19 avril 2021
Français
Original : anglais

Rapport sur la réunion du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenue à Vienne du 6 au 8 avril 2021

I. Introduction

1. Dans sa résolution 65/230, l'Assemblée générale a prié la Commission pour la prévention du crime et la justice pénale de créer, conformément au paragraphe 42 de la Déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux : les systèmes de prévention du crime et de justice pénale et leur évolution dans un monde en mutation, un groupe intergouvernemental d'experts à composition non limitée qui se réunirait avant sa vingtième session en vue de faire une étude approfondie du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, notamment l'échange d'informations 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 et pour en proposer de nouvelles.

2. Le Groupe d'experts a tenu sa première réunion à Vienne du 17 au 21 janvier 2011. Il y a examiné et adopté un ensemble de thèmes à aborder et une méthodologie à suivre pour l'étude (E/CN.15/2011/19, annexes I et II).

3. Le Groupe d'experts a tenu sa deuxième réunion à Vienne du 25 au 28 février 2013. Il y a pris note de la version préliminaire de l'étude approfondie sur le phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, réalisée par l'Office des Nations Unies contre la drogue et le crime (ONUDC) sous son égide, conformément au mandat énoncé dans la résolution 65/230 de l'Assemblée générale ainsi qu'à l'ensemble de thèmes à aborder et à la méthodologie à suivre qu'il avait lui-même adoptés à sa première réunion.

4. Dans la Déclaration de Doha sur l'intégration de la prévention de la criminalité et de la justice pénale dans le programme d'action plus large de l'Organisation des Nations Unies visant à faire face aux problèmes sociaux et économiques et à promouvoir l'état de droit aux niveaux national et international et la participation du public, adoptée au treizième Congrès des Nations Unies pour la prévention du crime et la justice pénale et approuvée par l'Assemblée générale dans sa résolution 70/174, les États Membres ont pris note des travaux du Groupe d'experts et invité la Commission à envisager de recommander que celui-ci continue, sur la base de ses travaux, d'échanger des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, afin de trouver des

moyens de renforcer les mesures juridiques ou autres prises aux niveaux national et international face à la cybercriminalité et d'en proposer de nouvelles.

5. Le Groupe d'experts a tenu sa troisième réunion à Vienne du 10 au 13 avril 2017. Il y a, entre autres, adopté les rapports succincts du Rapporteur sur les délibérations de ses première et deuxième réunions, examiné la version préliminaire de l'étude approfondie du phénomène de la cybercriminalité et les observations reçues à son sujet, et réfléchi à la voie à suivre en ce qui la concerne. Il a également échangé des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale.

6. Dans la résolution 26/4 qu'elle a adoptée à sa vingt-sixième session, en mai 2017, la Commission a prié le Groupe d'experts de poursuivre ses travaux et, dans ce cadre, de tenir des réunions périodiques et d'offrir une tribune pour les débats à venir sur les questions de fond relatives à la cybercriminalité, en suivant l'évolution des tendances dans ce domaine et conformément à la Déclaration de Salvador et à la Déclaration de Doha. Dans cette même résolution, elle l'a prié de continuer d'échanger des informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, afin de trouver des moyens de renforcer les mesures juridiques ou autres prises aux niveaux national et international face à la cybercriminalité et d'en proposer de nouvelles.

7. Le Groupe d'experts a tenu sa quatrième réunion à Vienne du 3 au 5 avril 2018. Il y a examiné la législation et les cadres législatifs relatifs à la cybercriminalité, ainsi que l'incrimination dans ce domaine. Il y a débattu des nouvelles lois et politiques mises en place pour lutter contre la cybercriminalité aux échelles nationale et internationale. Il y a en outre étudié la manière dont la cybercriminalité était incriminée dans les différents pays. À cette même réunion, il a adopté la proposition de la présidence concernant son plan de travail pour la période 2018-2021 (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. Le Groupe d'experts a tenu sa cinquième réunion à Vienne du 27 au 29 mars 2019. À cette occasion, il a axé ses discussions sur les activités de détection et de répression et les enquêtes, ainsi que sur les preuves électroniques et la justice pénale en rapport avec la cybercriminalité. Il y a été informé, entre autres, des efforts déployés avec succès au niveau national pour appliquer des mesures juridiques et procédurales face à la cybercriminalité, et pour mettre en place de nouveaux outils d'enquête qui permettraient de recueillir des preuves électroniques et d'en établir l'authenticité pour qu'elles puissent servir dans les procédures pénales. Le débat a également porté sur l'équilibre à trouver entre une répression efficace de la cybercriminalité et la protection des droits fondamentaux de la personne, en particulier le droit à la vie privée. Le Groupe d'experts a accordé la priorité au renforcement durable des capacités pour améliorer les compétences nationales et favoriser l'échange de bonnes pratiques et de données d'expérience en matière d'enquêtes.

9. À la sixième réunion du Groupe d'experts, tenue à Vienne du 27 au 29 juillet 2020, le Rapporteur a dressé une liste de recommandations et conclusions préliminaires concernant la coopération internationale et la prévention. Conformément au plan de travail du Groupe d'experts pour la période 2019-2021, cette liste rassemblant les suggestions faites par les États Membres a été incorporée dans le rapport sur les travaux de la sixième réunion (UNODC/CCPCJ/EG.4/2020/2) en vue de la réunion de bilan qui doit se tenir au plus tard en 2021.

10. Le Bureau élargi du Groupe d'experts a approuvé par procédure d'approbation tacite, le 23 novembre 2020, les dates du 6 au 8 avril 2021 pour la septième réunion. Il est convenu de l'ordre du jour provisoire, également par procédure d'approbation tacite, le 14 décembre 2020. Il a en outre été décidé par procédure d'approbation tacite, le 11 mars 2021, qu'en raison de la situation liée à la maladie à coronavirus (COVID-19), la septième réunion se tiendrait selon des modalités hybrides. À la réunion qu'il a tenue le 31 mars 2021, le Bureau élargi est convenu que le rapport de la septième réunion du Groupe d'experts serait un rapport de procédure qui ne

comprendrait pas de résumé des délibérations établi par la présidence, mais une annexe contenant les conclusions et recommandations.

II. Organisation de la réunion

A. Ouverture de la réunion

11. La réunion a été ouverte par André Rypl (Brésil), Vice-Président du Groupe d'experts, qui assurait la présidence de la septième réunion.

B. Adoption de l'ordre du jour et autres questions d'organisation

12. À sa 1re séance, le 6 avril 2021, le Groupe d'experts a adopté l'ordre du jour suivant :

1. Questions d'organisation :
   a) Ouverture de la réunion ;
   b) Adoption de l'ordre du jour.
2. Examen de toutes les conclusions et recommandations préliminaires issues des quatrième, cinquième et sixième réunions du Groupe d'experts, tenues en 2018, 2019 et 2020, et formulation des conclusions et recommandations à présenter à la Commission pour la prévention du crime et la justice pénale.
3. Débat relatif aux futurs travaux du Groupe d'experts.
4. Questions diverses.
5. Adoption du rapport.

C. Déclarations

13. Au titre du point 1 de l'ordre du jour et comme proposé par la présidence, le Groupe d'experts a décidé que les délégations ne feraient pas de déclarations générales. Il a également décidé qu'en raison des contraintes de temps, chacune des déclarations faites au titre des points 2 et 3 serait limitée à trois minutes maximum, les délégations ayant par ailleurs la possibilité d'envoyer des déclarations par écrit au secrétariat, qui les afficherait sur la page Web consacrée à la septième réunion du Groupe d'experts.

14. Au titre du point 3 de l'ordre du jour, des déclarations ont été faites par l'Australie, le Chili, la Colombie, l'Union européenne (au nom de ses États membres), le Yémen, la République dominicaine, le Brésil, les Pays-Bas, la République bolivarienne du Venezuela, la Nouvelle-Zélande, le Guatemala, le Nigéria, les États-Unis d'Amérique, la Chine, la Fédération de Russie, la France, Cuba, le Japon, l'Afrique du Sud, la Pologne, le Canada, la Belgique, l'Autriche, l'Argentine, la Norvège, la République islamique d'Iran, le Portugal, le Kirghizistan, le Honduras, le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, l'Inde, le Mexique, le Nicaragua et la République arabe syrienne.

D. Organisation des travaux

15. À sa 1re séance, le 6 avril, le Groupe d'experts a commencé à examiner la liste des conclusions et recommandations qui étaient regroupées sous les rubriques « Législation et cadres » et « Incrimination » dans le document de séance intitulé « Compilation de l'ensemble des conclusions et recommandations préliminaires présentées par les États Membres lors des réunions du Groupe d'experts chargé de

réaliser une étude approfondie sur la cybercriminalité, tenues en 2018, 2019 et 2020 » (UNODC/CCPCJ/EG.4/2021/CRP.1). À cette fin, le Président a invité les délégations qui étaient opposées, soit sur le fond, soit sur la forme, à une conclusion ou à une recommandation à le faire savoir ; les objections formulées seraient alors consignées dans un texte évolutif projeté à l'écran et mis ultérieurement à la disposition des délégations par voie électronique.

16. À sa 2e séance, le 6 avril, le Groupe d'experts a procédé à une première lecture de la liste des conclusions et recommandations préliminaires correspondant à ses réunions de 2018 et 2019, et a commencé à examiner en détail les conclusions et recommandations dont la formulation ne faisait pas l'objet d'un consensus.

17. À sa 3e séance, le 7 avril, le Groupe d'experts a procédé à une première lecture de la liste des conclusions et recommandations correspondant à sa réunion de 2020 et a poursuivi son examen détaillé de certaines des conclusions et recommandations qui ne faisaient pas l'objet d'un consensus. Il a également débattu de la manière dont ces dernières seraient portées à l'attention de la Commission.

18. À sa 4e séance, le 7 avril, le Groupe d'experts a poursuivi l'examen détaillé de certaines conclusions et recommandations qui ne faisaient pas l'objet d'un consensus. Des opinions divergentes ont été exprimées quant à savoir si ces conclusions et recommandations devaient être présentées à la Commission.

19. À sa 5e séance, le 8 avril, le Groupe d'experts a poursuivi ses discussions pour déterminer s'il fallait présenter à la Commission les conclusions et recommandations préliminaires qui ne faisaient pas l'objet d'un consensus. Approuvant une proposition du Président, le Groupe d'experts est convenu que le présent rapport rendrait compte du fait que toutes les conclusions et recommandations contenues dans le document UNODC/CCPCJ/EG.4/2021/CRP.1 avaient fait l'objet d'un examen accéléré car, compte tenu des modalités d'organisation liées à la COVID-19, le temps disponible pour sa septième réunion avait été limité à un total de 12 heures au lieu des 18 heures habituelles. Le Groupe d'experts a également décidé de transmettre à la Commission les 63 conclusions et recommandations ayant été approuvées, telles qu'elles figurent à l'annexe du présent rapport.

20. À sa 5e séance également, le Groupe d'experts a examiné le point 3 de l'ordre du jour, intitulé « Débat relatif aux futurs travaux du Groupe d'experts ». Des opinions divergentes ont été exprimées à ce sujet, comme l'illustrent les déclarations téléchargées sur la page Web de la septième réunion du Groupe d'experts[1].

E. Participation

21. Ont participé à la réunion les représentantes et représentants de 111 États Membres, de 5 instituts appartenant au réseau du programme des Nations Unies pour la prévention du crime et la justice pénale, de 3 entités des Nations Unies et de 11 organisations intergouvernementales, ainsi que des représentantes et représentants du monde universitaire et du secteur privé.

22. La liste des participantes et participants est publiée sous la cote CTOC/COP/UNODC/CCPCJ/EG.4/2021/INF/1/Rev.1.

F. Documentation

23. Le Groupe d'experts était saisi des documents suivants :

a) Ordre du jour provisoire annoté (UNODC/CCPCJ/EG.4/2021/1) ;

[1] Voir https://www.unodc.org/unodc/fr/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime_2021.html.

b) Compilation de l'ensemble des conclusions et recommandations préliminaires présentées par les États Membres lors des réunions du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, tenues en 2018, 2019 et 2020 (UNODC/CCPCJ/EG.4/2021/CRP.1).

III. Adoption du rapport

24. À sa 6e séance, le 8 avril 2021, le Groupe d'experts a adopté le présent rapport.

Annexe

Conclusions et recommandations approuvées par le Groupe d'experts et soumises à l'examen de la Commission pour la prévention du crime et la justice pénale

Législation et cadres

1. Les États Membres devraient s'assurer que leurs dispositions législatives résistent à l'épreuve du temps en ce qui concerne de futurs progrès technologiques, en adoptant à cet effet des lois aux formulations technologiquement neutres qui incriminent l'activité jugée illicite et non les moyens employés. Lorsqu'ils l'estiment nécessaire et opportun, ils devraient également envisager d'établir une terminologie cohérente pour décrire les activités liées à la cybercriminalité au niveau national et permettre, dans la mesure du possible, l'interprétation exacte des lois pertinentes par les services de détection et de répression et le système judiciaire.

2. Les États Membres devraient aider l'Office des Nations Unies contre la drogue et le crime (ONUDC) à mettre en place un projet ou un programme éducatif axé sur la sensibilisation à la cybercriminalité et les mesures à prendre, à l'intention des autorités judiciaires, des organes chargés des poursuites et des experts en criminalistique numérique des États Membres, ainsi que des entités privées, et utiliser des outils de renforcement des capacités ou une plateforme électronique de gestion des connaissances pour sensibiliser la société civile aux incidences de la cybercriminalité.

3. L'ONUDC devrait s'engager activement dans le renforcement des capacités de tous les États Membres ayant besoin d'assistance, en particulier les pays en développement. Ces activités de renforcement des capacités devraient être politiquement neutres et exemptes de conditions, résulter de consultations approfondies et être acceptées volontairement par les pays bénéficiaires. Sur le fond, ces activités devraient couvrir au moins les domaines suivants : formation des juges, des procureurs, des enquêteurs et des services de détection et de répression aux enquêtes sur la cybercriminalité, au traitement des preuves électroniques, à la chaîne de conservation et à l'analyse criminalistique.

Incrimination

4. Les États Membres devraient tenir compte du fait que de nombreuses dispositions de droit pénal matériel visant la criminalité « hors ligne » peuvent également s'appliquer aux infractions commises en ligne. C'est pourquoi, afin de renforcer les activités de détection et de répression, ils devraient appliquer les dispositions existantes de droit national et international, selon qu'il convient, pour combattre la criminalité dans l'environnement numérique.

5. Dans la mesure où ils ne l'ont pas encore fait, les États Membres devraient envisager d'ériger en infraction pénale :

a) Le fait d'accéder illégalement à des systèmes informatiques ou de les pirater ;

b) Le fait d'intercepter ou d'endommager illégalement des données informatiques et d'endommager des systèmes informatiques ;

c) L'atteinte à l'intégrité des données et des systèmes informatiques.

6. Les États Membres devraient étudier les moyens qui permettraient de faire en sorte que l'échange d'informations entre les enquêteurs et les procureurs chargés de la lutte contre la cybercriminalité se fasse de manière rapide et sûre, y compris en renforçant les réseaux d'institutions nationales qui pourraient être disponibles 24 heures sur 24.

Détection et répression, et enquêtes

7. Les États sont encouragés à continuer d'accorder à l'ONUDC les mandats et les moyens financiers nécessaires pour que les projets de renforcement des capacités menés dans ce domaine débouchent sur des résultats tangibles.

8. Les pays devraient consacrer des ressources au développement des compétences nécessaires pour enquêter sur les affaires de cybercriminalité et à la création de partenariats qui tirent parti de mécanismes de coopération afin d'obtenir des éléments de preuve essentiels.

9. Les pays devraient investir dans les activités de sensibilisation de la population et du secteur privé pour tenter d'améliorer le taux de signalement des actes relevant de la cybercriminalité, qui est inférieur à celui d'autres types de criminalité.

10. Les règles de droit procédural interne doivent 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 cybercriminalité. Des lois adaptées devraient être rédigées en tenant compte des notions techniques applicables et des besoins concrets des enquêteurs chargés des affaires de cybercriminalité, dans le respect des garanties d'une procédure régulière, de la vie privée, des droits humains et des libertés fondamentales. En outre, les États Membres devraient consacrer des ressources à l'adoption d'une législation interne autorisant ce qui suit :

a) La collecte en temps réel de données relatives au trafic et de contenu lorsqu'il y a lieu ;

b) La coopération internationale entre les autorités nationales de détection et de répression.

Preuves électroniques[2] et justice pénale

11. Les États Membres devraient redoubler d'efforts pour renforcer les capacités du personnel chargé de la détection et de la répression, y compris les procureurs, le personnel des structures spécialisées et celui de l'appareil judiciaire, afin que tous disposent au minimum des connaissances techniques de base relatives aux preuves électroniques pour pouvoir répondre efficacement et rapidement aux demandes d'assistance concernant la localisation des communications et prendre d'autres mesures nécessaires aux fins des enquêtes sur les affaires de cybercriminalité.

12. Les États Membres devraient prendre les mesures nécessaires pour adopter une législation garantissant la recevabilité des preuves électroniques, tout en gardant à l'esprit qu'il appartient à chaque pays de se prononcer sur la recevabilité d'une preuve, y compris électronique, conformément au droit national.

13. Les États Membres sont encouragés à améliorer la mise en commun des données d'expérience et des informations dont ils disposent, notamment sur leur législation et leurs procédures nationales, sur les meilleures pratiques en matière d'enquêtes transnationales relatives à la cybercriminalité ainsi que sur les groupes criminels organisés et les techniques et méthodes qu'ils utilisent.

14. L'ONUDC devrait mettre au point un programme de formation à l'intention des autorités judiciaires et des autorités chargées des poursuites dans les États Membres afin de mieux faire connaître les mesures de lutte contre la cybercriminalité, en particulier la collecte de preuves électroniques.

15. Dans les systèmes juridiques qui utilisent les procédures inquisitoires et dans lesquels les agents des services judiciaires sont aussi enquêteurs, une formation

[2] Selon un État Membre, dans le terme « preuves électroniques », l'adjectif « électronique » qualifiait le mode de transmission ou de stockage des données, lequel pouvait par exemple inclure les ondes radio ou la fibre optique. Certains ont estimé qu'il était en fait question des « informations numériques », composées de 1 et de 0, et non des « preuves électroniques ». D'après un autre État Membre, les « preuves électroniques » englobaient des éléments de preuve tant numériques qu'analogiques.

spécialisée à la cybercriminalité devrait être dispensée au personnel de l'appareil judiciaire.

16. Les États souhaiteront peut-être inscrire dans leur législation nationale la possibilité d'utiliser comme preuves les données suivantes : les données relatives au trafic, comme les fichiers journaux ; les données relatives au contenu, comme les courriers électroniques ; les données relatives aux abonnés, comme les informations d'inscription des utilisateurs ; et d'autres données stockées, traitées et communiquées au format numérique et produites pendant l'infraction, et donc susceptibles de servir à démontrer les faits en cause.

17. Les États Membres devraient définir et appliquer des cadres légaux, des règles de compétence et d'autres dispositions procédurales afin que la cybercriminalité puisse faire l'objet d'enquêtes au niveau national et qu'une coopération internationale efficace soit mise en place dans ce domaine au moyen d'une action de détection et de répression efficace, dans le respect de la souveraineté nationale ainsi que de la protection de la vie privée et de tous les droits humains. Cela pourrait passer notamment par :

a) La modification des règles de preuve de telle sorte que les preuves électroniques puissent être recueillies, préservées, authentifiées et utilisées aux fins de poursuites pénales ;

b) L'adoption de dispositions permettant de tracer les communications aux niveaux national et international.

18. Les États Membres devraient prendre des mesures pour améliorer la coopération en matière de collecte de preuves électroniques. À cet égard, ils sont encouragés à envisager de faire, entre autres, ce qui suit :

a) Échanger des informations sur les menaces liées à la cybercriminalité ;

b) Favoriser la coopération et la coordination entre les services de détection et de répression, les procureurs et les autorités judiciaires ;

c) Mettre en commun les meilleures pratiques et les données d'expérience relatives aux enquêtes transnationales sur la cybercriminalité ;

d) Établir des partenariats public-privé avec les fournisseurs de services afin de définir des modalités de coopération en matière de détection et de répression, d'enquêtes sur la cybercriminalité et de collecte de preuves ;

e) Élaborer des lignes directrices à l'intention des fournisseurs de services pour aider les services de détection et de répression dans le cadre des enquêtes sur la cybercriminalité, notamment en ce qui concerne le format et la durée de conservation des preuves et informations numériques ;

f) Renforcer les capacités techniques et juridiques des services de détection et de répression, des juges et des procureurs au moyen de programmes de développement des compétences ;

g) Organiser des ateliers et des séminaires visant à mieux faire connaître les meilleures pratiques de lutte contre la cybercriminalité.

Coopération internationale

19. Il faudrait améliorer l'efficacité de la coopération internationale en mettant en place des dispositifs d'intervention rapide en la matière ainsi que des voies de communication entre les autorités nationales par l'intermédiaire d'agents de liaison et de systèmes informatiques aux fins de la collecte transfrontalière de preuves et du transfert en ligne de preuves électroniques.

20. Il faudrait optimiser les procédures de coopération internationale afin qu'une aide maximale soit fournie, dans les limites des possibilités découlant des cadres juridiques nationaux, pour répondre aux demandes de coopération internationale concernant la conservation des preuves électroniques ainsi que l'accès aux données

de connexion et aux informations d'enregistrement des utilisateurs, sans pour autant compromettre les droits humains et les libertés fondamentales ni les droits de propriété.

21. Les pays sont invités à accorder une attention particulière à la nécessaire proportionnalité des mesures d'enquête, tout en respectant les libertés fondamentales et les régimes de protection des données à caractère personnel associés à la correspondance privée.

22. Les pays sont encouragés à faciliter la coopération avec les entreprises et à renforcer la collaboration entre les autorités publiques et les fournisseurs d'accès privés, en particulier pour faire face aux problèmes que posent les contenus criminels nuisibles sur Internet.

23. Les pays sont invités à rejoindre les réseaux autorisés de praticiens pour conserver et échanger des preuves électroniques recevables, à les utiliser plus largement et à les renforcer, y compris les réseaux 24/7, les réseaux spécialisés dans la cybercriminalité et les canaux de l'Organisation internationale de police criminelle (INTERPOL) pour une coopération policière rapide, ainsi qu'à mettre en place des réseaux avec des partenaires stratégiquement alignés, en vue de partager des données sur les questions de cybercriminalité, d'intervenir rapidement et de réduire au minimum la perte de preuves essentielles. Il a en outre été recommandé de recourir à la coopération policière et à d'autres méthodes de coopération informelle avant d'utiliser les canaux d'entraide judiciaire.

24. Les États Membres devraient échanger des informations sur leur manière de résoudre les difficultés à accéder rapidement aux preuves numériques, pour que les autres États Membres puissent tirer parti de ces expériences et rendre leurs procédures plus efficaces.

25. Les États Membres devraient établir des pratiques qui permettent de transmettre et de recevoir des demandes d'entraide judiciaire par voie électronique afin de réduire les délais de transmission des documents entre les États.

26. Les pays devraient améliorer l'application des législations nationales et renforcer la coordination et les synergies internes dans le domaine de la collecte et du partage d'informations et d'éléments de preuve à des fins de poursuites.

27. Les États sont encouragés à créer des équipes d'enquête conjointes avec d'autres pays au niveau bilatéral, régional ou international afin de renforcer leurs capacités d'intervention.

28. Pour que la coopération internationale soit efficace, il faut que la législation nationale établisse des procédures qui la facilitent. Ainsi, la législation nationale doit permettre la coopération internationale entre services de détection et de répression.

29. Il faudrait accorder la priorité au renforcement durable des capacités et à l'assistance technique en vue d'améliorer les compétences dans tous les domaines opérationnels et de renforcer les moyens dont disposent les autorités nationales pour combattre la cybercriminalité, notamment par la constitution de réseaux, l'organisation de réunions et de formations conjointes, la mise en commun des meilleures pratiques et l'élaboration de supports de formation et de modèles de coopération. Ces activités de renforcement des capacités et de formation devraient inclure une formation hautement spécialisée à l'intention des praticiens, encourageant en particulier la participation de femmes spécialistes, et elles devraient répondre aux besoins des législateurs et des décideurs politiques afin qu'ils puissent mieux appréhender la question de la conservation des données à des fins répressives. Ces activités devraient également être axées sur l'amélioration des compétences des services de détection et de répression, des enquêteurs et des analystes en ce qui concerne la criminalistique, le recours à des données de source ouverte à l'appui des enquêtes et la chaîne de mise en sûreté des preuves électroniques, ainsi que la collecte et le partage des preuves électroniques à l'étranger. Elles devraient en outre viser à

renforcer les capacités des juges, des procureurs, des autorités centrales et des avocats pour leur permettre de juger et de traiter efficacement les affaires pertinentes.

30. La coopération internationale est importante pour ce qui est de recueillir des preuves électroniques et de les partager dans le cadre d'enquêtes transnationales et pour répondre rapidement et efficacement aux demandes d'entraide judiciaire liées à la conservation et à l'obtention de preuves électroniques. Il convient, dans ce contexte, de respecter les principes de souveraineté et de réciprocité.

31. L'ONUDC est encouragé à continuer de fournir aux experts gouvernementaux nationaux des programmes de formation et de renforcement des capacités pour lutter contre la cybercriminalité, afin de renforcer les capacités de détection et d'enquête dans ce domaine. Ces activités devraient tenir compte des besoins des pays en développement, se concentrer sur les faiblesses de chaque pays afin d'apporter une assistance technique adaptée et favoriser l'échange de connaissances aussi actualisées que possible dans l'intérêt des praticiens et des parties prenantes.

32. L'ONUDC a élaboré le Rédacteur de requêtes d'entraide judiciaire pour aider les praticiens de la justice pénale à rédiger ce type de demandes, ainsi que le Guide pratique sur la demande de preuves électroniques à l'étranger, destiné aux praticiens des États Membres et disponible sur demande. Les pays peuvent tirer parti de l'utilisation de ces outils essentiels mis au point par l'ONUDC.

33. Il a été demandé que tous les États Membres participent activement aux travaux du comité spécial ayant pour mission d'élaborer une nouvelle convention.

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

35. Les États Membres devraient également envisager de créer, au sein des autorités centrales responsables de l'entraide judiciaire, des unités distinctes chargées de la cybercriminalité et servant de base de connaissances 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 pour renforcer les capacités, par exemple au moyen d'une formation visant à répondre aux besoins des autorités nationales et étrangères sur la manière de bénéficier rapidement et efficacement d'une entraide judiciaire concernant des preuves électroniques dans le cadre d'affaires de cybercriminalité.

36. 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 concernant des preuves électroniques, afin de garantir la mise en place de mécanismes d'évaluation de l'efficacité.

37. Il convient de rappeler aux États Membres qu'ils doivent faire appel aux autorités centrales pour transmettre les demandes d'entraide judiciaire et pour collaborer avec les autorités compétentes aux fins de l'exécution de telles demandes, afin de garantir le respect des traités existants et de réduire les délais.

Prévention

38. Il convient de reconnaître que la prévention n'est pas seulement la responsabilité des États, mais qu'elle exige la participation de toutes les parties prenantes, y compris les services de détection et de répression, le secteur privé, en particulier les fournisseurs d'accès à Internet, les organisations non gouvernementales, les écoles et les universités ainsi que le public en général.

39. Il a été recommandé que le public puisse aisément accéder à des outils de prévention tels que des plateformes en ligne, des clips audio, des infographies présentées dans un langage simple et des plateformes de signalement.

40. Il a été jugé nécessaire d'élaborer un ensemble de politiques publiques de prévention à long terme, qui devraient inclure des campagnes de sensibilisation sur l'utilisation sûre d'Internet.

41. Dans le cadre de leurs activités visant à prévenir et combattre la cybercriminalité, les États devraient accorder une attention particulière à la prévention et à l'éradication de la violence fondée sur le genre, en particulier la violence à l'égard des femmes et des filles, et des crimes de haine.

42. Les activités de prévention doivent être proactives, régulières, continues et adaptées aux groupes vulnérables.

43. Les États devraient dispenser une formation aux juges spécialisés chargés des affaires de cybercriminalité et fournir aux organismes d'enquête des outils performants pour tracer les cybermonnaies et lutter contre leur utilisation à des fins criminelles.

44. Il a été recommandé de renforcer les capacités collectives des institutions compétentes et, dans le domaine de la prévention, de passer d'une culture réactive à une culture proactive. Il a également été recommandé de mettre en place un mécanisme solide pour stimuler et faciliter l'échange de renseignements sur les modes opératoires possibles des délinquants.

45. Les États Membres sont encouragés à continuer d'adopter des mesures de prévention efficaces aux niveaux national et international et à se concentrer sur des activités proactives telles que la sensibilisation aux risques liés à la cybercriminalité, en axant ces campagnes sur des modes opératoires tels que l'hameçonnage (phishing) ou les logiciels malveillants (ransomware) et en ciblant différents groupes tels que les jeunes et les personnes âgées. Les États Membres sont également encouragés à continuer d'axer leurs efforts sur la probabilité de poursuivre et de punir les délinquants et sur la prévention de la criminalité par l'identification et l'interruption des activités illicites qui se déroulent en ligne. Les services de police et les ministères publics doivent investir dans des stratégies visant à signaler et à détecter les menaces de cybercriminalité et à intervenir. Les partenariats public-privé sont indispensables. Ces activités de prévention ne requièrent pas de lois ou de règlements supplémentaires.

46. Compte tenu de la « fracture numérique », certains pays en développement n'ont pas les moyens de prévenir, de détecter et de combattre la cybercriminalité et sont plus vulnérables face aux défis qu'elle pose.

47. L'ONUDC a été vivement encouragé à continuer de fournir une assistance technique aux États qui en font la demande, pour prévenir et combattre la cybercriminalité.

48. Les États Membres sont encouragés à continuer d'adopter des mesures de prévention efficaces aux niveaux national et international et à se concentrer sur des activités en amont, comme la sensibilisation aux risques liés à la cybercriminalité et aux probabilités de poursuites et de condamnation des auteurs de ces actes, ainsi que sur des efforts visant à prévenir la commission de nouvelles infractions en repérant et en entravant les activités illicites en cours sur Internet.

49. Les pays devraient collecter un large éventail de données afin de mieux comprendre les tendances et de définir des politiques et mesures opérationnelles de lutte contre la cybercriminalité.

50. Les efforts visant à élaborer des stratégies de prévention de la cybercriminalité devraient également tenir compte de la protection des droits humains.

51. Les stratégies nationales de lutte contre la cybercriminalité devraient en outre s'intéresser aux « capacités en matière de justice pénale ». Il faudrait accorder la priorité à l'aide aux pays en développement pour renforcer les capacités des services de détection et de répression en matière de prévention dans ce domaine.

52. Les États devraient mettre au point des programmes d'aide aux victimes de la cybercriminalité ou renforcer les programmes existants.

53. Les États devraient mener des enquêtes pour mesurer l'impact de la cybercriminalité sur les entreprises, y compris les mesures adoptées, la formation des employés, les types de cyberincidents auxquels elles doivent faire face et les coûts associés au relèvement à la suite de cyberincidents et à leur prévention.

54. Les États devraient aider les entreprises et les communautés à faire mieux connaître les risques liés à la cybercriminalité, à promouvoir des stratégies de réduction des risques et à améliorer les cyberpratiques, ces éléments pouvant avoir d'importants effets préventifs en aval.

55. Il faudrait étudier en détail les modes opératoires des cybercriminels contemporains en se fondant sur l'analyse du renseignement et la recherche criminologique, en vue d'utiliser plus efficacement les ressources existantes et de recenser les facteurs de vulnérabilité.

56. Les pays devraient envisager des mesures spécifiques et adaptées pour assurer la sécurité des enfants en ligne. Il s'agit notamment de garantir la mise en place de cadres juridiques nationaux, de dispositions pratiques et d'accords de coopération internationale pour faciliter le signalement et la détection des cas d'exploitation sexuelle et d'atteintes sexuelles visant des enfants en ligne, de mener des enquêtes à ce sujet, d'en traduire en justice les auteurs et de prévoir des mesures dissuasives.

57. Les entreprises sont un partenaire clef dans la prévention de la cybercriminalité. Les pays devraient envisager de mettre en œuvre des mécanismes de coopération avec elles, notamment en ce qui concerne le renvoi aux autorités nationales compétentes et le retrait de contenus illicites nuisibles, y compris le retrait de contenus liés à l'exploitation sexuelle des enfants et de contenus violents odieux.

58. Des avis réguliers sur la prévention des incidents devraient être publiés et communiqués aux utilisateurs, aux organisations et aux autres parties prenantes pour leur permettre de prévenir les cyberincidents susceptibles de déboucher sur des activités criminelles.

59. Les États devraient associer des femmes spécialistes à la prévention de la cybercriminalité et aux enquêtes menées dans ce domaine.

60. Les expériences nationales et régionales en matière de prévention devraient être rassemblées pour créer un répertoire multilatéral qui permettrait la diffusion des bonnes pratiques dans divers contextes.

61. Il faudrait sensibiliser davantage le public et fournir une assistance législative sur les cadres réglementaires applicables dans la lutte contre le cyberharcèlement et les menaces de violence ou d'abus en ligne.

62. Il a été recommandé aux États d'investir dans le renforcement des capacités afin d'améliorer les compétences des agents de l'ensemble du système de justice pénale, ce qui constitue une mesure préventive efficace et dissuasive contre la cybercriminalité.

63. L'ONUDC devrait faciliter la mise en commun des meilleures pratiques en matière de mesures préventives efficaces et fructueuses contre la cybercriminalité.