés afin de fournir des formations spécialisées en matière de cybercriminalité.***

- ***Les institutions de l'UE devraient accroître le financement de l'UE visant à aider les États membres à organiser des formations plus spécialisées à l'intention des praticiens œuvrant dans le domaine de la cybercriminalité.***