Nations Unies E/CN.15/2013/24

Conseil économique et social

Distr. générale
5 mars 2013
Français
Original: anglais

Commission pour la prévention du crime et la justice pénale
Vingt-deuxième session
Vienne, 22-26 avril 2013
Point 7 de l'ordre du jour provisoire*
Tendances de la criminalité dans le monde et nouvelles questions et mesures prises dans le domaine de la prévention du crime et de la justice pénale

Promotion des activités visant à lutter contre la cybercriminalité, notamment l'assistance technique et le renforcement des capacités

Rapport du Secrétaire général

Résumé

Le présent rapport a été établi en application de la résolution 20/7 de la Commission pour la prévention du crime et la justice pénale intitulée "Promotion des activités visant à lutter contre la cybercriminalité, notamment l'assistance technique et le renforcement des capacités". Il contient un résumé des activités de l'Office des Nations Unies contre la drogue et le crime (ONUDC) en ce qui concerne la fourniture aux États Membres d'une assistance technique et en matière de renforcement des capacités, un aperçu des activités menées par l'ONUDC pour aider le groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité, ainsi que le résumé du projet d'étude sur la cybercriminalité.

* E/CN.15/2013/1.

V.13-80774 (F) 040413 050413

I. Introduction

1. Le présent rapport a été établi en application de la résolution 20/7 de la Commission pour la prévention du crime et la justice pénale intitulée “Promotion des activités visant à lutter contre la cybercriminalité, notamment l’assistance technique et le renforcement des capacités”.

2. Dans cette résolution, la Commission a demandé à l’Office des Nations Unies contre la drogue et le crime (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, ainsi que sur les enquêtes et les poursuites, sans préjudice des travaux et des résultats des réunions du groupe d’experts chargé de réaliser une étude approfondie sur la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour lutter contre ce phénomène.

3. En outre, la Commission a pris note des résultats de la première réunion du groupe d’experts (voir E/CN.15/2011/19) et a prié l’ONUDC de renforcer sa coopération avec les États Membres, les organisations compétentes, telles que l’Organisation internationale de police criminelle (INTERPOL), l’Office européen de police, l’Union internationale des télécommunications (UIT), la Commission européenne, le Conseil de l’Europe, l’Organisation de Shanghai pour la coopération et la Communauté d’États indépendants, ainsi qu’avec le secteur privé, y compris les sociétés d’informatique et les fournisseurs d’accès à l’Internet, en vue de combattre la cybercriminalité.

II. Travaux menés par l’Office des Nations Unies contre la drogue et le crime, en coopération avec les États Membres, les organisations internationales et régionales, et le secteur privé pour fournir une assistance technique et une formation aux États

4. En 2012, l’ONUDC a mis au point un programme mondial contre la cybercriminalité, qui adoptait une démarche globale axée sur: a) la formation des agents des services de détection et de répression et des praticiens de la justice pénale sur les techniques d’enquête et les approches pénales de la cybercriminalité; b) la prévention de la cybercriminalité et la sensibilisation à cette dernière; c) le renforcement de la coopération nationale, régionale et internationale en matière de lutte contre la cybercriminalité; et d) la collecte de données, la recherche et l’analyse des liens entre la criminalité organisée et la cybercriminalité. Dans le cadre de ce programme, l’ONUDC favorisera un renforcement à long terme et durable des capacités, par le biais notamment de sessions de formation, en coopération avec une gamme de partenaires, dont l’UIT, le secteur privé et des experts du monde universitaire.

5. Toutes les activités du programme mondial contre la cybercriminalité visent à renforcer à long terme et de manière durable les capacités nationales de prévention

de la cybercriminalité et de lutte contre celle-ci. Les activités définies par le programme seront principalement mises à exécution par l'ONUDC avec, si nécessaire et en fonction du domaine, de la demande du gouvernement concerné et du mandat pertinent, l'appui supplémentaire de l'UIT et des autres partenaires compétents.

6. En mai 2011, l'ONUDC a conclu avec l'UIT un mémorandum d'accord aux fins de coopération visant à fournir une assistance technique dans le domaine de la cybercriminalité et de la cybersécurité, dans les limites du mandat respectif de chaque organisation[1]. Conformément à ce mémorandum, l'ONUDC a collaboré avec l'UIT pour offrir une assistance technique aux États qui en faisaient la demande. Dans ce cadre, l'ONUDC se concentre sur la prévention de la criminalité et les aspects de justice pénale de la cybercriminalité, tandis que l'UIT œuvre à renforcer la cybersécurité, en protégeant notamment les infrastructures essentielles contre les attaques informatiques.

7. Dans sa résolution 2011/33 intitulée "Prévention, protection et coopération internationale contre l'utilisation des nouvelles technologies de l'information à des fins de maltraitance ou d'exploitation des enfants", le Conseil économique et social a prié l'ONUDC d'effectuer une étude permettant d'identifier, de décrire et d'évaluer les effets des nouvelles technologies de l'information sur la maltraitance et l'exploitation des enfants en tenant compte des données recueillies par le groupe d'experts. Dans cette résolution, le Conseil a également prié l'ONUDC de concevoir et d'effectuer une évaluation des besoins des États en ce qui concerne la formation en matière d'enquête sur les infractions commises contre des enfants à l'aide des nouvelles technologies de l'information et des communications et, sur la base des résultats de cette étude, d'élaborer un programme de formation et d'assistance technique pour aider les États Membres à lutter plus efficacement contre ces infractions.

8. En 2011 et au premier semestre 2012, l'ONUDC a commencé à examiner la documentation existante pour effectuer l'étude sur les effets des nouvelles technologies de l'information sur la maltraitance et l'exploitation des enfants, et a pris des mesures préparatoires concernant l'évaluation des besoins en formation. Conformément à la résolution 2011/33 du Conseil économique et social, un rapport sur l'application de cette résolution, notamment les activités liées à l'étude, sera soumis pour examen à la vingt-troisième session de la Commission, en 2014.

9. En avril et mai 2012, l'ONUDC a organisé des ateliers pour 10 pays d'Afrique orientale et australe à Nairobi, pour 12 pays d'Asie de l'Ouest à Beyrouth, et pour 11 pays d'Asie du Sud-Est et d'Asie du Sud à Bangkok. Ces ateliers lui ont permis d'obtenir des informations sur les besoins en assistance technique de ces pays dans le domaine de la cybercriminalité. Ils ont montré qu'il existait: a) un besoin identifié de formation des responsables politiques et des décideurs afin de renforcer la priorité accordée aux questions de cybercriminalité; b) une nécessité de renforcer les mécanismes de coopération internationale à la fois formelle et informelle entre les agents des services de détection et de répression et les procureurs; c) une nécessité d'améliorer l'accès au matériel informatique et aux logiciels de criminalistique et la formation sur ces éléments pour mener les enquêtes relatives à la cybercriminalité; et d) un besoin de promotion des partenariats public-privé afin

[1] Voir www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf.

de renforcer les mesures de prévention de la cybercriminalité. En se fondant sur les résultats des ateliers, l'ONUDC étudie actuellement les options de fourniture d'assistance technique dans le cadre du programme mondial contre la cybercriminalité et en collaboration avec les partenaires pertinents, dont l'UIT, et pour les pays d'Afrique orientale et australe.

10. Des représentants de l'ONUDC ont participé à des réunions avec les principaux fournisseurs mondiaux de services électroniques pour continuer de progresser en matière d'appui et d'engagement du secteur privé dans le programme mondial contre la cybercriminalité. Ce dernier prévoit une coopération étroite avec les partenaires du secteur privé et les organisations intergouvernementales pertinentes afin d'apporter un soutien commun aux programmes de renforcement des capacités. Il a été conçu pour faciliter les relations de travail entre les agents des services de détection et de répression, d'une part, et les bureaux locaux des principaux fournisseurs mondiaux de services électroniques, d'autre part, en prévoyant notamment la présentation par les prestataires de services des procédures d'entreprise et des exigences de procédure régulière aux agents spécialistes de la cybercriminalité et en facilitant la communication des informations relatives aux menaces stratégiques entre les principaux prestataires mondiaux de cybersécurité et les forces de l'ordre.

11. En février 2012, une évaluation initiale a été effectuée à la demande du Gouvernement panaméen en vue de renforcer la capacité nationale de lutte contre la cybercriminalité. Organisée conjointement par le siège de l'ONUDC et le Bureau régional pour l'Amérique centrale et les Caraïbes, la mission a collaboré avec un groupe de travail interministériel afin d'examiner et de réviser le cadre législatif relatif à la cybercriminalité. Ce groupe de travail, qui réunissait des autorités nationales et des guides d'opinion, ainsi que des entités du secteur privé, avait été créé pour travailler sur la législation panaméenne relative à la cybercriminalité. Des consultations ont été organisées pour définir une méthode vaste et globale de lutte contre ce phénomène dans ce pays. Les autorités panaméennes ont également exprimé leur intérêt pour l'approche commune UIT-ONUDC et pour l'appui dont elles pourraient bénéficier en matière de renforcement de la défense des infrastructures essentielles de leur pays.

12. Par ailleurs, en vue de renforcer la coopération et de sensibiliser à la cybercriminalité, l'ONUDC a organisé en 2012 un atelier en République islamique d'Iran, à la demande de ce pays: il s'agissait de dispenser des sessions de formation sur la cybercriminalité à 80 agents des services de détection et de répression et du ministère de la Justice. Des réunions ont également eu lieu au sein du bureau local d'INTERPOL, de la police et de la magistrature afin d'améliorer la coopération mondiale contre la cybercriminalité.

III. Activités menées par l'Office des Nations Unies contre la drogue et le crime pour renforcer la coopération avec les États Membres, les organisations intergouvernementales et le secteur privé

13. Pour renforcer la coopération contre la cybercriminalité à tous les niveaux, l'ONUDC a continué à participer en tant qu'observateur aux consultations du

Comité de la Convention sur la cybercriminalité du Conseil de l'Europe, dans le cadre de la Convention sur la Cybercriminalité du Conseil de l'Europe, et de sa conférence annuelle "Octopus".

14. L'ONUDC s'est également associé au projet "Commonwealth Cybercrime Initiative", et a cherché des moyens de renforcer sa coopération avec les autres partenaires de l'Initiative. Par ailleurs, il a participé en tant qu'observateur au European Cybercrime Training and Education Group, et a coopéré avec l'Organisation pour la sécurité et la coopération en Europe dans le contexte de sa réunion annuelle des experts de la police.

IV. Activités menées par l'Office des Nations Unies contre la drogue et le crime pour aider le groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité[a]

15. À sa première réunion, tenue à Vienne du 17 au 21 janvier 2011, le groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité a examiné et adopté un ensemble de sujets et une méthodologie pour l'étude (voir E/CN.15/2011/19). Cette méthodologie prévoyait l'envoi d'un questionnaire aux États Membres, aux organisations intergouvernementales et aux représentants du secteur privé et des institutions universitaires. Les informations ont été recueillies par l'ONUDC, conformément à la méthodologie convenue, entre février et juillet 2012[2].

16. En juin 2012, un projet de questionnaire a été adressé à tous les États Membres pour qu'ils fassent état de leurs observations. Après avoir reçu ces observations, l'ONUDC a établi la version définitive du questionnaire et l'a diffusée via un portail de collecte de données sur Internet. Afin de confirmer l'exactitude des informations réunies et analysées, l'ONUDC a envoyé à tous les États Membres un résumé de leurs propres dispositions législatives relatives à la cybercriminalité pour recueillir leurs observations et, si nécessaire, leurs corrections. En novembre 2012, l'ONUDC a consulté des experts nommés par chaque groupe régional concernant l'analyse préliminaire des résultats obtenus à partir des questionnaires remplis par les États Membres. Sur la base des réponses des États Membres, du secteur privé, des institutions universitaires et des organisations intergouvernementales, l'ONUDC a établi un projet d'étude devant être examiné par le groupe d'experts.

17. À sa deuxième réunion, tenue du 25 au 28 février 2013[3], le groupe d'experts a pris note de l'étude approfondie sur la cybercriminalité réalisée par l'ONUDC sous l'égide du groupe d'experts, et l'a examinée. Le groupe d'experts a noté que les délibérations, ainsi que l'étude, reflétaient un ensemble de vues et d'approches

---

[a] Le texte de la section IV a été initialement publié dans un document de base non modifié (UNODC/CCPCJ/EG.4/2013/2); dans le présent rapport, il a été modifié conformément aux normes établies du Secrétariat.

[2] Des informations ont été reçues de 69 États Membres répartis comme suit: Afrique (11), Amériques (13), Asie (19), Europe (24) et Pacifique (2). Des informations ont également été reçues de 40 organisations du secteur privé, de 17 institutions universitaires et de 11 organisations intergouvernementales. En outre, plus de 500 documents librement accessibles ont été examinés par le Secrétariat.

[3] Il est rendu compte du résultat de la réunion dans le document UNODC/CCPCJ/EG.4/2013/3.

différentes adoptées par les États pour prévenir et combattre le phénomène de la cybercriminalité. Lors des débats consacrés à l'étude de la cybercriminalité, il a été noté qu'il existait un large soutien au renforcement des capacités et à l'assistance technique, ainsi qu'au rôle joué par l'ONUDC à cet égard. Divers avis ont été exprimés en ce qui concerne le contenu, les résultats et les options présentés dans l'étude. Le groupe d'experts a examiné la voie à suivre et recommandé d'examiner plus avant l'étude à la vingt-deuxième session de la Commission.

18. Le résumé de l'étude approfondie figurant ci-dessous a été établi par l'ONUDC, qui s'est vu confier cette tâche par le groupe d'experts. Les résultats et options qui figurent dans l'étude et dans le résumé ont été établis par l'ONUDC sur la base des informations empiriques fournies et ne visent pas à constituer des recommandations[4].

A. Résumé de l'étude approfondie sur le phénomène de la cybercriminalité établi par l'Office des Nations Unies contre la drogue et le crime

1. Connectivité mondiale et cybercriminalité

19. En 2011, au moins 2,3 milliards de personnes, soit plus d'un tiers de la population mondiale totale, avaient accès à Internet. Plus de 60 % des utilisateurs d'Internet vivaient dans des pays en développement et 45 % avaient moins de 25 ans. D'ici à 2017, on estime que près de 70 % des habitants de la planète seront abonnés à des services mobiles à large bande. D'ici à 2020, les dispositifs en réseau ("l'Internet des objets") seront six fois plus nombreux que les humains, ce qui bouleversera les conceptions actuelles de l'Internet. Dans le monde hyperconnecté de demain, il sera difficile d'imaginer un "délit informatique", voire n'importe quel délit, pour lequel il n'existe pas de preuve électronique liée à la connectivité Internet (protocole IP).

20. La façon dont est définie la cybercriminalité dépend le plus souvent de l'objectif visé dans le contexte où ce terme est utilisé. Un nombre limité d'atteintes à la confidentialité, à l'intégrité et à la disponibilité des données ou des systèmes informatiques constituent la quintessence de la cybercriminalité. Cependant, d'autres agissements tels que l'utilisation d'ordinateurs pour réaliser un gain ou porter un préjudice, financier ou autre, y compris certaines formes d'usurpation d'identité et les atteintes aux contenus informatiques (qui relèvent tous de la "cybercriminalité" prise dans un sens plus large) ne facilitent pas les efforts visant à définir juridiquement ce terme dans sa globalité. Les principaux actes de cybercriminalité doivent être définis. Cependant, une "définition" de la cybercriminalité n'est pas aussi utile dans d'autres contextes, par exemple pour fixer la portée des pouvoirs spéciaux en matière d'enquête et de coopération internationale, où il vaut mieux privilégier les preuves électroniques de l'infraction, quelle qu'elle soit, plutôt qu'un concept étendu et artificiel de "cybercriminalité".

[4] L'étude complète n'est disponible qu'en anglais, dans le document E/CN.15/2013/CRP.5.

2. La cybercriminalité dans le monde

21. Dans de nombreux pays, la montée en flèche de la connectivité mondiale a coïncidé avec des transformations économiques et démographiques, une augmentation des disparités de revenus, une contraction des dépenses du secteur privé et une réduction des liquidités financières. Dans l'ensemble, les services de répression qui ont répondu à l'enquête constatent une augmentation de la cybercriminalité, car aussi bien les individus que les groupes criminels organisés, mus par l'appât du gain et leur intérêt personnel, y trouvent de nouveaux champs d'activité criminelle à exploiter. On estime que plus de 80 % des actes de cybercriminalité ont pour point de départ une activité organisée quelconque, des marchés noirs de la cybercriminalité s'étant constitués autour d'activités de création de logiciels malveillants, d'infection d'ordinateurs, de gestion de réseaux zombies, de collecte de données personnelles et financières, de vente de données et de commercialisation d'informations financières. Les cybercriminels n'ont plus besoin de compétences ou de techniques complexes. Les pays en développement en particulier ont vu apparaître une sous-culture de la fraude informatique financière pratiquée par de jeunes hommes, dont beaucoup commencent leur carrière cybercriminelle à la fin de l'adolescence.

22. D'une manière générale, les actes de cybercriminalité se répartissent entre les agissements à motivation financière et les atteintes aux contenus des ordinateurs, ainsi que les atteintes à la confidentialité, à l'intégrité et à l'accessibilité des systèmes informatiques. Cependant, les risques relatifs ne sont pas perçus de la même façon par les gouvernements et les entreprises du secteur privé. Actuellement, les statistiques sur la criminalité enregistrées par la police n'offrent pas une base solide pour des comparaisons entre pays, bien qu'elles puissent être souvent importantes pour l'élaboration des politiques au niveau national. Les deux tiers des pays considèrent que leurs systèmes de statistiques policières sont insuffisants pour l'enregistrement de la cybercriminalité. Les taux de cybercriminalité enregistrés par la police dépendent davantage du niveau de développement du pays et des moyens de la police spécialisée que des taux de criminalité sous-jacents.

23. Les enquêtes de victimisation constituent une meilleure base de comparaison. Elles font apparaître pour la cybercriminalité (fraude en ligne à la carte de crédit, usurpation d'identité, réponse à une tentative d'hameçonnage et accès non autorisé à un compte de messagerie électronique) des taux de victimisation nettement plus élevés (entre 1 et 17 % de la population en ligne dans 21 pays à travers le monde) que pour les formes de criminalité "classiques" telles que les cambriolages, les vols qualifiés et les vols de véhicules automobiles (moins de 5 % dans les mêmes pays). Les taux de victimisation concernant la cybercriminalité sont plus élevés dans les pays à faible niveau de développement, ce qui montre la nécessité de renforcer les efforts de prévention dans ces pays.

24. Les entreprises du secteur privé en Europe signalent des taux de victimisation similaires – entre 2 et 16 % – pour des actes tels que la violation de données par intrusion ou hameçonnage. Les outils préférés des auteurs de ces agissements criminels, par exemple les réseaux d'ordinateurs zombies, ont une portée mondiale. Plus d'un million d'adresses IP distinctes dans le monde entier étaient exploitées comme serveurs de commande et de contrôle de réseaux d'ordinateurs zombies en 2011. Les contenus Internet représentent aussi un important motif de préoccupation pour les gouvernements. Ceux-ci cherchent à éliminer non seulement les contenus

pédopornographiques ou ayant pour but l'incitation à la haine, mais aussi ceux qui sont diffamatoires ou critiques à leur égard, ce qui soulève des problèmes du point de vue des droits de l'homme dans certains cas. Selon les estimations, près de 24 % du trafic Internet dans le monde violerait les droits d'auteur, les téléchargements de contenus partagés de pair à pair (P2P) étant particulièrement élevés dans les pays d'Afrique, d'Amérique du Sud et d'Asie de l'Ouest et du Sud.

3. Législation sur la cybercriminalité

25. La législation est déterminante pour prévenir et combattre la cybercriminalité. Elle doit couvrir tous les domaines, notamment l'incrimination, la procédure, la compétence, la coopération internationale et la responsabilité des fournisseurs de services Internet. Au niveau national, les lois sur la cybercriminalité, qu'elles soient anciennes, nouvelles ou en projet, concernent le plus souvent l'incrimination et privilégient l'établissement d'infractions spéciales pour les principaux actes de cybercriminalité. Cependant, les pays sont de plus en plus conscients de la nécessité de légiférer dans d'autres domaines. Par rapport aux lois préexistantes, les lois sur la cybercriminalité nouvelles ou en projet traitent plus fréquemment des mesures d'enquête, de la compétence, des preuves électroniques et de la coopération internationale. Moins de la moitié des pays ayant répondu considèrent que leur droit pénal et leurs règles de procédure sont suffisants, et ce chiffre masque de grandes disparités régionales. Alors que plus des deux tiers des pays européens jugent leur législation suffisante, le rapport est inversé en Afrique, dans les Amériques et en Asie et dans le Pacifique, où plus de deux tiers des pays la jugent seulement en partie, voire pas du tout suffisante. Seulement la moitié des pays ayant signalé que leur législation était insuffisante ont également indiqué que l'adoption de nouvelles lois était en cours ou prévue, révélant ainsi un besoin urgent de renforcement législatif dans ces régions.

26. Des progrès importants ont été réalisés au cours de la dernière décennie dans la mise en œuvre d'instruments internationaux et régionaux de lutte contre la cybercriminalité, obligatoires ou non, qui ont été élaborés dans le cadre des organisations ci-après ou qui en sont inspirés: i) Conseil de l'Europe ou Union européenne, ii) Communauté d'États indépendants ou Organisation de Shanghai pour la coopération, iii) organisations intergouvernementales africaines, iv) Ligue des États arabes, et v) Organisation des Nations Unies. Tous ces instruments s'enrichissent mutuellement et partagent en particulier les concepts et les approches de la Convention du Conseil de l'Europe sur la cybercriminalité. Une analyse de 19 instruments multilatéraux relatifs à la cybercriminalité montre que ceux-ci présentent des dispositions de base communes, mais aussi des divergences importantes quant au fond.

27. Au total, 82 pays ont signé et/ou ratifié un ou plusieurs instruments multilatéraux contraignants relatifs à la cybercriminalité[5]. Ces instruments ont également eu une influence indirecte sur les législations nationales d'États non

[5] Un ou plusieurs des instruments ci-après: Convention du Conseil de l'Europe sur la cybercriminalité, Convention de la Ligue des États arabes sur la lutte contre les infractions liées aux technologies de l'information, Accord de coopération de la Communauté d'États indépendants en matière de lutte contre les infractions dans le domaine informatique et Accord de l'Organisation de Shanghai pour la coopération dans le domaine de la sécurité internationale de l'information.

parties parce que ceux-ci les ont utilisés comme modèles ou se sont inspirés de la législation des États parties. Les parties à un instrument multilatéral relatif à la cybercriminalité ont davantage tendance à considérer que leur droit pénal et procédural national est suffisant, ce qui montre que les dispositions multilatérales actuelles dans ces domaines sont généralement jugées efficaces. Il ressort d'informations fournies par plus de 40 pays que la Convention du Conseil de l'Europe sur la cybercriminalité est l'instrument multilatéral le plus utilisé pour l'élaboration de dispositions législatives sur la cybercriminalité. Les pays qui utilisaient d'autres instruments multilatéraux étaient environ deux fois moins nombreux.

28. Un tiers des pays ayant répondu ont fait état de niveaux élevés, voire très élevés, d'harmonisation législative avec les pays jugés importants aux fins de la coopération internationale. Ces niveaux varient cependant selon les régions, les plus élevés ayant été signalés dans les Amériques et en Europe. Cela peut s'expliquer par l'utilisation, dans certaines régions, d'instruments multilatéraux spécialement conçus pour contribuer à une telle harmonisation. Il se peut que la fragmentation au niveau international et la diversité des législations nationales en ce qui concerne l'incrimination des actes de cybercriminalité, la compétence juridictionnelle et les mécanismes de coopération soient corrélées à l'existence de multiples instruments de lutte contre la cybercriminalité ayant une portée thématique et géographique différente. Les divergences qui existent actuellement aussi bien entre les instruments que les régions traduisent des différences juridiques et constitutionnelles sous-jacentes, y compris des conceptions différentes des droits et de la vie privée.

4. Incrimination

29. Des informations sur la législation pénale relative à la cybercriminalité ont été recueillies au moyen du questionnaire d'enquête ainsi qu'en analysant des textes législatifs constituant des sources primaires qui avaient été rassemblés par le Secrétariat[6]. Le questionnaire d'enquête mentionnait 14 actes généralement englobés dans la notion de cybercriminalité[7]. Les réponses fournies montrent que ces 14 actes sont largement incriminés, à l'exception notable de l'envoi massif de messages non sollicités ("spams") et, dans une certaine mesure, des agissements faisant intervenir des outils informatiques malveillants, présentant un caractère raciste ou xénophobe ou consistant à solliciter en ligne des enfants à des fins sexuelles ("grooming"). Cela traduit un certain consensus de base sur les comportements cybercriminels à réprimer. Des pays ont signalé l'existence de

---

[6] Le Secrétariat a analysé, en tant que source primaire, des textes législatifs provenant de 97 États Membres (dont 56 avaient répondu au questionnaire) répartis comme suit: Afrique (15), Amériques (22), Asie (24), Europe (30) et Pacifique (6).

[7] Accès illégal à un système informatique; accès illégal à des données informatiques, interception ou acquisition illégale de données informatiques; atteinte à l'intégrité des données ou à l'intégrité du système; production, distribution ou possession d'outils informatiques malveillants; violation de la vie privée ou de la protection des données; fraude ou falsification informatiques; usurpation d'identité numérique; atteintes aux droits d'auteur et aux marques par voie informatique; envoi massif ou contrôle de l'envoi massif de messages non sollicités ("spams"); actes informatiques causant un préjudice personnel; actes informatiques à caractère raciste ou xénophobe; production, diffusion ou possession de pornographie enfantine par voie informatique; sollicitation en ligne d'enfants à des fins sexuelles ("grooming"); actes informatiques visant à faciliter les infractions terroristes.

plusieurs autres infractions non mentionnées dans le questionnaire, qui concernaient principalement les contenus numériques, notamment à caractère obscène, les paris en ligne et le recours à des cybermarchés illicites, par exemple pour le trafic de drogue et la traite des êtres humains. S'agissant des 14 actes mentionnés dans le questionnaire, les pays ont signalé l'existence d'infractions spécifiques pour les principales formes de cybercriminalité portant atteinte à la confidentialité, à l'intégrité et à l'accessibilité des systèmes informatiques. Les autres formes de cybercriminalité étaient le plus souvent traitées comme des infractions générales (non spécifiques à la cybercriminalité). Cependant, l'une ou l'autre approche pouvait être utilisée dans le cas des actes informatiques constituant une violation de la vie privée, une fraude ou une falsification ou une atteinte à l'identité.

30. Malgré l'existence d'un large consensus quant aux grandes catégories d'infractions, l'analyse détaillée des dispositions des textes législatifs analysés révèle des approches divergentes. Les infractions liées à l'accès illégal à des systèmes et des données informatiques diffèrent en fonction de leur objet (données, systèmes ou informations) et de la question de savoir si le simple accès est incriminé ou si une intention supplémentaire, par exemple celle de causer un préjudice, est nécessaire. L'élément intentionnel requis est également différent selon les approches suivies pour incriminer l'atteinte à l'intégrité des données ou à l'intégrité du système. Dans la plupart des pays, cette atteinte doit être intentionnelle, alors que dans d'autres, les atteintes par négligence sont également incriminées. Les actes constituant une atteinte à l'intégrité de données informatiques peuvent comprendre l'endommagement, la suppression, la modification, la dissimulation, la saisie ou la transmission de ces données. L'interception illégale n'est pas incriminée de la même façon selon qu'elle porte sur des transmissions de données publiques ou privées et qu'elle se limite ou non à recourir à des moyens techniques. Tous les pays n'incriminent pas les actes faisant intervenir des outils informatiques malveillants. Lorsqu'ils le font, la portée de l'infraction peut être différente selon qu'elle englobe ou non la possession, la distribution ou l'utilisation de logiciels (tels que les logiciels malveillants) et/ou de codes d'accès informatiques (comme les mots de passe des victimes). Dans le contexte de la coopération internationale, ces différences peuvent avoir une incidence sur l'établissement de la double incrimination entre les pays.

31. Plusieurs pays ont érigé en infractions spécifiques la fraude et la falsification informatiques et l'usurpation d'identité numérique. D'autres étendent les dispositions générales applicables en matière de fraude ou de vol, ou se fondent sur des infractions qui en englobent les éléments constitutifs – comme l'accès illégal, l'atteinte à l'intégrité des données et la falsification dans le cas de l'usurpation d'identité. Un certain nombre d'actes liés aux contenus, en particulier la pornographique enfantine, sont largement incriminés. Il y a cependant des différences en ce qui concerne la définition du terme "enfant", les contenus "visuels" soumis à restrictions, l'exclusion des représentations virtuelles et les actes couverts. L'immense majorité des pays incriminent par exemple la production et la distribution de pornographie enfantine, mais en ce qui concerne la possession et l'accès, la situation est plus contrastée. S'agissant des atteintes aux droits d'auteur et aux marques par voie informatique, les pays ont le plus souvent indiqué que celles-ci étaient traitées comme des infractions pénales générales sanctionnant des actes commis délibérément à une échelle commerciale.

32. L'utilisation croissante des réseaux sociaux et de contenus Internet produits par les utilisateurs a conduit les gouvernements à intervenir, y compris sur le plan pénal, ce qui a suscité des appels en faveur du respect de la liberté d'expression. Les pays ayant répondu fixent différentes limites à cette liberté, notamment en ce qui concerne la diffamation, les outrages, les menaces, l'incitation à la haine, l'offense aux sentiments religieux, les représentations obscènes et les atteintes à l'autorité de l'État. La dimension socioculturelle de certaines de ces limites apparaît non seulement dans les législations nationales, mais aussi dans des instruments multilatéraux. Dans certains instruments régionaux sur la cybercriminalité, par exemple, la violation de la moralité publique, la pornographie et les atteintes aux valeurs ou aux principes religieux ou familiaux constituent des infractions dont le champ est étendu.

33. Le droit international des droits de l'homme constitue une arme aussi bien offensive que défensive puisqu'il oblige à la fois à incriminer (de façon limitée) les formes d'expression extrêmes et à protéger les autres formes. Certaines limites à la liberté d'expression, notamment celles interdisant l'incitation au génocide, les propos haineux constituant une incitation à la discrimination, à l'hostilité ou à la violence, l'incitation au terrorisme et la propagande en faveur de la guerre, s'imposent donc aux États qui sont parties aux instruments internationaux pertinents relatifs aux droits de l'homme. Les autres disposent d'une certaine marge d'appréciation pour déterminer les limites des formes d'expression acceptables compte tenu de leurs cultures et de leurs traditions juridiques. Néanmoins, à partir d'un certain point, le droit international des droits de l'homme s'appliquera. Par exemple, lorsqu'il s'agira d'appliquer à des propos tenus en ligne des dispositions pénales sur la diffamation, l'outrage à l'autorité et les propos injurieux, il sera difficile de démontrer que les sanctions sont proportionnées, appropriées et le moins intrusives possibles. Lorsqu'un contenu est illégal dans un pays mais qu'il est légal de le produire et de le diffuser dans un autre, les États devront cibler leur riposte pénale sur les personnes accédant à ce contenu qui relèvent de leur juridiction et non sur le contenu si celui-ci a été produit à l'étranger.

5. Répression et enquêtes

34. Plus de 90 % des pays ayant répondu ont indiqué que les actes de cybercriminalité étaient le plus souvent portés à l'attention des services de répression par les déclarations des personnes physiques ou morales qui en avaient été victimes. Selon leurs estimations, la proportion de ces actes signalés à la police se situait dans une fourchette dont la valeur la plus basse était 1 %. Selon une enquête mondiale du secteur privé, 80 % des victimes des principales infractions de cybercriminalité ne signalent pas ces infractions à la police. Cette sous-déclaration s'explique par le manque de sensibilisation à ces infractions et la méconnaissance des mécanismes de déclaration, la honte et l'embarras des victimes, et, dans le cas des entreprises, la crainte de voir leur réputation compromise. Dans toutes les régions du monde, il a été fait état d'initiatives visant à accroître le taux de déclaration, notamment grâce à des systèmes d'information en ligne et des permanences téléphoniques, des campagnes d'information, des contacts avec le secteur privé et un renforcement de la communication et du partage des informations avec la police. La répression au coup par coup des actes de cybercriminalité doit cependant s'accompagner d'enquêtes tactiques à moyen et long terme ciblées sur les marchés criminels et leurs organisateurs. Les autorités

répressives des pays développés sont actives dans ce domaine, notamment en menant des opérations d'infiltration sur les réseaux sociaux, les forums de discussion et les services de messagerie instantanée et P2P. Les innovations en matière de délinquance, les difficultés d'accès aux preuves électroniques et l'insuffisance des capacités, des ressources et des moyens logistiques internes compliquent les enquêtes sur la cybercriminalité. Les suspects ont fréquemment recours à des moyens qui leur permettent d'agir anonymement et de brouiller les pistes, et les nouvelles techniques criminelles se diffusent rapidement et largement par le biais des cybermarchés de la criminalité.

35. Les enquêtes policières sur la cybercriminalité nécessitent de recourir à une combinaison de techniques traditionnelles et nouvelles. Bien que certaines activités d'enquête puissent être menées dans le cadre des pouvoirs habituels, de nombreuses règles de procédure convenant à une approche territoriale et matérielle sont inadaptées dans le contexte du stockage électronique de données et des flux de données en temps réel. Le questionnaire mentionnait 10 mesures d'enquête sur la cybercriminalité de caractère général comme la perquisition et la saisie ou spécialisées comme la conservation de données informatiques[8]. Les pays ont le plus souvent signalé l'existence de pouvoirs généraux (non spécifiques à la cybercriminalité) pour l'ensemble des mesures d'enquête mentionnées. Un certain nombre de pays ont également signalé l'existence d'une législation spécifique, notamment pour assurer la conservation rapide de données informatiques et obtenir des données stockées relatives aux abonnés. De nombreux pays ont signalé l'absence de dispositions légales autorisant le recours à des méthodes avancées comme la cybercriminalistique. Bien que l'application des règles de procédure classiques puisse être étendue au cyberespace, dans de nombreux cas une telle approche peut aussi être un facteur d'insécurité juridique et constituer un motif de contestation de la légalité des conditions dans lesquelles les preuves ont été recueillies, et donc de la recevabilité de ces preuves. Dans l'ensemble, les approches nationales concernant les pouvoirs d'enquête sur la cybercriminalité présentent moins de points communs que celles concernant l'incrimination de nombreux actes de cybercriminalité.

36. Quelle que soit la forme juridique des pouvoirs d'enquête, tous les répondants ont déclaré recourir à la perquisition et à la saisie pour prendre physiquement possession d'équipements informatiques et intercepter des données informatiques. La majorité des pays font également ordonner la remise de données informatiques stockées par des fournisseurs de services Internet. En dehors de l'Europe, cependant, environ un tiers des pays signalent qu'il est difficile d'obliger des tiers à fournir des informations pour les besoins d'une enquête. Environ les trois quarts des pays ont recours à des mesures d'enquête spécialisées comme la collecte en temps réel ou la conservation rapide de données. La mise en œuvre de mesures d'enquête nécessite généralement un minimum d'éléments de preuve initiaux ou une

[8] Perquisition de matériel ou de données informatiques; saisie de matériel ou de données informatiques; injonction de communiquer l'identité de l'abonné ou de produire des données le concernant; injonction de produire des données stockées relatives au trafic; injonction de produire des données stockées relatives au contenu; collecte en temps réel des données relatives au trafic; collecte en temps réel des données relatives au contenu; conservation rapide de données informatiques; emploi de logiciels de criminalistique à distance; accès transfrontière à un système ou à des données informatiques.

déclaration signalant un acte de cybercriminalité. Des mesures plus intrusives comme la collecte de données en temps réel ou l'accès au contenu de données nécessitent souvent des seuils plus élevés, par exemple la preuve qu'un acte grave a été commis, la production d'éléments suffisants ou l'existence de motifs raisonnables.

37. L'interaction entre les services répressifs et les fournisseurs de services Internet est particulièrement complexe. Les fournisseurs de services détiennent des informations concernant leurs abonnés, notamment des factures, certains relevés de connexion, des données de localisation (comme les données des tours de téléphonie cellulaire) et le contenu de communications, qui peuvent constituer des preuves électroniques essentielles concernant une infraction. Les obligations imposées par la législation nationale et les politiques du secteur privé concernant la conservation et la communication des données varient beaucoup selon les pays, les entreprises et le type de données. Les pays ont le plus souvent déclaré avoir recours à des ordonnances judiciaires pour obtenir des preuves auprès des fournisseurs de services. Dans certains cas, cependant, les services répressifs peuvent obtenir directement des données stockées relatives aux abonnés, des données relatives au trafic et même des données relatives au contenu. À cet égard, les organisations du secteur privé ont souvent déclaré qu'elles avaient pour règle fondamentale de ne communiquer des données que dans le cadre d'une procédure régulière, mais qu'elles répondaient aussi volontairement dans certaines circonstances aux demandes présentées directement par les services répressifs. Les relations informelles entre les services répressifs et les fournisseurs de services, dont l'existence a été signalée par plus de la moitié des pays ayant répondu, facilitent l'échange d'informations et contribuent à la confiance. Les réponses indiquent la nécessité de trouver un équilibre entre le respect de la vie privée et les exigences d'une procédure régulière et en particulier d'obtenir la communication des preuves en temps opportun, afin que le secteur privé ne devienne pas un point mort pour les enquêtes.

38. Les enquêtes sur la cybercriminalité touchent invariablement à des questions de protection de la vie privée régies par le droit international relatif aux droits de l'homme. Les normes relatives aux droits de l'homme précisent que les lois doivent indiquer de façon suffisamment claire les circonstances dans lesquelles les autorités sont habilitées à utiliser une mesure d'enquête donnée, et que des garanties adéquates et suffisantes contre les abus doivent être offertes. Les pays ont indiqué comment la protection de la vie privée était assurée par leur droit national et présenté les diverses limites et garanties dont étaient assorties les enquêtes. Cependant, dans le cas d'enquêtes transnationales, l'existence de niveaux de protection différents peut rendre imprévisible l'accès aux données en application de la loi étrangère et se traduire par des lacunes juridictionnelles dans les régimes de protection de la vie privée.

39. Plus de 90 % des pays ayant répondu au questionnaire ont commencé à mettre en place des structures spécialisées chargées d'enquêter sur la cybercriminalité et les infractions pour lesquelles il existe des éléments de preuve électroniques. Dans les pays en développement, cependant, ces structures manquent de ressources et de capacités. Les pays les moins développés ont beaucoup moins de policiers spécialisés (environ 0,2 pour 100 000 internautes nationaux). Ce taux est de deux à cinq fois plus élevé dans les pays plus développés. Il a été indiqué que 70 % des

policiers spécialisés dans les pays les moins développés manquaient de compétences et de matériel informatiques, et que la moitié seulement bénéficiaient de plus d'une formation par an. Plus de la moitié des pays d'Afrique et un tiers des pays des Amériques ont indiqué dans leurs réponses que leurs services chargés d'enquêter sur la cybercriminalité ne disposaient pas de ressources suffisantes. À l'échelle mondiale, la situation est sans doute encore pire. Par exemple, seulement 20 % des 50 pays les moins avancés ont répondu au questionnaire. Tous les pays d'Afrique et plus de 80 % des pays des Amériques et d'Asie et du Pacifique qui ont répondu ont déclaré avoir besoin d'une assistance technique. Les techniques d'enquête sur la cybercriminalité en général étaient le domaine dans lequel il avait été le plus souvent indiqué qu'une telle assistance était requise. Parmi les pays nécessitant une assistance, 60 % ont déclaré que c'étaient leurs services répressifs qui en avaient besoin.

6. Preuve électronique et riposte pénale

40. La preuve est un moyen permettant d'établir sur des faits la culpabilité ou l'innocence de l'accusé lors du procès. On entend par preuve électronique tout élément qui existe sous forme électronique, transitoire ou non. Il peut s'agir de fichiers informatiques, de transmissions, de relevés, de métadonnées ou de données réseau. La criminalistique numérique a pour objet de récupérer des informations souvent instables et facilement contaminées qui peuvent avoir une valeur probante. Ses techniques comprennent la réalisation de copies "bit à bit" d'informations stockées et effacées, le blocage à l'écriture afin que l'information originale ne puisse pas être modifiée, et le hachage cryptographique des fichiers ou les signatures numériques, qui peuvent mettre en évidence les modifications apportées. Presque tous les pays ont déclaré qu'ils disposaient de certaines capacités de criminalistique numérique. De nombreux pays dans toutes les régions ont cependant signalé un manque d'experts en criminalistique, des différences entre les capacités de l'État fédéral et celles des entités fédérées, un manque d'outils criminalistiques et des retards en raison d'un volume énorme de données à analyser. La moitié des pays indiquent que des suspects ont recours au chiffrement, ce qui, en l'absence de la clef de déchiffrement, rend l'accès aux preuves électroniques long et difficile. Dans la plupart des pays, l'analyse des preuves électroniques est une tâche qui incombe à la police. Les procureurs doivent cependant consulter ces preuves et les comprendre pour établir les faits en vue du procès. Tous les pays d'Afrique et un tiers des pays des autres régions ont signalé que les procureurs ne disposaient pas de ressources suffisantes à cet effet. Leurs compétences en informatique sont généralement inférieures à celles des enquêteurs. Environ 65 % des pays ayant répondu ont fait état d'une certaine spécialisation en matière de cybercriminalité au sein du ministère public. Seulement 10 % des pays ont mentionné l'existence de magistrats spécialisés. La grande majorité des affaires de cybercriminalité sont traitées par des juges non spécialisés qui, dans 40 % des pays ayant répondu, ne bénéficient d'aucune formation dans le domaine de la cybercriminalité. Organiser à l'intention des magistrats des activités de formation concernant la législation sur la cybercriminalité, la collecte de preuves et les techniques informatiques de base et avancées est une priorité.

41. Plus de 60 % des pays ayant répondu ne font pas de distinction sur le plan juridique entre les preuves électroniques et les preuves physiques. Bien que leurs approches soient différentes, de nombreux pays considèrent qu'il s'agit là d'une

bonne pratique qui permet d'assurer un degré de recevabilité satisfaisant par rapport à tous les autres types de preuves. Un certain nombre de pays non européens n'admettent pas du tout la preuve électronique, ce qui rend impossible l'ouverture de poursuites pour des actes de cybercriminalité ou toute autre infraction dont la réalité est établie par des informations électroniques. Bien que, d'une manière générale, les pays n'aient pas de règles de preuve distinctes pour la preuve électronique, un certain nombre d'entre eux ont évoqué un certain nombre de règles et de principes (règle de la meilleure preuve, pertinence des preuves, interdiction de la preuve par ouï-dire, authenticité et intégrité, par exemple) qui peuvent tous s'appliquer de façon spécifique à la preuve électronique. De nombreux pays ont mentionné les difficultés que soulevaient l'imputation d'actes à une personne déterminée et le recours fréquent à des preuves indirectes dans ce contexte.

42. En raison des difficultés auxquelles se heurtent aussi bien les policiers enquêteurs que les procureurs, le pourcentage de cybercriminels traduits en justice est faible. Dans le cas des infractions de pornographie enfantine, le nombre de suspects identifiés par rapport au nombre d'infractions enregistrées par la police est comparable à celui constaté pour les autres infractions sexuelles. En revanche, pour les actes tels que l'accès illégal à des systèmes et la fraude ou la falsification informatiques, ce nombre n'est que d'environ 25 pour 100 infractions. Très peu de pays ont pu fournir des données sur les personnes poursuivies ou condamnées. Les chiffres relatifs aux infractions de cybercriminalité communiqués par un pays montrent cependant que le nombre de personnes condamnées par rapport au nombre d'infractions enregistrées est nettement plus faible que pour les infractions "classiques".

7. Coopération internationale

43. Les pays qui ont répondu au questionnaire ont indiqué qu'entre 30 et 70 % des actes de cybercriminalité ont une dimension transnationale, ce qui implique des enquêtes transnationales, soulève des questions ayant trait à la souveraineté, à la compétence et aux preuves extraterritoriales, et nécessite une coopération internationale. Une infraction de cybercriminalité présente une dimension transnationale lorsqu'elle comprend un élément ou produit un effet substantiel sur le territoire d'un autre pays, ou y est en partie réalisée. Le droit international pose un certain nombre de règles relatives à la compétence sur de tels actes, fondées notamment sur le territoire ou sur la nationalité. Certaines de ces règles figurent également dans les instruments multilatéraux relatifs à la cybercriminalité. Alors que tous les pays d'Europe estiment que leurs cadres juridiques nationaux sont suffisants pour incriminer les actes de cybercriminalité extraterritoriaux et en poursuivre les auteurs, entre un tiers et plus de la moitié environ des pays des autres régions jugent les leurs insuffisants. Dans de nombreux pays, il existe des dispositions traduisant le principe qu'il n'est pas nécessaire qu'une infraction ait été entièrement commise dans un État pour qu'elle relève de la compétence territoriale de celui-ci. Des liens territoriaux peuvent être établis en se référant à des éléments ou à des effets de l'acte, ou au lieu de situation des systèmes ou des données informatiques utilisés pour l'infraction. Les éventuels conflits de compétence sont généralement réglés dans le cadre de consultations formelles et informelles entre les pays. Il ne ressort pas des réponses faites par les pays qu'il soit actuellement nécessaire de prévoir d'autres formes de compétence sur un hypothétique "cyberespace". Au contraire, les règles relatives à la compétence territoriale ou à la

compétence fondée sur la nationalité permettent presque toujours d'établir un lien suffisant entre les actes de cybercriminalité et au moins un État.

44. La coopération internationale en matière pénale comprend l'extradition, l'entraide judiciaire, la reconnaissance mutuelle des jugements étrangers et la coopération informelle entre polices. En raison de la nature transitoire des preuves électroniques, la collaboration pénale internationale dans le domaine de la cybercriminalité suppose que des réponses rapides soient apportées et que des mesures d'enquête spécialisées telles que la conservation de données informatiques puissent être demandées. Le recours aux formes traditionnelles de coopération reste prédominant pour obtenir des preuves extraterritoriales dans des affaires de cybercriminalité, plus de 70 % des pays ayant déclaré adresser des demandes formelles d'entraide judiciaire à cette fin. Près de 60 % des demandes présentées dans le cadre de cette coopération formelle utilisent des instruments bilatéraux comme fondement juridique. Des instruments multilatéraux sont utilisés dans 20 % des cas. Le temps nécessaire aux mécanismes formels pour répondre aussi bien aux demandes d'extradition qu'aux demandes d'entraide judiciaire est de l'ordre de plusieurs mois, ce qui pose des problèmes pour la collecte des preuves électroniques de nature transitoire. Dans 60 % des pays d'Afrique, des Amériques et d'Europe, et 20 % des pays d'Asie et du Pacifique, il existe des mécanismes pour transmettre les demandes urgentes, mais leur incidence sur les délais de réponse est incertaine. Le recours à des mécanismes de coopération informels est possible dans environ les deux tiers des pays déclarants, mais rares sont ceux qui ont une politique régissant l'utilisation de tels mécanismes. Les processus de coopération informelle ainsi que ceux visant à faciliter la coopération formelle, comme les réseaux 24/7, pourraient largement contribuer à raccourcir les délais de réponse, mais ils sont sous-utilisés puisqu'ils ne traitent qu'environ 3 % du nombre total d'affaires de cybercriminalité dont les services répressifs ont à connaître dans les pays déclarants.

45. Les modes formels et informels de coopération ont pour objet de faciliter le processus d'obtention du consentement d'un État pour la conduite d'enquêtes policières étrangères ayant une incidence sur sa souveraineté. Or, lorsqu'ils recueillent des preuves, les enquêteurs accèdent de plus en plus souvent, consciemment ou inconsciemment, à des données extraterritoriales sans le consentement de l'État où ces données se trouvent effectivement. Cette situation résulte en particulier du recours à l'informatique en nuage, qui consiste à stocker des données dans divers centres de données situés dans différents lieux géographiques. Bien qu'il soit techniquement possible de le connaître, le "lieu de situation" des données est une notion de plus en plus artificielle dans la mesure où même les demandes d'entraide judiciaire classiques sont souvent adressées au pays où le fournisseur de services a son siège, plutôt qu'au pays où le centre de données se trouve effectivement. Des enquêteurs étrangers peuvent avoir directement accès à des données extraterritoriales lorsqu'ils établissent une connexion à partir d'un ordinateur appartenant à un suspect ou lorsqu'ils utilisent des codes d'accès à ces données obtenus légalement. Ils peuvent à l'occasion obtenir, en en faisant directement la demande de façon informelle, des données auprès de fournisseurs de services extraterritoriaux, bien que ceux-ci exigent habituellement une procédure régulière. Ces situations ne sont pas suffisamment prises en compte par les dispositions existantes concernant "l'accès transfrontières" qui figurent dans la Convention sur la cybercriminalité du Conseil de l'Europe et la Convention de la Ligue des États arabes sur la lutte contre les infractions liées aux technologies de

l'information, car celles-ci mettent l'accent sur le "consentement" de la personne légalement habilitée à communiquer les données et la connaissance présumée du lieu de situation des données au moment de la réception ou de l'accès.

46. La situation actuelle en matière de coopération internationale porte en elle le risque de voir apparaître des groupes de pays disposant des pouvoirs et des procédures nécessaires pour coopérer entre eux, alors que pour tous les autres, il faille s'en tenir aux modes de coopération internationale "traditionnels", qui ne tiennent pas compte des spécificités de la preuve électronique et du caractère mondial de la cybercriminalité. Tel est en particulier le cas pour la coopération en matière d'enquêtes. Faute d'approche commune, y compris dans les instruments multilatéraux de lutte contre la cybercriminalité en vigueur, les requêtes portant sur des mesures telles que la conservation rapide de données en dehors de pays tenus par leurs obligations internationales d'y pourvoir sur demande peuvent être difficiles à satisfaire. L'inclusion de ce pouvoir dans le projet de Convention de l'Union africaine sur la cybersécurité (projet de Convention sur la création d'un cadre juridique crédible pour la cybersécurité en Afrique) peut dans une certaine mesure contribuer à combler cette lacune. D'une manière générale, le fait que les dispositions relatives à la coopération des instruments multilatéraux et bilatéraux ont des champs d'application différents, l'absence d'obligation de répondre dans un délai donné, l'absence d'accord autorisant l'accès direct aux données extraterritoriales, la multiplicité des réseaux policiers informels et les écarts entre les garanties offertes en matière de coopération nuisent beaucoup à l'efficacité de la coopération pénale internationale en matière de preuve électronique.

8. Prévention de la cybercriminalité

47. La prévention de la criminalité englobe des stratégies et des mesures qui visent à réduire les risques d'infractions et les effets préjudiciables que ces dernières peuvent avoir sur les personnes et sur la société. Les pays ayant répondu ont déclaré soit qu'il existait une loi ou une politique nationale relative à la prévention de la cybercriminalité (près de 40 %), soit que des initiatives étaient en cours (20 %). Les pays ont mis en avant comme bonnes pratiques en matière de prévention de la cybercriminalité la promulgation de textes législatifs, l'exercice efficace de l'autorité, le renforcement des capacités de la justice pénale et des services répressifs, l'éducation et la sensibilisation, la constitution d'une solide base de connaissances et la coopération au sein des pouvoirs publics, des collectivités et du secteur privé, ainsi qu'au niveau international. Plus de la moitié des pays ont signalé l'existence de stratégies de lutte contre la cybercriminalité. Dans de nombreux cas, ces stratégies sont étroitement intégrées dans des stratégies de cybersécurité. Environ 70 % des stratégies nationales dont il a été fait état comprennent des volets relatifs à la sensibilisation, à la coopération internationale et aux capacités répressives. Les organes les plus souvent cités comme principaux responsables de la coordination en matière de lutte contre la cybercriminalité sont la police et le ministère public.

48. Des enquêtes montrent que la plupart des utilisateurs d'Internet prennent désormais des précautions élémentaires en matière de sécurité, y compris dans les pays en développement. Dans leurs réponses, les gouvernements, les entités du secteur privé et les institutions universitaires ont souligné l'importance que continuaient de revêtir les campagnes de sensibilisation du public, notamment celles

portant sur les nouvelles menaces ou s'adressant à des auditoires spécifiques comme les enfants. L'éducation des utilisateurs est plus efficace lorsqu'elle est associée à des systèmes qui les aident à atteindre leurs objectifs de manière sécurisée. Si les mesures de sécurité ont pour l'utilisateur un coût supérieur au profit direct qu'elles lui procurent, celui-ci ne sera guère incité à les appliquer. Les entités du secteur privé ont également déclaré que la sensibilisation des utilisateurs et du personnel devait faire partie intégrante d'une approche globale de la sécurité. Un certain nombre de principes fondamentaux et de bonnes pratiques ont été mentionnés, notamment l'application du principe de responsabilité en ce qui concerne la sensibilisation, les politiques et les pratiques de gestion des risques, l'efficacité de la direction et la formation du personnel. Les deux tiers des répondants du secteur privé ont effectué une évaluation des risques en matière de cybercriminalité et la plupart ont recours à des mesures de cybersécurité comme les pare-feu, la préservation des preuves numériques, l'identification des contenus, la détection d'intrusions et la surveillance et le contrôle des systèmes. On a cependant exprimé la crainte que les petites et moyennes entreprises ne prennent pas des mesures suffisantes pour protéger leurs systèmes ou pensent à tort qu'elles ne seront pas la cible d'attaques.

49. Les cadres réglementaires ont un rôle important à jouer dans la prévention de la cybercriminalité, aussi bien au niveau du secteur privé en général que des fournisseurs de services en particulier. Près de la moitié des pays ont adopté des lois relatives à la protection des données qui énoncent des règles concernant la protection et l'utilisation des données personnelles. Certaines prévoient des règles spécifiques applicables aux fournisseurs de services Internet et aux autres fournisseurs de communications électroniques. Bien que ces lois exigent que les données personnelles soient supprimées lorsqu'elles ne sont plus nécessaires, certains pays ont prévu pour les besoins des enquêtes pénales des exceptions qui obligent les fournisseurs de services Internet à stocker certains types de données pendant une période déterminée. De nombreux pays développés ont aussi des règles qui, en cas de violation de données, imposent aux organisations concernées d'en informer les intéressés et les organismes de réglementation. La responsabilité des fournisseurs de services Internet se limite en général à un simple rôle de "collecteur" de données. Cette responsabilité se trouve accrue en cas de modification du contenu des données transmises ou de connaissance réelle ou présumée d'une activité illégale. En revanche, elle se trouve réduite si des mesures sont prises rapidement comme suite à une notification. Bien que le filtrage du contenu Internet par les fournisseurs de services soit techniquement possible, les restrictions de l'accès à Internet sont subordonnées au respect des exigences de prévisibilité et de proportionnalité prévues par les dispositions du droit international relatif aux droits de l'homme visant à protéger la liberté de rechercher, de recevoir et de diffuser des informations.

50. Les partenariats public-privé jouent un rôle essentiel dans la prévention de la cybercriminalité. Plus de 50 % des pays ont fait état de tels partenariats, conclus pour la moitié d'entre eux sur la base d'un accord informel et pour l'autre moitié sur la base d'un accord juridique en bonne et due forme. Les entités du secteur privé arrivent en tête pour le nombre de partenariats conclus, suivies par les institutions universitaires et les organisations internationales et régionales. On a principalement recours à des partenariats pour faciliter l'échange d'informations sur les menaces et leur évolution, mais aussi pour mener des activités de prévention et intervenir dans

certaines affaires. Dans le cadre de certains partenariats public-privé, des entités du secteur privé ont effectivement mené des enquêtes et engagé des poursuites contre les auteurs d'actes de cybercriminalité. Ces interventions complètent celles des services répressifs et peuvent contribuer à réduire les préjudices subis par les victimes. Les institutions universitaires jouent divers rôles dans la prévention de la cybercriminalité, notamment en formant des spécialistes, en élaborant des règles de droit, des politiques et des normes techniques et en mettant au point des solutions. Des universités accueillent des experts en cybercriminalité, certaines équipes informatiques d'intervention rapide et des centres de recherche spécialisés, dont elles appuient également les travaux.

B. Résumé des principaux résultats de l'étude

51. Les principaux résultats ci-après se dégagent de l'étude approfondie sur le phénomène de la cybercriminalité:

a) Il se peut que la fragmentation au niveau international et la diversité des législations nationales sur la cybercriminalité soient corrélées à l'existence de multiples instruments dont la portée thématique et géographique diffère. Si ces instruments traduisent à juste titre des différences socioculturelles et régionales, les divergences concernant l'étendue des pouvoirs procéduraux et des dispositions sur la coopération internationale portent en elles le risque de voir apparaître une coopération par "groupes" de pays, laquelle n'est pas toujours la mieux adaptée à la nature mondiale de la cybercriminalité;

b) Le recours aux moyens traditionnels de coopération internationale formelle dans les affaires de cybercriminalité ne constitue pas à ce jour une solution suffisamment rapide pour obtenir des preuves électroniques instables par nature. Étant donné qu'un nombre croissant d'infractions obligent à recueillir des preuves électroniques en différents lieux géographiques, cette situation posera problème non seulement pour la cybercriminalité mais également pour toutes les formes de criminalité en général;

c) Dans un monde où se développent l'informatique en nuage et les centres de données, il est nécessaire de repenser le rôle de la "localisation" des éléments de preuve, notamment pour dégager un consensus autour des questions concernant l'accès direct à des données extraterritoriales par les services de répression;

d) L'analyse des cadres juridiques nationaux en place révèle l'insuffisance de l'harmonisation entre les "principaux" actes de cybercriminalité, les pouvoirs d'enquête et les règles d'admissibilité des preuves électroniques. Le droit international des droits de l'homme constitue un important point de référence externe pour les dispositions sur l'incrimination et les procédures;

e) Les services de répression, les procureurs et les juges des pays en développement ont besoin d'une assistance et d'un appui techniques complets, durables et viables pour pouvoir enquêter sur la cybercriminalité et combattre ce phénomène;

f) Les activités de prévention de la cybercriminalité doivent être renforcées dans tous les pays, grâce à une approche globale qui repose sur une sensibilisation plus poussée, sur des partenariats entre secteur public et secteur privé et sur

l'intégration des stratégies de lutte contre la cybercriminalité dans le cadre plus vaste de la cybersécurité.

C. Résumé des options contenues dans l'étude

52. Les options présentées dans l'étude établie par l'ONUDC reposent sur les réponses des pays à une question relative aux options envisageables pour renforcer les mesures, juridiques ou autres, prises aux échelons national et international contre la cybercriminalité et pour en proposer de nouvelles, ainsi que sur les principaux résultats. Selon l'étude, une ou plusieurs des options suivantes peuvent être envisagées[9]:

a) Élaboration de dispositions internationales types sur l'incrimination des principaux actes de cybercriminalité, afin d'aider les États à priver les délinquants de tout refuge en adoptant des infractions communes;

b) Élaboration de dispositions internationales types sur les pouvoirs d'enquête pour l'obtention de preuves électroniques, afin d'aider les États à se doter des outils procéduraux nécessaires pour enquêter sur les infractions nécessitant la collecte de preuves électroniques;

c) Élaboration de dispositions types sur la compétence, pour prévoir des chefs de compétence communs et effectifs dans les affaires pénales de cybercriminalité;

d) Élaboration de dispositions types sur la coopération internationale en matière de preuves électroniques, qui pourraient être incorporées dans des instruments bilatéraux ou multilatéraux, y compris une version révisée du Traité type des Nations Unies sur l'entraide judiciaire, comme le propose le Guide de discussion destiné au treizième Congrès des Nations Unies pour la prévention du crime et la justice pénale;

e) Élaboration d'un instrument multilatéral sur la coopération internationale concernant les preuves électroniques en matière pénale, de sorte à prévoir un mécanisme international permettant de coopérer rapidement pour conserver et obtenir des preuves électroniques;

f) Élaboration d'un instrument multilatéral global sur la cybercriminalité, afin de mettre en place une approche internationale en matière d'incrimination, de pouvoirs procéduraux, de compétence et de coopération internationale;

g) Renforcement des partenariats internationaux, régionaux et nationaux, notamment avec le secteur privé et les institutions universitaires, afin de fournir une assistance technique plus efficace pour prévenir et combattre la cybercriminalité dans les pays en développement.

---

[9] D'autres informations figurent dans le document UNODC/CCPCJ/EG..4/2013/2.

V. Recommandations concernant la promotion des activités visant à lutter contre la cybercriminalité, notamment l'assistance technique et le renforcement des capacités

53. La Commission souhaitera peut-être demander à l'ONUDC, à la lumière entre autres des activités exposées dans la section II du présent rapport, de continuer à fournir une assistance technique aux États Membres en matière de lutte contre la cybercriminalité et prier instamment les États Membres de verser des contributions extrabudgétaires à cette fin, en vue de renforcer à long terme et de manière durable les capacités de lutte contre la cybercriminalité des pays en développement.