Nations Unies E/CN.15/2020/12

Conseil économique et social

Distr. générale
17 mars 2020
Français
Original : anglais

Commission pour la prévention du crime et la justice pénale
Vingt-neuvième session
Vienne, 18-22 mai 2020
Point 6 d) de l'ordre du jour provisoire*
Intégration et coordination de l'action de l'Office des Nations Unies contre la drogue et le crime et des États Membres dans le domaine de la prévention du crime et de la justice pénale : autres questions liées à la prévention du crime et à la justice pénale

Favoriser l'assistance technique et le renforcement des capacités pour intensifier l'action nationale et la coopération internationale contre la cybercriminalité, y compris l'échange d'informations

Rapport du Secrétaire général

Résumé

Le présent rapport a été établi conformément à la résolution 74/173 de l'Assemblée générale, intitulée « Favoriser l'assistance technique et le renforcement des capacités pour intensifier l'action nationale et la coopération internationale contre la cybercriminalité, y compris l'échange d'informations », dans laquelle l'Assemblée a prié le Secrétaire général de rendre compte à la Commission pour la prévention du crime et la justice pénale, à sa vingt-neuvième session, de l'application de cette résolution.

Le rapport décrit les progrès accomplis en 2019 par l'Office des Nations Unies contre la drogue et le crime pour ce qui est de favoriser et de mettre en œuvre l'assistance technique et le renforcement des capacités en vue d'intensifier l'action nationale et la coopération internationale contre la cybercriminalité, y compris l'échange d'informations.

* E/CN.15/2020/1.

V.20-01891 (F) 170420 200420

Merci de recycler

I. Introduction

1. Dans sa résolution 64/179, adoptée en 2009, l'Assemblée générale a appelé l'attention sur le fait que la cybercriminalité était un nouveau problème relevant des pouvoirs publics, concernant en particulier les activités de coopération technique de l'Office des Nations Unies contre la drogue et le crime (ONUDC), et elle a invité celui-ci à rechercher, dans le cadre de son mandat, les moyens de s'y attaquer.

2. En 2010, dans sa résolution 65/230, l'Assemblée générale a prié l'ONUDC de viser, lorsqu'il concevait et exécutait ses programmes d'assistance technique, l'obtention de résultats viables et durables en matière de prévention du crime et de poursuite et châtiment des délinquants, en particulier grâce à la mise en place de systèmes de justice pénale et à la modernisation et au renforcement des systèmes existants, ainsi qu'à la promotion de l'état de droit, et de concevoir ces programmes de telle sorte que ces objectifs soient atteints pour toutes les composantes du système de justice pénale, de manière intégrée et dans une perspective à long terme, de façon à renforcer la capacité des États demandeurs de prévenir et réprimer les différents types de criminalité qui sévissent dans les sociétés, notamment la criminalité organisée et la cybercriminalité.

3. En 2001, dans sa résolution 20/7, la Commission pour la prévention du crime et la justice pénale a prié l'ONUDC, en coopération avec les États Membres, les organisations internationales et régionales compétentes et, le cas échéant, le secteur privé, de continuer à fournir aux États en faisant la demande une assistance technique et une formation adaptées aux besoins nationaux, portant en particulier sur la prévention et la détection de la cybercriminalité sous toutes ses formes.

4. En outre, en 2013, dans sa résolution 22/8, la Commission pour la prévention du crime et la justice pénale a invité l'ONUDC à progresser dans la mise en œuvre du Programme mondial contre la cybercriminalité, et l'a prié de resserrer les partenariats portant sur l'assistance technique et le renforcement des capacités pour lutter contre la cybercriminalité avec les États Membres, les organisations compétentes, le secteur privé et la société civile.

5. En 2019, dans sa résolution 74/173, l'Assemblée générale a prié l'ONUDC de continuer à fournir aux États Membres, sur demande et en fonction de leurs besoins nationaux, une assistance technique et des services de renforcement durable des capacités pour les aider à faire face à la cybercriminalité, par l'intermédiaire du Programme mondial contre la cybercriminalité et, entre autres, de ses bureaux régionaux, en ce qui concerne la prévention, la détection, les enquêtes et les poursuites visant la cybercriminalité sous toutes ses formes, sachant que la coopération avec les États Membres, les organisations internationales et régionales compétentes, le secteur privé, la société civile et les autres parties prenantes pouvait faciliter cette activité.

6. En conséquence, l'ONUDC – principalement dans le cadre de son programme mondial contre la cybercriminalité – fournit aux États Membres, aux niveaux national, régional et mondial, des services d'assistance technique et de renforcement des capacités en matière de cybercriminalité. Il fait aussi office de secrétariat technique pour le Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité. L'action de prévention contre la cybercriminalité est également soutenue dans une large mesure par le Programme mondial de l'ONUDC pour la mise en œuvre de la Déclaration de Doha, à travers son initiative Éducation pour la justice.

7. Dans la planification et la mise en œuvre de ses activités de lutte contre la cybercriminalité, l'ONUDC coopère étroitement avec différents partenaires et forums clefs en matière de cybercriminalité, auxquels il fournit également conseils et orientations, notamment l'Organisation internationale de police criminelle (INTERPOL), l'Union internationale des télécommunications, l'Agence de l'Union européenne pour la coopération en matière de répression des services répressifs, le Groupe européen de formation et d'enseignement sur la cybercriminalité, la Banque mondiale, le Fonds des Nations Unies pour l'enfance (UNICEF), l'Association des

nations de l'Asie du Sud-Est (ASEAN), la Conférence mondiale sur Internet, le Partenariat mondial pour l'élimination de la violence envers les enfants et le Forum mondial sur la cyberexpertise.

8. En 2019, l'ONUDC a continué d'apporter un soutien global aux États Membres pour les activités de prévention, de détection, d'enquête et de poursuite engagées contre la cybercriminalité sous toutes ses formes, en tenant dûment compte des droits humains et des libertés fondamentales dans l'utilisation des technologies de l'information et des communications. Cela inclut notamment des efforts visant à obtenir et à exploiter de manière proportionnée, légale et responsable les preuves criminalistiques numériques existantes.

9. Tout au long de la période considérée, et suivant les priorités fixées dans la Stratégie du Secrétaire général en matière de nouvelles technologies, l'ONUDC a continué de contribuer aux travaux de l'Assemblée générale, du groupe de travail sur les cybermonnaies de l'UNICEF et du Groupe de haut niveau sur la coopération numérique. En outre, l'Office a régulièrement fourni des orientations et des conseils au sujet des conséquences de la cybercriminalité sur la cybersécurité, la paix et la sécurité.

II. Évolution de la situation, progrès accomplis et meilleures pratiques recensées

10. Conformément à la résolution 73/187 de l'Assemblée générale, relative à la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, le Secrétaire général a présenté un rapport (A/74/130) exposant les vues des États Membres quant aux difficultés qu'ils rencontrent dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles. Ce rapport rendait compte des communications de 61 États Membres, reproduites sous la forme de résumés établis par le Secrétariat. Les contributions des États Membres portaient sur les difficultés rencontrées aux niveau national et international, ainsi que sur les mesures adoptées pour y remédier. Les États Membres y décrivaient aussi les obstacles techniques et technologiques auxquels ils se heurtaient et expliquaient ce qu'ils faisaient pour les surmonter. Ils soulignaient également l'importance de la coopération internationale dans la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles.

11. L'ONUDC a suivi le processus d'adoption de la résolution 74/247 de l'Assemblée générale, relative à la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, qui inclue un mandat visant l'établissement d'un comité intergouvernemental spécial d'experts à composition non limitée, représentatif de toutes les régions et 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. Dans cette perspective, l'ONUDC fournira un appui technique et administratif à la session d'organisation du comité, qui doit se tenir à New York en août 2020.

III. Appui normatif et soutien au renforcement des capacités

12. Les mentors spécialisés en cybercriminalité, qui sont en poste en Autriche, en El Salvador, au Guatemala, au Kenya, au Sénégal et en Thaïlande, ont continué d'aider les pays à lutter contre les infractions commises ou facilitées par Internet et à exploiter et échanger des preuves électroniques. En outre, en 2019, l'ONUDC a poursuivi ses efforts de renforcement des capacités pour répondre aux besoins des pays en développement, en mettant l'accent sur les vulnérabilités qu'ils avaient eux-mêmes identifiées afin de fournir une assistance technique adaptée et de favoriser l'échange de connaissances aussi actualisées que possible. Cette démarche a permis

d'apporter aux agents des services de détection et de répression des États Membres les conseils nécessaires, en matière de planification tactique et opérationnelle, pour avoir une réelle influence aux niveaux local, régional et international.

13. Au Moyen-Orient et en Afrique du Nord, dans le cadre d'un projet régional axé sur les capacités à prévenir et combattre la cybercriminalité et à développer la criminalistique numérique, les mentors de l'ONUDC pour la cybercriminalité en poste au Caire ont continué de fournir un appui à l'Algérie, à l'Égypte, à la Jordanie, au Liban, à la Libye, au Maroc, au Soudan, à la Tunisie et à l'État de Palestine, avec des activités qui ont inclus :

a) La conduite, en collaboration avec des experts nationaux et internationaux, d'un examen d'ensemble destiné à recenser les dispositions juridiques régissant la prévention et la répression de la cybercriminalité, y compris dans des sources de droit dérivé, des règlements et des directives ;

b) Le développement des supports de formation et des connaissances spécialisées de l'ONUDC, ainsi que l'élaboration et la mise à disposition des services de police scientifique de modules de formation consacrés à la collecte de preuves électroniques ;

c) La conduite, dans certains États, d'évaluations sur le degré actuel de sensibilisation de l'opinion publique et sur le niveau de signalement des faits de cybercriminalité ;

d) La fourniture de conseils techniques concernant la mise en place d'un système de points de contact pour les services responsables de l'entraide judiciaire et de l'extradition au sein des ministères de la justice de différents pays ;

e) L'acquisition et la livraison d'un matériel criminalistique de triage des données numériques.

14. Par ailleurs, afin de proposer des services de renforcement des capacités et de soutien technique qui tiennent compte des besoins recensés, l'ONUDC a procédé, sur demande, à une évaluation complète des capacités de détection et de répression et des moyens d'action judiciaire contre la cybercriminalité au Costa Rica, en Ouganda, au Pakistan et au Pérou. Les autorités de ces pays ont reçu les rapports d'évaluation, dans lesquels figuraient des recommandations visant à faciliter l'élaboration et la mise en œuvre de politiques et de mesures spécifiques contre la cybercriminalité. Au Costa Rica, compte tenu de l'évaluation de l'ONUDC, le Bureau du Procureur général a commencé à envisager la possibilité de mettre en place une unité spécialisée en matière de cybercriminalité. Les besoins en matière de formation des services de détection et de répression et des praticiens de la justice pénale ont en outre été recensés dans le pays, et des activités de renforcement des capacités ont été planifiées pour 2020.

15. Chacun des États membres de l'ASEAN a mis en place, avec le soutien de l'ONUDC, un mécanisme national intégré de coordination, de coopération et d'échange d'informations sur les questions de cybercriminalité, intitulé « Table ronde nationale sur la cybercriminalité ». Ce mécanisme a été conçu pour aider les autorités nationales compétentes à collaborer et à favoriser la coopération interinstitutions en matière de cybercriminalité, de criminalistique numérique et de cybermonnaies. L'ONUDC contribue ainsi à rapprocher les entités publiques et privées concernées pour qu'elles examinent les questions et difficultés qui se posent en matière de cybersécurité, de cybercriminalité et de criminalistique numérique, ainsi que les mesures que chacune d'elles pourrait prendre pour y remédier. Ces discussions, qui servent de cadre à l'échange d'informations et de bonnes pratiques, fournissent à l'ONUDC les informations nécessaires à l'élaboration des programmes d'assistance technique qu'il consacre à la cybercriminalité au niveau national et dans l'ensemble de l'Asie du Sud-Est.

Enquêtes sur la cybercriminalité et criminalistique numérique

16. Dans sa résolution 74/173, l'Assemblée générale a encouragé les États Membres à élaborer et à adopter des mesures pour assurer au niveau national l'efficacité des enquêtes et des poursuites relatives aux affaires de cybercriminalité et aux infractions dans lesquelles les preuves électroniques jouaient un rôle important et garantir une coopération internationale efficace à cet égard, dans le respect du droit interne et conformément au droit international applicable, notamment aux instruments internationaux relatifs aux droits humains applicables.

17. Dans la même résolution, l'Assemblée a prié instamment les États Membres d'encourager la formation des agents des services de détection et de répression, des autorités chargées des enquêtes, des procureurs et des juges dans le domaine de la cybercriminalité, notamment en leur permettant d'acquérir les compétences nécessaires en matière de collecte de preuves et de technologies de l'information, et de leur donner les moyens de s'acquitter efficacement de leurs rôles respectifs dans les enquêtes, les poursuites et les jugements ayant trait à la cybercriminalité.

18. Au cours de la période considérée, l'ONUDC a formé 1 817 praticiens de la justice pénale de 36 pays dans les domaines suivants : mesures de lutte contre l'exploitation sexuelle des enfants en ligne ; utilisation de matériel informatique et de logiciels spécialisés ; manipulation et analyse criminalistique de preuves numériques ; recours à des outils de renseignement de source ouverte ; coopération internationale ; droit relatif à la cybercriminalité ; renseignement en matière de cybermenaces ; cybermonnaies ; enquêtes sur le darknet ; enquêtes en ligne sur la criminalité liée aux espèces sauvages ; renseignement relatif aux cybermenaces dans les opérations de lutte contre le terrorisme ; et enquêtes sur les logiciels malveillants.

19. Dans le cadre de ces activités, environ 85 agents des services de détection et de répression de l'Érythrée, de l'Éthiopie, du Kenya, de l'Ouganda et de la République-Unie de Tanzanie ont été formés à l'exploitation de preuves numériques et aux techniques d'enquête en ligne. En association avec INTERPOL, l'ONUDC a également formé 19 agents de police de toute l'Afrique à des techniques perfectionnées d'enquête sur les logiciels malveillants. Au Kenya, du matériel spécialisé de criminalistique numérique a été fourni aux services de police, qui ont également bénéficié d'un accompagnement dans les domaines de la criminalistique numérique et des techniques de triage. Le matériel et l'appui ainsi fournis aident les services de police à se concentrer sur les éléments de preuve essentiels et à obtenir les meilleurs résultats possibles avec un minimum de ressources. De plus, en coopération avec INTERPOL et l'Organisation de coopération des chefs de police de l'Afrique de l'Est (EAPCCO), l'ONUDC a commencé l'élaboration du manuel de l'EAPCCO sur les enquêtes relatives à la cybercriminalité.

20. En Amérique centrale, en coopération avec le Ministère de la justice des États-Unis d'Amérique et le Conseil national de la magistrature d'El Salvador, l'ONUDC a formé plus de 200 juges salvadoriens à la lutte contre la cybercriminalité et au traitement des preuves électroniques, élaborant également à l'intention des magistrats des lignes directrices sur la recevabilité des preuves numériques devant les tribunaux. De plus, les procureurs, enquêteurs et analystes en criminalistique numérique d'Amérique latine ont bénéficié d'un renforcement de leurs capacités pour l'exploitation de renseignements de source ouverte, l'obtention de preuves électroniques à l'étranger et d'autres aspects des enquêtes et des poursuites relatives à la cybercriminalité. Des équipements de protection contre l'intrusion à distance ont été fournis à l'unité de la Police nationale civile d'El Salvador chargée de la cybercriminalité, ce qui rend le Gouvernement mieux à même de promouvoir la bonne gouvernance et l'état de droit. Au Guatemala, deux unités régionales d'assistance technique (laboratoires de criminalistique numérique), qui relèvent de la Direction des enquêtes criminelles du Bureau du Procureur général, ont été constituées, équipées et formées, permettant au ministère public de conduire des enquêtes rapides et efficaces. Le délai de réaction institutionnelle, qui était auparavant de deux mois, a été réduit à moins de 10 jours grâce à la création de ces unités.

21. En Asie du Sud-Est, une formation sur les enquêtes relatives à la cybercriminalité a été dispensée à des formateurs de cinq États membres de l'ASEAN (Indonésie, Malaisie, Philippines, Thaïlande et Viet Nam), afin qu'ils soient capables de concevoir et de dispenser des programmes de formation à l'intention des services de détection et de répression et des institutions de justice pénale de leurs pays respectifs. En République démocratique populaire lao, l'ONUDC a aidé les forces de police à constituer et à former le personnel du tout premier laboratoire de criminalistique numérique. Cela a eu pour conséquence immédiate de protéger l'État des risques de criminalité fondée sur Internet ou facilitée par le réseau, puisque les autorités ont désormais les moyens de répondre à ces menaces quel que soit le type de criminalité ou de terrorisme concerné, en se conformant à un cadre général fondé sur les droits humains. Ainsi, l'ONUDC a contribué à renforcer la coopération internationale et à atténuer les menaces. En outre, des rencontres de niveau ministériel organisées en Chine, notamment à l'occasion de la Conférence mondiale sur Internet, ont favorisé les partenariats public-privé dans toute l'Asie. Cela a créé les conditions d'une collaboration plus facile et plus efficace entre les services de détection et de répression et les entreprises spécialisées dans les technologies, l'objectif étant de veiller à ce que les preuves numériques soient bien préservées et mises à disposition, dans les délais voulus.

Enquêtes sur les cybermonnaies et le darknet

22. Au cours de la période considérée, l'ONUDC a fourni des conseils pour les politiques gouvernementales de lutte contre la criminalité associée aux cybermonnaies, ainsi qu'à l'appui des travaux du Groupe d'action financière sur les actifs virtuels. Les outils de formation en ligne de l'ONUDC aident les décideurs à mieux comprendre la menace et la nécessité d'y faire face au moyen d'une politique cohérente, ce qui est particulièrement important compte tenu de l'augmentation de la criminalité, du terrorisme et des probables activités de prolifération concordant avec les intérêts d'États qui sont facilitées par les cybermonnaies.

23. Au niveau régional, l'Asie du Sud-Est a continué de renforcer les capacités des praticiens impliqués dans les enquêtes sur les cybermonnaies, en s'appuyant sur la stratégie de formation des formateurs mise en œuvre par l'ONUDC. Cette approche a permis aux États Membres de mieux prendre conscience de la menace, et a contribué au développement d'une capacité de réaction cohérente en matière de détection et de répression. Les pays de l'ASEAN, sous la conduite de l'ONUDC, analysent les législations et cadres nationaux relatifs aux cybermonnaies ainsi que la façon dont ils pourraient être utilisés contre le blanchiment d'argent, le financement du terrorisme et d'autres activités criminelles. Ce processus a conduit la Thaïlande à rédiger de nouvelles réglementations sur l'utilisation et les opérations de change de cybermonnaies.

24. Les autorités des États membres de l'ASEAN ont également commencé à constituer et à renforcer des unités d'enquête sur les cybermonnaies, chargées de localiser et de saisir les avoirs détenus sous cette forme. Par exemple, comme suite directe au renforcement des capacités assuré par l'ONUDC, l'unité malaisienne d'enquête sur les cybermonnaies a élargi son personnel de 2 à 16 enquêteurs, permettant ainsi des améliorations à long terme et auto-entretenues en matière d'organisation stratégique. Deux autres pays de l'ASEAN sont actuellement engagés dans la mise en place d'unités de ce genre, tirant profit des services de mentorat de l'ONUDC pour mener à bien ce processus.

25. En outre, des lignes directrices pour la saisie de cybermonnaies ont été rédigées par un groupe de travail spécialisé constitué d'experts des pays de l'ASEAN, d'organisations internationales et d'entreprises privées. Ces lignes directrices, qui ne peuvent être consultées que par des acteurs certifiés de la justice pénale, sont souples et adaptables à l'évolution du marché des cybermonnaies.

26. En 2019, plus de 200 agents de services de détection et de répression, des autorités de banques centrales, de services de renseignement financier et de ministères

publics d'Asie du Sud-Est et de Chine ont reçu une formation pratique sur les enquêtes relatives aux cybermonnaies et au darknet. Les conseils tactiques que l'ONUDC a fournis dans le prolongement direct de cette formation ont aidé à prendre des mesures en réponse à différentes affaires d'enlèvement en Asie du Sud-Est.

Exploitation et atteintes sexuelles visant les enfants sur Internet

27. Dans sa résolution 74/174, l'Assemblée générale a prié l'ONUDC d'aider les États Membres qui le demandaient à élaborer et mettre en œuvre des mesures visant à améliorer l'accès à la justice et à la protection, y compris par des mesures législatives et autres en faveur des enfants victimes d'exploitation et d'atteintes sexuelles sur Internet, en prévoyant des procédures adaptées aux enfants et tenant compte des questions de genre, afin de leur donner accès rapidement et équitablement à des voies de recours en cas de violation de leurs droits. Elle a également encouragé les États Membres à fournir des ressources à l'ONUDC, notamment au Programme mondial contre la cybercriminalité, afin de lutter contre l'exploitation et les atteintes sexuelles visant les enfants sur Internet.

28. Au Kenya, le mentor de l'ONUDC en matière de cybercriminalité a organisé des sessions régulières au sein de l'Unité de lutte contre la traite des personnes et de protection de l'enfance, qui relève de la Direction des enquêtes criminelles. Ces activités de formation ont porté essentiellement sur les preuves électroniques et la criminalistique numérique. L'ONUDC a également soutenu l'opération Safisha, lancée par l'Unité de lutte contre la traite des personnes et de protection de l'enfance pour s'attaquer à la maltraitance des enfants sur Internet.

29. En Amérique latine, en partenariat avec INTERPOL et le Centre international pour les enfants disparus et exploités, l'ONUDC a formé plus de 250 praticiens de la justice pénale de la Barbade, du Belize, du Chili, du Costa Rica, d'El Salvador, du Honduras, du Panama et du Pérou à la conduite d'enquêtes relatives à l'exploitation sexuelle des enfants sur Internet. Des organisations non gouvernementales contribuant à promouvoir et à défendre les droits des enfants au Costa Rica ont été informées de la manière dont les cybercriminels utilisaient les technologies de l'information et des communications pour gagner la confiance des enfants et, à terme, leur faire subir des sévices sexuels et les exploiter sexuellement. Comme suite à des échanges continus qui avaient été engagés, avec l'appui de l'ONUDC, entre les autorités costariciennes, le Centre international pour les enfants disparus et exploités et Facebook, le Gouvernement s'est engagé à prendre des mesures pour mettre en œuvre le mécanisme Cybertip, administré par le National Center for Missing and Exploited Children, afin de signaler les cas d'exploitation et d'atteintes sexuelles visant des enfants sur Internet. Au Belize, l'ONUDC s'est entretenu avec les autorités pour recommander que le Code pénal soit modifié de manière à incriminer les infractions commises avec l'aide d'Internet contre les femmes et les enfants.

30. Par ailleurs, toujours en Amérique latine, une équipe spéciale chargée d'identifier les victimes a été créée en collaboration avec INTERPOL. Onze pays (Argentine, Brésil, Chili, Colombie, Costa Rica, El Salvador, Équateur, Guatemala, Honduras, Mexique et Pérou) ont collaboré pour identifier 66 enfants et 14 délinquants, grâce à l'exploitation efficace de la base de données internationale sur l'exploitation sexuelle des enfants.

31. En Asie du Sud-Est, l'ONUDC a aidé six pays (Cambodge, Malaisie, Myanmar, République démocratique populaire lao, Thaïlande et Viet Nam) à renforcer les mesures multisectorielles prises au niveau national pour prévenir et combattre l'exploitation et les atteintes sexuelles visant des enfants sur Internet.

Utilisation d'Internet à des fins terroristes

32. L'utilisation d'Internet à des fins terroristes reste l'une des activités criminelles posant les plus grandes difficultés aux praticiens de la justice pénale et aux enquêteurs au moment d'ouvrir et de mener les enquêtes et les poursuites qui s'ensuivent.

33. À cet égard, l'ONUDC a apporté son aide aux États Membres en concevant et en dirigeant des exercices régionaux de collaboration en matière de renseignement sur les cybermenaces pour l'adoption de mesures conjointes contre la cybercriminalité et le terrorisme, ce qui a permis de renforcer les synergies sur ces questions aux niveaux national et international.

34. Grâce aux exercices conjoints de formation organisés entre l'ONUDC, INTERPOL et l'Union européenne, avec la participation de plusieurs partenaires du secteur privé, une soixantaine de praticiens exerçant en première ligne dans 12 pays d'Afrique de l'Est ont été formés à des techniques reposant sur l'exploitation de renseignements de source ouverte pour enquêter sur les suites d'incidents terroristes. Pour les praticiens de la justice pénale, ces activités ont également été l'occasion de nouer des liens de coopération informelle avec leurs homologues régionaux.

35. Une quarantaine d'enquêteurs financiers, d'agents des services de détection et de répression et de représentants d'organisations à but non lucratif de Maurice ont reçu une formation sur les liens existant entre les médias sociaux et la radicalisation et l'infiltration d'organisations à but non lucratif par des groupes terroristes.

36. À la demande de l'Unité de police antiterroriste du Kenya et dans le cadre d'un accompagnement continu, le mentor de l'ONUDC en matière de cybercriminalité a contribué à l'enquête sur les suites de l'attentat perpétré à l'hôtel Dusit en fournissant du matériel et des conseils opérationnels pour permettre un examen plus efficace des appareils numériques qui avaient été saisis.

37. En Asie du Sud et du Sud-Est, les capacités de plus de 200 praticiens de la justice pénale à prévenir les cyberattaques organisées par des terroristes et à enquêter sur ces derniers ont été renforcées. Les intéressés ont été formés aux moyens de chercher, de rassembler et d'analyser des renseignements de source ouverte et de suivre la trace de groupes criminels organisés et de terroristes sur le darknet, ainsi qu'à d'autres techniques spécialisées en matière d'enquêtes sur la cybercriminalité.

Coopération internationale pour l'obtention de preuves électroniques

38. Les 10 et 11 décembre 2019, dans le cadre de l'initiative mondiale visant à renforcer la capacité des autorités centrales et des procureurs et enquêteurs chargés de lutter contre le terrorisme à obtenir des preuves numériques auprès des fournisseurs de services de communication privés dans le cadre d'enquêtes transnationales, en particulier en matière de lutte contre le terrorisme, l'ONUDC, la Direction exécutive du Comité contre le terrorisme et l'Association internationale des procureurs et poursuivants ont organisé conjointement à Washington un atelier spécialisé entièrement consacré à l'obtention de preuves électroniques au moyen des mécanismes d'entraide judiciaire, suivant le *Guide pratique sur la demande de preuves électroniques à l'étranger*, publié en 2019. Cet atelier a permis aux praticiens présents (parmi lesquels des magistrats de liaison en poste aux États-Unis, des procureurs nationaux et représentants d'autorités centrales, des représentants du Ministère de la justice des États-Unis et des experts techniques) d'examiner les aspects pratiques de la coopération et les obstacles restant à surmonter, mais aussi de recenser et de mettre en commun les bonnes pratiques suivies pour contribuer au traitement rapide des demandes d'entraide judiciaire impliquant les États-Unis, avec l'objectif de renforcer l'efficacité des enquêtes et des poursuites relatives au terrorisme et à d'autres formes graves de criminalité dans le monde.

IV. Échange d'informations

39. Dans sa résolution 74/173, l'Assemblée générale a réaffirmé que, conformément à la résolution 22/8 de la Commission pour la prévention du crime et la justice pénale, en date du 26 avril 2013, l'ONUDC avait pour rôle de centraliser les données sur les lois et les enseignements relatifs à la cybercriminalité afin de faciliter l'évaluation

continue des besoins et des capacités de la justice pénale ainsi que la prestation et la coordination de l'assistance technique.

40. En 2019, l'ONUDC a poursuivi son travail consistant à inclure des ressources relatives à la cybercriminalité dans le portail de gestion des connaissances pour la mise en commun de ressources électroniques et de lois contre la criminalité. En janvier 2020, le portail contenait plus de 1 300 textes de loi sur la cybercriminalité ainsi que 39 cas de jurisprudence relatifs à des infractions commises ou facilitées par Internet, qui illustraient les liens entre la cybercriminalité et d'autres types d'infractions telles que la participation à un groupe criminel organisé, le blanchiment d'argent et le trafic de drogues.

41. L'ONUDC a également continué de s'appuyer sur les médias sociaux pour diffuser des informations relatives au cyberespace et accroître considérablement la visibilité de ses travaux auprès du grand public. Ces efforts se sont traduits par plus de 2,8 millions d'impressions Twitter et par une reconnaissance accrue des travaux de l'Office.

V. Recherche et analyse

42. En 2019, l'ONUDC a lancé des travaux de recherche sur les menaces associées au darknet en Asie du Sud-Est. Ces travaux se poursuivaient en 2020, et l'Office sera en mesure de fournir de plus amples informations à ce sujet vers la fin de l'année.

VI. Prévention

43. Au début de l'année 2019 a été achevée une série de modules universitaires sur la cybercriminalité [1], qui est l'aboutissement d'une collaboration engagée entre d'éminents experts et universitaires issus de plus de 25 pays de six continents différents, ainsi qu'avec INTERPOL et le Haut-Commissariat des Nations Unies aux droits de l'homme. Conçue dans le cadre de l'initiative Éducation pour la justice du Programme mondial pour la mise en œuvre de la Déclaration de Doha, cette série est constituée d'un guide pédagogique et de 14 modules. Lors des ateliers organisés par l'ONUDC pour promouvoir l'utilisation de la série de modules universitaires sur la cybercriminalité, des professeurs d'université d'Afrique, d'Europe et d'Asie occidentale et centrale ont pu se familiariser davantage avec ces modules, qu'ils ont appris à adapter et à intégrer dans des cours nouveaux ou préexistants. L'ONUDC a ainsi fourni à des professeurs de 40 universités, dans 25 pays et sur cinq continents, les moyens de préparer pour l'année universitaire 2019-2020 des cours complets et interdisciplinaires sur la cybercriminalité. Sur la base de la série de modules élaborée par l'ONUDC, plus de 7 200 étudiants du monde entier ont pu être sensibilisés à divers aspects de la cybercriminalité. La compréhension des principales questions relatives à la cybercriminalité aidera les jeunes, qui sont les futurs décideurs politiques, praticiens de la justice pénale et spécialistes des technologies de l'information, à élaborer des solutions efficaces pour rendre le monde plus sûr contre la criminalité, aussi bien en ligne que hors ligne.

44. L'ONUDC, dans le cadre de son initiative Éducation pour la justice et en coopération avec d'éminents experts de l'éducation, a mis au point des outils d'apprentissage innovants sur des sujets tels que la sécurité en ligne et la cybercriminalité, notamment des vidéos animées, des jeux informatiques et non électroniques et des bandes dessinées, qui sont adaptés aux établissements d'enseignement primaire et secondaire. Les vidéos et les bandes dessinées sont accompagnées d'un manuel pédagogique et de programmes de cours pour aider les enseignants à exploiter ces outils en classe. Tout au long de l'année, l'ONUDC a sensibilisé l'opinion publique, les praticiens et les décideurs du monde entier à la

[1] Disponible à l'adresse : https://www.unodc.org/e4j/fr/tertiary/cybercrime.html.

cybercriminalité, en faisant un usage actif des médias sociaux, sur lesquels il a cumulé plusieurs millions d'impressions et d'échanges. Le Programme mondial contre la cybercriminalité compte 8 110 abonnés et, avec une moyenne de 220 tweets par mois, il a cumulé 2,5 millions d'impressions Twitter ; comme conséquence directe de cette activité, différentes personnes ont sollicité des conseils après avoir été victimes de la cybercriminalité, ou fait part de leur reconnaissance concernant l'action menée par l'ONUDC contre ce phénomène. Les coordonnateurs résidents des Nations Unies, les diplomates et les autorités des États Membres ont contacté l'ONUDC pour solliciter des conseils et des informations sur les politiques relatives à la cybercriminalité.

45. Au Guatemala et en El Salvador, l'ONUDC a aidé les ministères de l'éducation à concevoir, adopter et mettre en œuvre dans les établissements scolaires une stratégie de prévention de la cybercriminalité. Cette stratégie incluait une formation spécialisée en vue d'une campagne de sensibilisation, ainsi que l'élaboration de deux notes d'orientation à l'intention des enseignants sur la manière d'aborder la prévention de la cybercriminalité. Les deux ministères ont introduit dans leurs activités régulières des mesures visant à prévenir la cybercriminalité, en ciblant non seulement les élèves mais aussi les enseignants. Le Ministère de l'éducation d'El Salvador a précisé que cette stratégie avait concerné 3 222 enseignants, 37 361 étudiants et 12 511 parents, tandis que celui du Guatemala a indiqué qu'il avait touché 188 477 étudiants et 9 042 enseignants.

46. Des expositions permanentes sur la cybercriminalité ont été imaginées, préparées et lancées aux musées des enfants du Guatemala et d'El Salvador. Élaborées en coordination avec l'initiative Éducation pour la justice, ces expositions ont été conçues pour faire connaître et promouvoir les droits des enfants sur Internet, à travers une série de 10 droits et devoirs relatifs aux technologies de l'information et des communications et dans le cadre d'un jeu de réalité virtuelle soulignant l'importance d'adopter une démarche responsable en matière d'accès et de recours aux technologies de l'information et des communications à des fins informatives et récréatives. Des partenariats ont été noués avec des entreprises privées telles que Telefónica, ainsi qu'avec l'organisation à but non lucratif Fundación Azteca et une station de radio, afin de promouvoir la prévention de la cybercriminalité en El Salvador et au Guatemala.

VII. Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité

47. De par ses fonctions d'appui technique et de secrétariat, l'ONUDC contribue aux travaux du Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité et aux mesures prises par les États Membres, la communauté internationale et le secteur privé, y compris en matière d'échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, afin d'examiner les options envisageables pour renforcer les mesures juridiques ou autres prises à l'échelle nationale et internationale face à la cybercriminalité et pour en proposer de nouvelles. Le Groupe d'experts a été créé par la Commission pour la prévention du crime et la justice pénale en application de la résolution 65/230 de l'Assemblée générale, dans laquelle cette dernière a fait sienne 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, qui avait été adoptée par le douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale. Le mandat du Groupe d'experts a été renouvelé 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, qui a été adoptée par le 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.

48. Le Groupe d'experts a tenu au total cinq réunions, en 2011, 2013, 2017, 2018 et 2019, et sa sixième réunion aura lieu du 6 au 8 avril 2020. Dans sa résolution 26/4, la Commission pour la prévention du crime et la justice pénale a prié le Groupe d'experts de poursuivre ses travaux. Sur la base d'un plan de travail structuré, l'objectif est de formuler un ensemble de recommandations devant être examinées lors d'une réunion de bilan qui se tiendra au plus tard en 2021, en vue d'établir une liste récapitulative et complète des conclusions et recommandations adoptées qui sera soumise à la Commission pour la prévention du crime et la justice pénale.

49. La cinquième réunion du Groupe d'experts, qui s'est tenue du 27 au 29 mars 2019, a été consacrée aux activités de détection et de répression, aux enquêtes, aux preuves électroniques et à la justice pénale. Lors de cette réunion, le Groupe d'experts a été informé du succès d'actions entreprises au niveau national pour appliquer des mesures juridiques et procédurales face à la cybercriminalité, élaborer et mettre en œuvre des stratégies et politiques en matière de cybersécurité, promulguer et améliorer la législation sur la cybercriminalité, mettre en place de nouveaux outils d'enquête qui permettraient de rassembler des preuves électroniques et d'établir leur authenticité pour qu'elles servent d'éléments de preuve dans les procédures pénales, et mettre en œuvre des dispositions institutionnelles visant à assurer une utilisation plus efficace des ressources destinées à lutter contre la cybercriminalité. La nécessité de disposer de pouvoirs procéduraux appropriés pour obtenir des preuves électroniques a été soulignée, de même que les problèmes liés aux conflits de compétence territoriale. 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 humains fondamentaux, en particulier le droit à la vie privée. Le Groupe d'experts était d'avis que la priorité devait être accordée au renforcement durable des capacités au sein des systèmes nationaux de détection et de répression et de justice pénale, en ce qu'elles étaient indispensables pour améliorer les compétences nationales et permettre l'échange de bonnes pratiques d'enquête, de données d'expérience, et de nouvelles techniques.

50. Dans sa résolution 74/173, l'Assemblée générale a, entre autres choses, estimé qu'il importait que le Groupe d'experts continue 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 pour lutter contre la cybercriminalité et d'en proposer de nouvelles ; noté avec satisfaction que le Groupe d'experts formulerait, conformément à son plan de travail pour la période 2018-2021, d'éventuelles conclusions et recommandations qu'il présenterait à la Commission pour la prévention du crime et la justice pénale ; reconnu que le Groupe d'experts offrait un espace de choix pour 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 pour lutter contre la cybercriminalité et d'en proposer de nouvelles ; prié l'ONUDC de continuer à recueillir périodiquement des informations sur l'évolution de la situation, les progrès accomplis et les meilleures pratiques recensées et de rendre compte périodiquement de ces informations au Groupe d'experts et à la Commission ; et invité le Groupe d'experts à fournir, sur la base de ses travaux, des conseils à l'ONUDC, y compris en ce qui concerne le Programme mondial contre la cybercriminalité, afin de l'aider, sans préjudice d'autres questions relevant de son propre mandat, à recenser les besoins urgents en matière de renforcement des capacités et les mesures à prendre pour y répondre efficacement, sans porter atteinte au rôle de la Commission en sa qualité d'organe directeur du programme contre le crime de l'Office.