Distr. limitée
27 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 (*suite*)

A. Détection et répression, et enquêtes

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, et leur mention ne signifie pas qu'elles ont l'aval du Groupe d'experts.

III. Résumé des délibérations

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

2. Au cours du débat qui a suivi, le Groupe d'experts s'est penché sur des exemples d'actes criminels présumés commis dans l'environnement numérique et qui posent d'importantes difficultés pour les praticiens de la justice pénale et les enquêteurs au moment de l'ouverture d'une enquête, ou pendant l'enquête et lors des poursuites engagées par la suite. Ces exemples comprenaient notamment la fraude en ligne, l'utilisation d'Internet à des fins terroristes, l'utilisation de l'Internet sombre (dark Web) pour mener des activités illicites, ainsi que la maltraitance et l'exploitation sexuelles des enfants au moyen de l'utilisation criminelle des technologies de l'information et de la communication. Le Groupe d'experts a en outre été informé de l'interdépendance conceptuelle de la cybercriminalité et de la cybersécurité, ainsi que des tendances de la cybercriminalité et des problèmes qu'elle pose, y compris les attaques par des logiciels rançonneurs ; les méthodes d'ingénierie sociale utilisées pour commettre des fraudes (hameçonnage, y compris vocal ou par SMS, harponnage, etc.) ; l'utilisation de la plateforme Cobalt Strike pour commettre des attaques visant le système bancaire ; l'Internet des objets ; le minage et le détournement de cryptomonnaies ; ainsi que le clonage et les infractions connexes.

3. Les participants à la réunion du Groupe d'experts se sont interrogés une fois encore si un nouvel instrument juridique international complet sur la cybercriminalité était nécessaire, ou, au contraire, si les États devraient s'attacher à donner dûment effet aux instruments existants, notamment à la Convention du Conseil de l'Europe

sur la cybercriminalité (Convention de Budapest). D'une part, on a fait valoir qu'un nouvel instrument juridique international complet sur la cybercriminalité n'était pas nécessaire, étant donné que la Convention de Budapest offrait un cadre adéquat pour l'élaboration de mécanismes de coopération nationale et internationale appropriés face à la cybercriminalité. Il a été rappelé que la Convention de Budapest comptait 63 États parties, ce qui montrait que des États non membres du Conseil de l'Europe pouvaient également y adhérer. En outre, on a fait valoir que d'autres État parties s'inspiraient de cette convention pour harmoniser les normes législatives nationales tant de procédure que de fond. Il a également été dit que par « harmonisation des normes nationales » on entendait non seulement la cohérence et des définitions communes, mais également l'utilisation de normes internationales aux fins de l'élaboration de règles nationales. On a fait référence à la complémentarité entre la Convention de Budapest et d'autres instruments régionaux comme la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (2014) et le Code de conduite international pour la sécurité de l'information, établi par l'Organisation de coopération de Shanghai.

4. Par ailleurs, il a été noté qu'un nouvel instrument juridique mondial sur la cybercriminalité dans le cadre de l'Organisation des Nations Unies était nécessaire afin de relever les défis que posait le développement rapide de la technologie d'Internet et qui n'étaient pas couverts par les mécanismes existants auxquels tous les pays du monde n'étaient pas parties. Il a été souligné qu'un tel instrument était envisagé dans le cadre d'un processus dirigé par l'ONU dans lequel tous les États Membres pourraient s'approprier les efforts déployés pour lutter à l'échelle mondiale contre la cybercriminalité et en assumer la responsabilité, tout en tirant parti des instruments existants tels que la Convention de Budapest et la Convention susmentionnée de l'Union africaine. Dans ce contexte, il a été fait référence à la résolution 73/187 de l'Assemblée générale du 18 décembre 2018, intitulée « Lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles », dans laquelle l'Assemblée priait le Secrétaire général de solliciter les vues des États Membres quant aux difficultés qu'ils rencontraient dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles et de lui présenter un rapport fondé sur ces vues pour examen à sa soixante-quatorzième session. D'autres avis ont été exprimés, selon lesquels la Convention de Budapest ne répondait pas aux préoccupations de tous les États Membres de l'ONU et prévoyait des procédures complexes pour modifier son libellé, ce qui risquait d'être désavantageux compte tenu de l'évolution constante de la cybercriminalité.

5. Il a été fait référence au processus de négociations en cours pour l'adoption d'un deuxième protocole additionnel à la Convention de Budapest, qui visait à établir des règles précises et des procédures plus efficaces dans les buts suivants : assurer une coopération internationale plus efficace et plus rapide ; autoriser la coopération directe avec les prestataires de services d'autres pays dans le cadre de demandes concernant la communication d'informations sur les abonnés et la conservation de données et les demandes urgentes ; établir un cadre plus clair et renforcer les mesures de protection en ce qui concerne les pratiques existantes pour l'accès aux données transfrontalières ; et prévoir des mesures de protection, notamment en matière de protection des données.

6. Il a également été souligné que la Convention contre la criminalité organisée pourrait être un outil utile pour lutter contre les problèmes liés à la cybercriminalité en raison notamment de leur caractère transnational. Il a été proposé d'envisager de négocier un protocole additionnel à la Convention contre la criminalité organisée qui traiterait expressément de la cybercriminalité.

7. Des délégations et des participants ont informé le Groupe d'experts du succès d'actions entreprises au niveau national pour mettre en place et appliquer des mesures juridiques et procédurales face à la cybercriminalité. Pour certains, la Convention de Budapest et les projets de renforcement des capacités qui l'accompagnent jouaient un rôle essentiel à cet égard. Les réformes législatives entreprises au niveau national,

notamment leur portée, ont été examinées plus avant. L'attention a été appelée sur la nécessité de procéder de manière participative et inclusive pour que les avis des différentes parties prenantes soient pris en compte. Il a été fait référence à la nécessité de garantir la clarté et la sécurité juridique sur la base du principe *nullum crimen nulla poena sine lege* ainsi qu'à la nécessité d'employer un langage « neutre sur le plan technologique » dans la nouvelle législation afin qu'elle reste compatible malgré l'évolution rapide des technologies de l'information et de la communication.

8. La discussion a également porté sur les problèmes liés aux conflits de compétence, en particulier dans les cas où le prestataire de services avait son siège dans un pays, alors que le contrôleur des données se situait dans un autre pays ou que les données étaient stockées dans un ou dans plusieurs pays. Il a été noté que l'émergence de l'informatique en nuage posait de nouvelles difficultés d'ordre pratique et juridique dans le cadre des enquêtes criminelles. Il a également été noté qu'il pourrait être utile de 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.

9. Le Groupe d'experts a également insisté sur la nécessité de disposer de pouvoirs procéduraux appropriés pour obtenir des preuves électroniques relatives non seulement à la cybercriminalité, mais aussi à des formes de criminalité classique, notamment des informations sur les abonnés, des données relatives au contenu ou au trafic. Il a été noté que, du fait de l'apparition de nouvelles évolutions technologiques comme des logiciels d'anonymisation, le cryptage de haut niveau et les monnaies virtuelles dans les enquêtes sur des infractions impliquant des preuves électroniques, les enquêteurs devraient peut-être adopter de nouvelles stratégies et examiner la possibilité de recourir à des techniques d'enquête spéciales et à la criminalistique numérique à distance pour rassembler de telles preuves tout en garantissant leur admissibilité et leur utilisation devant les tribunaux.

10. Le débat a également porté sur la manière de trouver un équilibre entre la nécessité d'une répression efficace de la cybercriminalité et la protection des droits fondamentaux de l'homme, en particulier le droit à la vie privée. Le dénominateur commun est que, par exemple, l'adoption de lois sur la conservation des données pourrait être une mesure pragmatique visant à ce que les fournisseurs de services de communication puissent jouer un plus grand rôle dans la lutte contre la cybercriminalité en collaborant davantage avec les services de détection et de répression, à condition que leur application soit accompagnée des garanties procédurales et des dispositions relatives à la protection de la vie privée qui s'imposent. Il a été fait référence au rapport du Haut-Commissariat des Nations Unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique, qui a été soumis au Conseil des droits de l'homme conformément à la résolution 68/167 de l'Assemblée générale (A/HRC/27/37).

11. Le Groupe d'experts a réaffirmé l'importance de la coopération internationale dans le cadre des enquêtes et poursuites transfrontières relatives à la cybercriminalité. On a reconnu que le nombre de demandes d'entraide judiciaire visant à obtenir des preuves électroniques ou à les préserver augmentait rapidement et que les modalités actuelles de coopération, en particulier la longueur des procédures d'entraide judiciaire, étaient insuffisantes pour permettre d'obtenir un accès rapide et probant aux données, en raison de la nature transitoire de ces preuves, qui pouvaient être transmises ou supprimées « en un seul clic de souris ».

12. Différentes pratiques ont été citées comme exemples de promotion de la coopération internationale pour l'obtention de preuves électroniques, plus particulièrement au niveau opérationnel, notamment : la transmission directe des demandes d'entraide judiciaire entre les autorités compétentes des États coopérants ; l'utilisation plus fréquente d'outils de coopération internationale adaptés pour protéger l'intégrité des preuves électroniques tels que la protection rapide des données informatiques ; les enquêtes communes ; l'utilisation de moyens électroniques pour

communiquer les demandes d'entraide judiciaire, en particulier l'éventuelle utilité de l'initiative d'INTERPOL prévoyant la transmission électronique sécurisée des échanges relatifs à l'entraide judiciaire (e-MLA) ; l'échange d'informations entre les points de contact du réseau 24/7 ; et une coopération directe plus fréquente entre les services de police, y compris avec l'aide d'INTERPOL, pour le renseignement. Il a aussi été fait mention du Centre européen de lutte contre la cybercriminalité (EC3), qu'Europol a créé en 2013 pour renforcer les mesures de détection et de prévention de l'Union européenne destinées à lutter contre la cybercriminalité.

13. Le Groupe d'experts a également évoqué la question de l'accès aux données par-delà les frontières. Dans l'ensemble, il a été noté que les pratiques et procédures utilisées par les États, ainsi que les conditions et les mesures de protection de ces procédures, variaient considérablement d'une Partie à l'autre. En outre, l'accent a été mis sur les droits procéduraux des suspects, la confidentialité et la protection des données personnelles, la légalité de l'accès aux données stockées dans une autre juridiction, ainsi que sur le respect de la souveraineté nationale.

14. Le Groupe d'experts a souligné l'importance d'un renforcement durable des capacités pour améliorer l'efficacité et les compétences de toutes les autorités compétentes au niveau opérationnel pour qu'elles puissent relever les défis posés par la cybercriminalité. Dans ce contexte, des orateurs ont évoqué l'utilité des échanges de bonnes pratiques et de données d'expérience entre praticiens, non seulement au niveau national mais aussi avec d'autres États. Certains orateurs ont mentionné le renforcement de la formation et de la constitution de capacités, parallèlement au développement de structures ou d'unités spécialisées dans la cybercriminalité au sein même des services de poursuite, de détection et de répression. À cet égard, il a été souligné qu'étant donné par ailleurs l'utilisation de plus en plus généralisée de preuves électroniques dans les enquêtes sur les infractions classiques, il était crucial de mettre en place des structures spécialisées pour enquêter sur ces infractions, dotées de compétences, de connaissances et de capacités opérationnelles particulières.

15. Le Groupe d'experts a examiné plus avant la coopération des autorités nationales avec le secteur privé, en particulier les fournisseurs de services de communication, en vue d'améliorer la préservation des données et l'accès à celles-ci. Même si l'importance croissante de cette coopération au niveau national, en particulier dans les situations d'urgence impliquant des infractions graves, a été soulignée, il a également été reconnu qu'il fallait redoubler d'efforts pour assurer un niveau de coopération similaire dans les affaires transnationales. À cet égard, le « risque de double conformité » pour les fournisseurs de services de communication, à savoir leurs difficultés à trouver un juste milieu face aux exigences légales des États concernés, a été mentionné.

IV. Organisation de la réunion

B. Déclarations (*suite*)

16. Des déclarations ont été faites par les experts des États suivants : Algérie, Burkina Faso, Canada, Chili, Chine, Colombie, France, Inde, Italie, Japon, Koweït, Mauritanie, Pays-Bas, Norvège et Sri Lanka.

17. L'Union européenne, organisation intergouvernementale, a également fait une déclaration.