Distr. limitée
28 mars 2019
Français
Original : anglais

Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité
Vienne, 27-29 mars 2019

Projet de rapport

Additif

II. Recommandations et conclusions préliminaires

A. Détection et répression, et enquêtes (*suite*)

1. Conformément au plan de travail, la présente section contient les propositions formulées par les États Membres au titre du point 2 de l'ordre du jour intitulé « Détection et répression, et enquêtes ». Ces recommandations et conclusions préliminaires ont été soumises par les États Membres, leur mention ne signifie pas qu'elles ont l'aval du Groupe d'experts et leur ordre de présentation ne reflète pas leur degré d'importance :

a) D'une part, il a été proposé que les États Membres adoptent de nouvelles mesures internationales pour lutter contre la cybercriminalité en envisageant de négocier un nouvel instrument juridique international sur la cybercriminalité dans le cadre de l'Organisation des Nations Unies, qui refléterait les préoccupations et les intérêts de tous les États Membres et tiendrait compte également du projet de convention des Nations Unies sur la coopération dans la lutte contre la cybercriminalité, présenté au Secrétaire général le 11 octobre 2017 (A/C.3/72/12, annexe) ;

b) D'autre part, on a fait remarquer qu'il n'était ni nécessaire ni opportun d'envisager un nouveau traité mondial dans la mesure où les activités de renforcement des capacités, les échanges actifs et la coopération entre les services de détection et de répression ainsi que l'application des instruments existants comme la Convention de Budapest étaient les meilleurs moyens de faire face aux problèmes que posait la cybercriminalité et dispenser une formation adéquate aux enquêteurs, procureurs et juges. D'après cette proposition, les États Membres devraient continuer d'utiliser les instruments juridiques multilatéraux existants dans le domaine de la cybercriminalité, tels que la Convention de Budapest, ou y adhérer, étant donné que nombre de ces États estiment que cette convention représente l'instrument d'orientation le plus spécifique et le mieux adapté pour élaborer une législation interne appropriée – tant de procédure que de fond – et faciliter la coopération internationale en matière de cybercriminalité ;

c) Compte tenu de la nature transnationale de la cybercriminalité et du fait que la grande majorité des actes de cybercriminalité à l'échelle mondiale sont commis par des groupes organisés, les États Membres devraient également avoir davantage recours à la Convention contre la criminalité organisée pour faciliter la mise en

Merci de recycler

commun des informations et des éléments de preuve dans le cadre des enquêtes visant ce type de criminalité ;

d) Les États Membres devraient promouvoir et participer à la coopération internationale pour faire face à la cybercriminalité, en utilisant les instruments existants et en concluant des accords bilatéraux se fondant sur le principe de la réciprocité ; et en encourageant, en collaboration avec l'ONUDC, la création de réseaux et l'échange régulier d'informations entre les autorités judiciaires et les services de répression ;

e) Les pays devraient développer les compétences des services de police en matière d'enquête sur la cybercriminalité en les encourageant à participer aux formations dispensées par de nombreux pays ainsi que par l'ONUDC et d'autres partenaires régionaux, l'objectif étant de renforcer les capacités pour ce qui est de détecter la cybercriminalité et d'enquêter sur les affaires y relatives et d'accroître les capacités collectives de lutte contre la cybercriminalité. Les activités de renforcement des capacités menées dans ce domaine devraient en particulier tenir compte des besoins des pays en développement, mettre l'accent sur les vulnérabilités de chaque pays afin d'assurer une assistance technique adaptée, et promouvoir l'échange de connaissances de pointe dans l'intérêt des bénéficiaires ;

f) Les États sont encouragés à continuer de confier à l'ONUDC les mandats et les ressources nécessaires afin que les projets de renforcement des capacités menés dans ce domaine débouchent sur des résultats tangibles ;

g) Les pays doivent consacrer des ressources au développement des compétences nécessaires pour mener des enquêtes sur les affaires de cybercriminalité ; et à la création de partenariats afin de tirer parti de mécanismes de coopération pour obtenir des éléments de preuve essentiels ;

h) Les États Membres devraient continuer de s'efforcer à mettre en place des services, organismes ou structures spécialisés dans la lutte contre la cybercriminalité au sein des services de détection et de répression, des services de poursuite et de l'appareil judiciaire, et leur fournir l'appui nécessaire en les dotant des compétences et des moyens nécessaires pour les aider à faire face aux défis que pose la cybercriminalité et à obtenir, échanger et utiliser des preuves électroniques dans les procédures pénales ;

i) Pour lutter contre la cybercriminalité, il faut adopter des stratégies de détection et de répression à moyen et à long terme et coopérer avec des partenaires internationaux afin de perturber les marchés. Ces stratégies devraient donc être proactives et de préférence cibler les groupes cybercriminels organisés dont les membres peuvent se trouver dans différents pays ;

j) Les pays devraient continuer de s'attacher à adopter des législations de fond portant sur les formes nouvelles et émergentes de criminalité dans le cyberespace en utilisant des formulations technologiquement neutres afin qu'elles restent compatibles en dépit des progrès réalisés dans le domaine de l'informatique et de la communication ;

k) Des règles de droit procédural interne sont nécessaires pour rester en phase avec les avancées technologiques et faire en sorte que les services de détection et de répression soient en mesure de lutter contre la criminalité en ligne. Des lois pertinentes devraient être rédigées en tenant compte des notions techniques applicables et des besoins concrets des enquêteurs chargés des affaires de cybercriminalité et dans le respect des droits de la défense, de la vie privée, des libertés civiles et des droits de la personne, ainsi que des principes de proportionnalité et de subsidiarité et des garanties en matière de contrôle judiciaire. En outre, les États Membres devraient consacrer des ressources à l'adoption d'une législation interne autorisant ce qui suit :

i) Les demandes de protection rapide des données informatiques adressées à la personne qui contrôle ces données – à savoir les fournisseurs de services

informatiques et de services de télécommunications – en vue de conserver les données et de préserver leur intégrité pendant une période déterminée compte tenu de leur volatilité possible ;

ii) Les perquisitions et les saisies de données stockées sur des appareils numériques qui constituent souvent les éléments de preuve les plus pertinents pour identifier l'auteur d'une infraction électronique ;

iii) Les ordonnances demandant la production de données informatiques soumises à un régime de protection de la vie privée moins rigoureux, comme les données concernant le trafic et les abonnés ;

iv) La collecte en temps réel de données relatives au trafic et de contenus au besoin ; et

v) La coopération internationale entre les services nationaux de détection et de répression.

l) Étant donné que les enquêtes sur la cybercriminalité exigent une certaine créativité, une perspicacité technique et la coopération entre les procureurs et les services de police, les pays devraient encourager ces derniers à travailler en étroite collaboration dès l'ouverture de l'enquête afin de réunir suffisamment de preuves pour inculper les personnes identifiées ;

m) Les agents des services de répression devraient être encadrés par des enquêteurs lors de la conduite d'enquêtes sur des affaires de cybercriminalité afin de veiller au respect des droits de la défense ;

n) Les services nationaux de détection et de répression devraient prendre contact et collaborer avec les fournisseurs de services informatiques et d'autres entités du secteur privé. Ces contacts sont utiles dans le cadre des enquêtes criminelles dans la mesure où ils favorisent la confiance et la coopération entre les parties prenantes ;

o) Les pays devraient faire preuve de souplesse en ce qui concerne la détermination de la base juridictionnelle applicable aux affaires de cybercriminalité, notamment en s'appuyant davantage sur le lieu depuis lequel les services informatiques étaient fournis et non sur le lieu où les données étaient stockées ;

p) Les pays devraient investir dans la sensibilisation de la population et du secteur privé en vue d'améliorer leurs connaissances sur la cybercriminalité et remédier ainsi au faible taux de signalement de la cybercriminalité, qui est inférieur à celui d'autres types de criminalité ;

q) Les États Membres devraient encourager les partenariats public-privé dans le domaine de la cybercriminalité, notamment en adoptant des lois et en mettant en place des mécanismes de dialogue à cette fin, l'objectif étant de promouvoir la coopération entre les services de détection et de répression et les fournisseurs de services de communication ainsi que les milieux universitaires en vue de développer les connaissances et renforcer l'efficacité des mesures prises face à la cybercriminalité.

III. Résumé des délibérations

A. Détection et répression, et enquêtes (*suite*)

2. De nombreux orateurs ont rendu compte des mesures prises au niveau national pour élaborer et mettre en œuvre des stratégies et politiques en matière de cybersécurité ; promulguer et/ou améliorer la législation sur la cybercriminalité ; mettre en place de nouveaux outils d'enquête qui permettront de rassembler des preuves électroniques et d'établir leur authenticité pour qu'elles servent d'éléments de preuve dans les procédures pénales, tout en tenant compte des garanties relatives aux droits de la personne ; mettre en œuvre des dispositions institutionnelles visant à assurer une utilisation plus efficace des ressources destinées à la lutte contre la

cybercriminalité ; et promouvoir la coopération internationale en matière de lutte contre la cybercriminalité. Un orateur a mentionné les différences entre la cybersécurité et la cybercriminalité comme étant le principal facteur à prendre en considération au moment de structurer les mesures à prendre au niveau national et de définir les compétences institutionnelles dans ces domaines.

3. De nombreux orateurs ont appuyé les travaux du Groupe d'experts en tant que seule instance d'envergure et instance la plus appropriée – au niveau mondial – pour faciliter le débat et l'échange de vues entre États Membres sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, en vue d'examiner les options envisageables pour renforcer les mesures, juridiques ou autres, prises aux échelons national et international contre la cybercriminalité. La valeur ajoutée de la Commission pour la prévention du crime et la justice pénale à cet égard a également été mentionnée. Il a été suggéré que le Groupe d'experts ait un mandat unique lui permettant de servir de mécanisme de concertation dans ce domaine, toutefois cela n'exclurait pas nécessairement d'autres initiatives visant à développer une « gouvernance mondiale » globale contre la cybercriminalité au niveau international.

4. Il a été fait référence à une manifestation parallèle organisée par le Gouvernement australien, les États-Unis, la République dominicaine, Samoa et Vanuatu en marge de la réunion du Groupe d'experts sur le thème « Approaches in Tackling Cybercrime : Perspectives from across the Pacific and Beyond » (Mesures contre la cybercriminalité : perspectives dans la région du Pacifique et au-delà).

5. Un appui a été exprimé en faveur des travaux que mène l'ONUDC dans le domaine de l'assistance technique et du renforcement des capacités pour mettre au point des ripostes cohérentes face à la cybercriminalité.

6. En outre, certains orateurs se sont également félicités de la publication du Guide pratique pour les demandes de preuves électroniques internationales. Ce Guide, rédigé et publié conjointement par l'Office des Nations Unies contre la drogue et le crime (ONUDC), la Direction exécutive du Comité contre le terrorisme de l'ONU (DECT) et l'Association internationale des magistrats du parquet, a été mis à la disposition des États Membres et des agents des services de justice pénale sur le portail SHERLOC de l'ONUDC. Élaboré en collaboration avec les États Membres, d'autres organisations internationales et régionales et des fournisseurs de services de communication tels que Facebook, Google, Microsoft et Uber, il présente des informations propres à faciliter la recherche des mesures à prendre au niveau national pour recueillir, conserver et partager les preuves électroniques dans le but général qui est d'assurer l'efficacité des pratiques d'entraide juridique.

IV. Organisation de la réunion

B. Déclarations (*suite*)

7. Des déclarations ont été faites par les experts des États suivants : Arménie, Costa Rica, République dominicaine, Estonie, Géorgie, Malaisie, Mexique, Maroc, Paraguay, Pérou, Philippines, Slovaquie, Espagne, Thaïlande et Émirats arabes unis.

8. Le Conseil de l'Europe, organisation intergouvernementale, a également fait une déclaration.