27 juillet 2020
Français
Original : anglais

**Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité**
Vienne, 27-29 juillet 2020

# Projet de rapport

**Additif**

## II. Liste de recommandations et conclusions préliminaires (*suite*)

### A. Coopération internationale

1. Dans certaines interventions, il a été recommandé que la Commission pour la prévention du crime et la justice pénale renouvelle le mandat du Groupe d'experts sur la cybercriminalité et convienne d'un plan de travail au-delà de 2021, qui devrait également prendre en compte les nouvelles formes de cybercriminalité et l'examen des questions liées à l'exploitation et aux atteintes sexuelles visant les enfants en ligne.

2. Il a en outre été recommandé que le comité intergouvernemental spécial d'experts à composition non limitée établi en vertu de la résolution 74/247 de l'Assemblée générale, ayant pour mission d'élaborer une convention internationale générale sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, ne commence ses travaux que lorsque le Groupe aura conclu ses recommandations et les aura transmises à la Commission pour la prévention du crime et la justice pénale en 2021.

3. Toutefois, dans une autre intervention, il a été déclaré qu'il n'était pas nécessaire que le Groupe d'experts poursuive ses travaux au-delà de 2021, compte tenu de l'adoption de la résolution 74/247 de l'Assemblée générale. Cela permettra de se concentrer sur la mise en œuvre de cette résolution et la négociation d'une nouvelle convention, ainsi que d'utiliser au mieux les ressources financières disponibles.

4. Dans leurs interventions, certains États Membres ont salué l'adoption de la résolution 74/247 de l'Assemblée générale. Il a été déclaré que l'élaboration de la nouvelle convention, conformément à la résolution 74/247 de l'Assemblée générale, devrait être inclusive, transparente et faire l'objet d'un consensus, pour lequel les travaux antérieurs des Nations Unies relatifs à l'élaboration de la Convention contre la criminalité organisée et la Convention contre la corruption pourraient servir d'exemple.

5. Il a été demandé que tous les États Membres participent activement à l'élaboration des travaux du comité spécial ayant pour mission d'élaborer une nouvelle convention.

6. Parallèlement, dans d'autres interventions, il a également été déclaré qu'en termes de contenu, toute nouvelle convention devrait tenir compte des cadres et des instruments existants et ne pas être incompatible avec ces derniers. Il a été recommandé, dans l'éventuelle nouvelle convention, de tenir compte des questions relatives à la collecte transfrontalière de preuves, des dispositions relatives à l'incrimination et du respect de la souveraineté.

7. La communauté internationale devrait donner la priorité au renforcement des capacités et à d'autres formes d'assistance visant à améliorer la capacité des autorités nationales à lutter contre la cybercriminalité et en particulier contre l'exploitation et les atteintes sexuelles des enfants en ligne.

8. Les États Membres devraient s'accorder mutuellement une entraide judiciaire pour obtenir des preuves électroniques dans toute la mesure du possible, y compris dans les affaires dans lesquelles les TIC sont utilisées pour inciter à commettre ou commettre des actes liés au terrorisme ou à son financement ; il a en outre été déclaré que les entités du secteur privé avaient la responsabilité de coopérer avec les autorités nationales à cet égard.

9. Les États Membres devraient envisager d'investir dans des forces centralisées spécialisées dans la lutte contre la cybercriminalité ainsi que dans des unités technologiques régionales chargées des enquêtes pénales.

10. Les États Membres devraient également envisager de créer, au sein des autorités centrales, des unités distinctes chargées de la cybercriminalité et de l'entraide judiciaire en la matière, qui serviraient de base de connaissance dans ce domaine complexe de la coopération internationale. Ces unités spécialisées sont non seulement utiles dans la pratique quotidienne de l'entraide judiciaire, mais elles permettent en outre d'offrir une assistance ciblée au renforcement des capacités, par exemple au moyen d'une formation visant à répondre aux besoins des autorités nationales et étrangères sur la manière d'obtenir rapidement et efficacement une assistance en matière de preuves électroniques, dans le cadre de l'entraide judiciaire, pour les affaires liées au cyberespace.

11. Les États Membres devraient envisager de tenir à jour des bases de données électroniques qui facilitent l'accès aux statistiques relatives aux demandes d'entraide judiciaire reçues et envoyées en matière de preuves électroniques, afin de garantir la mise en place de mécanismes d'évaluation de l'efficacité.

12. Il convient de rappeler aux États Membres de tirer parti du rôle essentiel joué par les autorités centrales dans la transmission des demandes d'entraide judiciaire et la collaboration avec les autorités compétentes pour l'exécution des demandes d'entraide judiciaire, afin de garantir le respect des traités existants et de réduire les délais.

13. En vue d'obtenir des données pour mener des enquêtes sur la cybercriminalité, les États devraient s'appuyer sur des instruments internationaux éprouvés, ce sujet complexe nécessitant un cadre institutionnel ayant fait ses preuves et apportant une valeur ajoutée. À cet égard, on a souligné le rôle de la Convention de Budapest, qui, au fil des ans, a servi de référence en matière d'obtention de preuves électroniques, donnant au quotidien des résultats concrets pour les services de répression du monde entier. Il a en outre été recommandé aux États de réduire les conflits de lois s'agissant des dispositions juridiques applicables, en prenant comme point de départ, en cas d'injonction de production immédiate, la législation de l'État où se trouve le FAI concerné ou la législation de l'État du suspect.

14. Il est recommandé de créer un cadre dans lequel il apparaît clairement qu'en cas de « perte de localisation », la décision d'ouvrir une enquête exige un effort pour déterminer quel est le territoire concerné et le lieu où l'intégrité des réseaux automatisés est vitale pour pouvoir se consulter sur les questions de compétence et la manière la plus appropriée de poursuivre l'enquête.

15. Il a été recommandé que le droit international soit applicable dans le cyberespace, y compris les principes de souveraineté, d'intégrité territoriale et de non-intervention dans les affaires intérieures, que les TIC ne soient pas utilisées comme armes et que les attaques lancées avec le consentement d'un État soient condamnées et que les responsables soient tenus de rendre des comptes.

# IV. Organisation de la réunion (*suite*)

## C. Déclarations

16. Des déclarations ont été faites par des spécialistes des États Membres suivants : Allemagne, Australie, Autriche, Azerbaïdjan, Chine, Cuba, Espagne, France, Grèce, Honduras, Hongrie, Indonésie, Iraq, Israël, Italie, Japon, Mongolie, Nigéria, Nouvelle-Zélande, Paraguay, Philippines, Pologne, République islamique d'Iran, Royaume-Uni, Thaïlande et Venezuela (République bolivarienne du).

17. Des déclarations ont également été faites par les représentants des organisations intergouvernementales suivantes : Conseil de l'Europe, Organisation internationale de police criminelle et Union européenne. En outre, une déclaration a été faite par un observateur, l'Université normale de Beijing.