Nations Unies E/CN.15/2013/25

Conseil économique et social

Distr. générale
19 février 2013
Français
Original: anglais

Commission pour la prévention du crime et la justice pénale
Vingt-deuxième session
Vienne, 22-26 avril 2012
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 la justice pénale

Note verbale en date du 19 février 2013 adressée à l'Office des Nations Unies contre la drogue et le crime par la Mission permanente de la République argentine auprès de l'Organisation des Nations Unies à Vienne

La Mission permanente de la République argentine auprès de l'Organisation des Nations Unies à Vienne présente ses compliments à l'Office des Nations Unies contre la drogue et le crime et a l'honneur de lui transmettre, en application de la résolution 2011/35 du Conseil économique et social en date du 28 juillet 2011, le rapport de la sixième réunion du groupe restreint d'experts sur la criminalité liée à l'identité, tenue à Vienne du 16 au 18 janvier 2013, rapport qu'elle le prie de bien vouloir communiquer sous forme de document officiel à la vingt-deuxième session de la Commission pour la prévention du crime et la justice pénale, qui doit se tenir à Vienne du 22 au 26 avril 2013.

La Mission permanente de la République argentine auprès de l'Organisation des Nations Unies à Vienne saisit cette occasion pour renouveler à l'Office des Nations Unies contre la drogue et le crime les assurances de sa très haute considération.

* E/CN.15/2013/1.

V.13-80750 (F)

Annexe à la note verbale datée du 19 février 2013, adressée à l'Office des Nations Unies contre la drogue et le crime par la Mission permanente de la République argentine auprès de l'Organisation des Nations Unies à Vienne

Rapport du groupe restreint d'experts sur la criminalité liée à l'identité sur les travaux de sa sixième réunion

Vienne, 16-18 janvier 2013*

I. Introduction

1. Suite à la publication en 2007 de l'étude des Nations Unies sur la fraude et l'abus et la falsification d'identité à des fins criminelles, établie à sa demande et présentée à la Commission pour la prévention du crime et la justice pénale à sa seizième session[1], et sur la base de ses mandats découlant des résolutions 2004/26 et 2007/20 du Conseil économique et social, l'ONUDC a lancé une plate-forme de consultation sur la criminalité liée à l'identité. L'objectif de la plate-forme était de réunir des représentants des gouvernements, du secteur privé ainsi que des milieux universitaires, et des représentants d'organisations internationales et intergouvernementales pour mettre en commun des données d'expérience, élaborer des stratégies, faciliter la poursuite des travaux de recherche et convenir de mesures pratiques pour lutter contre la criminalité liée à l'identité. La plate-forme est devenue opérationnelle avec les travaux du groupe restreint d'experts, qui a été créé en 2007.

2. À ses cinq précédentes réunions, le groupe restreint a élaboré une série de principes directeurs pour orienter les activités à venir, comme la réalisation de recherches supplémentaires, l'intensification des consultations avec le secteur privé, la préparation de rapports de recherche, la compilation d'exemples de législation pertinente, l'élaboration de documents sur la meilleure manière de promouvoir la coopération internationale pour lutter contre la criminalité liée à l'identité, et la compilation des meilleures pratiques en matière de protection des victimes. Ses travaux ont en outre conduit à la publication d'un manuel sur la criminalité liée à l'identité intitulé *Handbook on Identity-related Crime* (2011), qui comprend un guide pratique sur la coopération internationale dans la lutte contre cette forme de criminalité qu'il est prévu d'utiliser à des fins didactiques dans les programmes d'assistance technique et les activités de renforcement des capacités pour parfaire les connaissances spécialisées dont on dispose sur les moyens de traiter les problèmes juridiques, institutionnels et opérationnels relatifs à la nouvelle forme de criminalité qu'est la criminalité liée à l'identité[2].

3. Dans sa résolution 2011/35 en date du 28 juillet 2011, le Conseil économique et social a salué les efforts déployés par l'Office des Nations Unies contre la drogue

---

* La version originale anglaise du présent rapport n'a pas été revue par les services d'édition.

[1] E/CN.15/2007/8 et Add.1 à 3.

[2] On trouvera des informations plus complètes sur les travaux des réunions précédentes du groupe restreint à l'adresse www.unodc.org/unodc/en/organized-crime/emerging-crimes.html#Identity_related_crime.

et le crime pour faciliter les travaux du groupe restreint d'experts sur la criminalité liée à l'identité.

4. Dans la même résolution, le Conseil a également prié l'Office des Nations Unies contre la drogue et le crime, agissant en consultation avec la Commission des Nations Unies pour le droit commercial international, de poursuivre ses efforts visant à promouvoir une compréhension mutuelle et un échange de vues entre les entités des secteurs public et privé sur les questions se rapportant à la fraude économique et à la criminalité liée à l'identité et, en particulier, d'axer les travaux futurs du groupe restreint d'experts sur la criminalité liée à l'identité sur, entre autres, les diverses questions liées à l'utilisation des ressources et de l'expertise du secteur privé dans la mise en place et la fourniture d'une assistance technique en la matière.

5. Dans la résolution 2011/35, le Conseil a en outre prié l'Office des Nations Unies contre la drogue et le crime de poursuivre, notamment via le groupe restreint d'experts sur la criminalité liée à l'identité, ses efforts visant à recueillir des informations et des données sur les problèmes que posent la fraude économique et la criminalité liée à l'identité dans différentes régions géographiques.

6. La sixième réunion du groupe restreint a été convoquée du 16 au 18 janvier 2013 à Vienne, conformément aux mandats contenus dans la résolution 2011/35 du Conseil économique et social.

II. Organisation de la réunion

A. Ouverture de la réunion

7. La réunion a été ouverte le 16 janvier 2013 par le Directeur de la Division des traités de l'Office des Nations Unies contre la drogue et le crime, qui, après avoir remercié les participants de leur présence, est revenu sur les travaux préparatoires du groupe restreint. Il a souligné que la composition du groupe restreint s'inscrivait dans le cadre d'une approche multipartite visant, d'une part, à faciliter un échange de vues, d'informations et de connaissances spécialisées entre différentes parties, d'autre part, à promouvoir une compréhension mutuelle et la coopération dans la lutte contre la criminalité liée à l'identité. Il a également insisté sur le fait que le groupe restreint avait réussi à mettre bien en vue la question des problèmes que posent la criminalité liée à l'identité en tant que forme de criminalité distincte, "nouvelle et émergente" dans les débats de diverses instances internationales traitant de la prévention du crime et de la justice pénale (Commission pour la prévention du crime et la justice pénale, Congrès des Nations Unies pour la prévention du crime et la justice pénale, Conférence des Parties à la Convention des Nations Unies contre la criminalité transnationale organisée et Conférence des États parties à la Convention des Nations Unies contre la corruption).

8. Dans ses observations préliminaires, le Président du groupe restreint, l'Ambassadeur Eugenio Curia, représentant du Gouvernement argentin à Vienne, a rappelé le texte portant autorisation de l'organisation de la réunion et présenté brièvement chacun des points à son ordre du jour.

B. Participation

9. Les experts suivants ont participé à la réunion:

a) Secteur public

Eugenio Curia, Ambassadeur, Représentant permanent de l'Argentine auprès de l'Organisation des Nations Unies à Vienne (Argentine) (Président du groupe restreint); *John Unsworth*, Directeur adjoint Chef du renseignement et des interventions à la National Fraud Intelligence Bureau (NFIB) de la Police de la ville de Londres (Royaume-Uni); *Jonathan Rusch*, Chef adjoint chargé des stratégies et des politiques à la Section de la fraude de la Division criminelle du Ministère de la Justice (États-Unis d'Amérique).

b) Secteur privé

Anko Blokzijl, Président, Safran Morpho (Pays-Bas); *Fons Knopjes*, Centre de gestion de l'identité (Pays-Bas); *Pat Cain*, Chargé de recherche résident, Groupe de travail sur la lutte contre le hameçonnage (États-Unis d'Amérique); *Ferdinand Piatti*, Price Waterhouse Coopers (Autriche); *Sébastien Saillard*, Chargé de projets internationaux, RESOCOM (France); *Matthew Allen*, Directeur chargé de la criminalité financière, Association des banquiers britanniques (BBA) (Royaume-Uni); *Andrew Webster*, Responsable au Groupe de la conformité en matière de criminalité financière internationale (EMEA) de l'Association des banquiers britanniques (BBA) (Royaume-Uni); *Jonathan Shatford*, Chef des investigations (EMEA), Association des banquiers britanniques (BBA) (Royaume-Uni).

c) Organisations internationales et intergouvernementales

Jae Sung Lee, Secrétaire du Groupe de travail IV (Commerce électronique), Commission des Nations Unies pour le droit commercial international (CNUDCI); *Kate Lannan*, juriste à la Division du droit commercial international du Bureau des affaires juridiques, Commission des Nations Unies pour le droit commercial international (CNUDCI); *Christopher Hornek*, Directeur du programme de la sécurité des documents de voyage, Unité d'action contre le terrorisme, Département contre les menaces transnationales, Organisation pour la sécurité et la coopération en Europe (OSCE); *Paul Picard*, Spécialiste de la lutte contre le terrorisme, Organisation pour la sécurité et la coopération en Europe (OSCE).

d) Universitaires/experts siégeant à titre personnel

Gilberto Martins de Almeida, Martins de Almeida Advogados (Brésil); *Marco Gercke*, Professeur de droit pénal, Université de Cologne (Allemagne); *Nikos Passas*, Northeastern University, Faculté de criminologie et de justice pénale, Boston (États-Unis d'Amérique).

e) Secrétariat

Dimosthenis Chrysikos, Spécialiste de la prévention du crime et de la justice pénale, Service de la lutte contre la corruption et la criminalité économique, Section de l'appui à la Conférence, Division des traités, Office des Nations Unies contre la

drogue et le crime; *Arnaud Chaltin*, Spécialiste adjoint de la prévention du crime et de la justice pénale, Section de l'appui à la Conférence, Service de la lutte contre la corruption et la criminalité économique, Division des traités, Office des Nations Unies contre la drogue et le crime; *Steven Malby*, Spécialiste du contrôle des drogues et de la prévention du crime, Section de l'appui à la Conférence, Service de la criminalité organisée et du trafic illicite de la Division des traités, Office des Nations Unies contre la drogue et le crime.

C. Adoption de l'ordre du jour

10. L'ordre du jour de la réunion a été adopté comme suit:

1. Ouverture de la réunion.
2. Adoption de l'ordre du jour et organisation des travaux.
3. Criminalité liée à l'identité et cybercriminalité.
4. Approches comparatives: problèmes que pose la criminalité liée à l'identité dans différentes régions géographiques.
5. Éléments fondamentaux d'une stratégie nationale de lutte contre la criminalité liée à l'identité: exemples indicatifs.
6. Travaux menés par d'autres organisations internationales et intergouvernementales.
7. Assistance technique:
   a) Domaines d'intervention: mesures législatives, gestion de l'identité et prévention de la criminalité liée à l'identité;
   b) Participation du secteur privé à l'élaboration et à la fourniture de l'assistance technique: partenariats public-privé.
8. Présentation d'exemples indicatifs de projets universitaires comportant des aspects de prévention et de détection de la criminalité liée à l'identité.
9. Autres questions.
10. Conclusions recommandations sur les mesures à prendre.

III. Délibérations

A. Criminalité à l'identité et cybercriminalité

11. Le Secrétariat a fait part des progrès accomplis par le Groupe intergouvernemental d'experts sur la cybercriminalité dans ses travaux[3]. Il a été rappelé à cet égard que dans sa résolution 65/230 en date du 21 décembre 2010, l'Assemblée générale avait fait sienne la Déclaration de Salvador sur des stratégies globales pour faire face aux défis mondiaux: les systèmes de prévention du crime et

[3] Voir également E/CN.15/2013/24.

de justice pénale et leur évolution dans un monde en mutation, telle qu'adoptée par le douzième Congrès des Nations Unies pour la prévention du crime et la justice pénale. Dans cette résolution, l'Assemblée avait prié la Commission pour la prévention du crime et la justice pénale de créer, conformément au paragraphe 42 de la Déclaration de Salvador, un groupe intergouvernemental d'experts à composition non limitée chargé de faire une étude exhaustive du phénomène de la cybercriminalité et des mesures prises par les États Membres, la communauté internationale et le secteur privé pour y faire face, notamment l'échange d'informations sur les législations nationales, les meilleures pratiques, l'assistance technique et la coopération internationale, en vue d'examiner les options envisageables pour renforcer les mesures, juridiques ou autres, prises aux échelons national et international face à la cybercriminalité et pour en proposer de nouvelles.

12. Le Groupe intergouvernemental d'experts sur la cybercriminalité a tenu sa première réunion à Vienne du 17 au 21 janvier 2011. À cette occasion, il a passé en revue et adopté un ensemble de thèmes ainsi que la méthodologie de l'étude qui prévoyait la distribution d'un questionnaire aux États Membres, à des organisations intergouvernementales et à des représentants du secteur privé et d'établissements universitaires. Des réponses au questionnaire ont été reçues de 69 États Membres de différents groupes régionaux. Des réponses ont également été reçues de 50 entreprises. La collecte des informations a été faite par le Secrétariat entre février et juillet 2012 conformément à la méthodologie. Le Secrétariat a par la suite établi, sur la base des informations recueillies, un résumé analytique du projet d'étude, pour examen à la deuxième réunion à Vienne, du 25 au 28 février 2013, du Groupe intergouvernemental d'experts sur la cybercriminalité[4], qui devra se prononcer sur l'état d'avancement de l'étude.

13. Des informations sur la législation pénale relative à la cybercriminalité ont été recueillies au moyen du questionnaire, ainsi que par l'analyse de textes législatifs de plus de 100 pays constituant des sources primaires. Le questionnaire faisait référence à 14 actes généralement inclus dans la notion de cybercriminalité. Les réponses fournies par les pays ont montré que ces 14 actes étaient 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")[5]. S'agissant de ces 14 actes, 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

[4] Voir UNODC/CCPCJ/EG.4/2013/2.

[5] 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; 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"); et actes informatiques visant à faciliter les infractions terroristes.

pouvait être utilisée dans le cas des actes informatiques constituant une atteinte à l'identité. S'agissant plus particulièrement des infractions d'atteinte à l'identité signalées, la cible variait et concernait notamment les données personnelles et les informations d'identification.

14. Il a été noté que, d'une manière générale, les services de répression constataient 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.

15. L'étude a également fait 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.

16. Le groupe restreint a souligné qu'il fallait prendre des mesures efficaces contre l'utilisation de systèmes sophistiqués pour commettre des infractions de cybercriminalité dont l'abus et la falsification d'identité à des fins criminelles. Un participant a rappelé que, face à la multiplication de cas où des particuliers ne prenaient aucune précaution pour bien se protéger, il importait de mettre en œuvre des programmes de sensibilisation et de protection des victimes. Quelques participants ont appelé l'attention sur la nécessité de renforcer les capacités nationales pour lutter contre ces infractions dans les pays en développement en particulier.

B. Approches comparatives: problèmes que pose la criminalité liée à l'identité dans différentes régions géographiques

17. Conformément à la pratique établie à ses précédentes réunions, le groupe restreint a servi de cadre pour présenter et comparer les questions de criminalité liée à l'identité dans différentes régions géographiques. À cet égard, deux interventions ont été faites: l'une, par M. Marco Gercke sur l'évolution de la criminalité liée à l'identité dans l'Union européenne, les Caraïbes et en Asie et dans le Pacifique, et l'autre, par M. Gilberto Martins de Almeida, le nouveau cadre juridique brésilien de la lutte contre la cybercriminalité et la criminalité liée à l'identité.

18. M. Gercke a tout d'abord souligné que, si au sein de l'Union européenne, le droit pénal restait pour une large part un processus déterminé par les États, le Traité modificatif de Lisbonne donnait pour la première fois aux organes de l'Union, au-delà de la simple coopération intergouvernementale, un mandat fort dans le domaine du droit pénal, y compris de la cybercriminalité. Des travaux étaient

actuellement menés sur deux projets de directive contre la pornographie impliquant des enfants, d'une part et les attaques contre les systèmes informatiques, d'autre part. De même, en son article 77, le Traité énonce un mandat sur les "politiques relatives aux contrôles aux frontières, à l'asile et à l'immigration", qui traite aussi de questions concernant la sauvegarde de l'intégrité et de la sécurité des documents d'identité.

19. Le Plan d'action 2010-2014 adopté par l'Union européenne pour mettre en œuvre le programme de Stockholm sur "Une Europe ouverte et sûre qui sert et protège les citoyens"[6] recommande que les États envisagent de soumettre de nouveaux projets de loi, notamment sur la cybercriminalité et la sécurité des réseaux d'information. Sur cette base, une étude d'impact d'une proposition de nouveau cadre juridique pour la répréhension de l'usurpation d'identité a été lancée en 2012. Le projet de l'étude, qui a été récemment soumis à la Commission européenne, a tenu compte, dans son contenu, des travaux du groupe restreint, dans la mesure il avait été demandé à l'ONUDC de faire part de ses observations au cours de la phase préparatoire de compilation des informations. Selon M. Gercke, les abus d'identité ne sauraient en soi être incriminés de manière efficace sans un système unifié de gestion de l'identité et les États membres de l'Union européenne ne seraient pas encore prêts à aller dans cette direction.

20. M. Gercke a également présenté trois projets conjoints de l'Union européenne et de l'Union internationale des télécommunications dont l'objectif est d'harmoniser les législations sur la cybercriminalité dans les Caraïbes, les pays insulaires du Pacifique et l'Afrique subsaharienne, grâce à l'établissement de législations types et à la fourniture d'une assistance technique pour leur mise en application dans chacun des pays concernés. Le premier projet, mené dans les Caraïbes, qui est aujourd'hui en passe d'être terminé, a commencé par un examen complet des législations des 15 pays sélectionnés et une étude régionale comparative. Des experts nationaux ont pris part à tout le processus. Une stratégie de mise en application de la nouvelle législation dans chacun des pays a également été élaborée. Le projet a été axé pour l'essentiel sur le développement de la compétitivité par l'harmonisation des politiques des technologies de l'information et de la communication et des procédures législatives et réglementaires. Grâce à une approche constructive, les pays ciblés ont pu adopter, dans le domaine de la cybercriminalité, des normes qui vont au-delà de celles établies par la plupart des pays européens. La pérennité du projet a été assurée par la participation d'experts nationaux dès les premières phases et pendant tout le processus, ce qui leur a permis de recevoir une formation spécifique. Le rôle joué par les bureaux de pays pour identifier les acteurs compétents est ressorti comme un des facteurs clefs de succès. Les leçons tirées de ces processus peuvent être consultées sur le site Web de l'UIT.

21. C'est la même approche qui a été suivie dans les deuxième et troisième projets présentés par M. Gercke. Le deuxième projet, lancé en 2011 à la demande des pays insulaires du Pacifique, était axé sur le renforcement des capacités et la formation dans le domaine des politiques et des réglementations relatives aux technologies de l'information et de la communication. Le troisième projet, mis en œuvre en Afrique subsaharienne pour harmoniser les politiques relatives aux technologies de l'information et de la communication dans la région, a été lancé début 2012.

---

[6] Voir Journal officiel de l'Union européenne, C 115/1, 4 mai 2010.

22. Dans les discussions qui ont suivi, les participants ont souligné qu'il était important d'élaborer des normes et en particulier, des législations types, et insisté sur le rôle que l'Organisation des Nations Unies pourrait jouer à cet égard. Il a toutefois été également souligné qu'il serait nécessaire de mettre en place, dans les pays qui disposaient déjà d'une législation, des mécanismes de sensibilisation et des formations sur l'application de ces normes.

23. M. Gilberto Martins de Almeida a, lui, fait une présentation sur l'évolution du "paysage législatif" brésilien de la cybercriminalité. Après un bref aperçu historique, il s'est appesanti sur la récente "vague" d'action normative qui a été menée selon une approche intégrée et qui a été rendue nécessaire par les problèmes que pose la criminalité liée à l'identité. Selon certaines informations, au Brésil, un consommateur serait victime de cette infraction toutes les 15 secondes. Les formes les plus courantes sont l'usurpation d'identité visant les cartes de crédits, l'achat d'articles électroniques et de téléphones mobiles et l'ouverture de comptes bancaires sur la base d'informations d'identification fausses ou falsifiées. Il a été souligné que, dans le cadre de la criminalité liée à l'identité, on était passé de l'utilisation de virus à celle de scanners, cette dernière méthode consistant à utiliser un robot pour détecter les vulnérabilités. Il a également été relevé que les attaques étaient essentiellement perpétrées au niveau national.

24. L'initiative législative brésilienne comprend un ensemble de 11 projets de lois dont certains ont déjà été approuvés (notamment celui sur la cybercriminalité et celui sur les libertés civiles). Pour le reste, en particulier les lois sur la liberté d'information, la cybercriminalité, la protection des données personnelles, les transactions électroniques, le commerce électronique (le code du consommateur), le paiement mobile, les nouveaux protocoles Internet, les normes procédurales (et techniques) et les règles et règlements (en matière de sécurité, de la Securities Exchange Commission), des consultations sont à un stade avancé en vue de leur mise en forme définitive et de leur approbation.

25. Les deux projets de lois approuvés ont été adoptés le même jour en décembre 2012. Ils se complètent, le premier étant axé sur des questions de fond plus pointues et le deuxième sur des questions de nature procédurale. La complémentarité de ces deux instruments législatifs s'inscrit dans le cadre d'une approche cohérente, qui s'illustre davantage par la similitude de leur terminologie, le fait qu'ils aient été rédigés en tenant compte des mêmes normes internationales (les normes ISO en l'occurrence) et l'objectif commun qu'ils poursuivent en énonçant des mesures préventives et répressives.

26. M. Martins de Almeida a indiqué que la définition utilisée dans les projets de lois approuvés couvrait aussi bien l'invasion que l'installation de vulnérabilités en vue d'obtenir un avantage illicite. Des circonstances aggravantes sont prévues pour ceux qui produisent, offrent, distribuent, vendent ou diffusent un dispositif ou un programme informatique pour obtenir cet avantage illicite, si l'on obtient le contenu de communications électroniques privées, de secrets commerciaux ou d'informations confidentielles, si un utilisateur non autorisé accède à distance au dispositif ou si, en cas de publication, le contenu des informations obtenues est commercialisé ou transféré aux tiers comme une simple marchandise. Une plate-forme unique d'établissement et de suivi des normes a été mise en place à l'intention des différentes institutions nationales.

C. Éléments fondamentaux d'une stratégie nationale de lutte contre la criminalité liée à l'identité: exemples indicatifs

27. Au titre de ce point de l'ordre du jour, les présentations et les débats se sont articulés autour de l'élaboration d'un cadre relatif aux éléments fondamentaux d'une stratégie nationale sur la prévention, les enquêtes, les poursuites et la condamnation de la criminalité liée à l'identité. À cet égard, le Secrétariat a indiqué que la question de l'élaboration d'un tel cadre avait été soulevée pour la première fois par le Conseil économique et social au paragraphe 6 f) de sa résolution 2009/22. Le Secrétariat a par ailleurs présenté un document qui avait été établi par le Rapporteur du groupe restreint, absent de la réunion[7]. Des indications étaient données dans ce document sur les partenaires ou les participants possibles, du secteur public comme du secteur privé, à une stratégie nationale. Le processus à suivre pour élaborer, mettre en œuvre et poursuivre une telle stratégie y était également décrit, de même que ses éléments les plus importants, en particulier l'évaluation des menaces et la compilation et l'analyse des informations pertinentes qui interviennent au cours de la phase initiale; la définition des priorités et la coordination; les aspects législatifs; les enquêtes, la détection et la répression; le volet prévention; le renforcement des capacités; les questions relatives aux ressources; et les mécanismes visant à renforcer la coopération entre les secteurs public et privé.

28. La stratégie nationale adoptée par les États-Unis d'Amérique pour résoudre les problèmes que pose la criminalité liée à l'identité a été présentée par M. Jonathan Rusch. Les États-Unis ont promulgué en 1998 la loi pour la dissuasion du vol et de l'usurpation d'identité (*Identity Theft and Assumption Deterrence Act*) qui a érigé, pour la première fois, le vol d'identité en infraction pénale spécifique. L'année suivante, un sous-comité sur le vol d'identité a été créé au sein du comité de la criminalité en col blanc du Procureur général. En 2006, une Équipe spéciale de la présidence chargée du vol d'identité a été constituée, avec le Procureur général à sa tête. L'Équipe spéciale a adopté un plan stratégique en 2007.

29. La stratégie porte sur les trois phases du "cycle de vie" du vol d'identité (tentative d'acquisition des informations personnelles de la victime; utilisation abusive des informations personnelles; et jouissance du produit du crime pendant que la victime prend conscience du mal qui lui a été fait). Elle met elle-même en évidence les principaux domaines où des améliorations devraient être apportées: la prévention (protéger les données sensibles et rendre difficile aux auteurs de l'infraction l'utilisation de données volées); réadaptation de la victime (aider la victime à se réadapter); dissuasion grâce à l'intensification des poursuites et à l'imposition de peines plus sévères.

30. S'agissant des solutions de prévention mises en œuvre dans le secteur public, M. Rusch a évoqué les pratiques visant à restreindre l'emploi inutile de numéros de sécurité sociale, ainsi que les programmes de formation offerts aux agents fédéraux sur la protection des données et les mesures adoptées pour lutter efficacement contre leur utilisation abusive. Parallèlement, des solutions ont été identifiées pour le secteur privé, notamment l'établissement de normes pour la protection des données et d'exigences de notification en cas de violation, la constitution de fichiers

[7] Voir E/CN.15/2013/CRP.2.

complets des numéros de sécurité sociale utilisés dans le secteur privé, l'organisation de formations plus pointues sur la protection des données, la réalisation d'enquêtes sur la violation de la sécurité des données et de campagnes de sensibilisation. Pour ce qui est de la réadaptation des victimes, la stratégie met l'accent sur les priorités ci-après: formation des agents qui fournissent une assistance directe aux victimes; assistance individualisée des victimes; modification des statuts de restitution pénale pour que les victimes recouvrent la valeur du temps passé à se remettre du tort qu'elles ont subi; et évaluation de l'efficacité des outils dont disposent les victimes. Dans le domaine de la détection et de la répression, la stratégie est essentiellement axée sur la coordination et l'échange d'informations, notamment avec la création d'un centre national, l'utilisation d'un formulaire unique pour les rapports et un échange de données et d'informations plus efficace (actuellement près de 40 États disposent de leurs propres normes pour signaler les cas de vol d'identité). Les autres activités prioritaires relatives à la détection et à la répression concernent l'intensification des poursuites de la criminalité liée à l'identité, la coordination avec les services homologues étrangers, la formation et le suivi menés pour mesurer le succès des opérations.

31. M. Rusch a en outre indiqué que l'implication accrue de groupes criminels organisés dans la criminalité liée à l'identité était également une source de préoccupation prise en compte dans la stratégie. Une des difficultés rencontrées à cet égard était l'utilisation de documents à des fins d'identification et au-delà de leur destination d'origine. Il importait donc de comprendre comment opéraient les groupes criminels organisés pour pouvoir les combattre efficacement. Il importait également de s'ouvrir au secteur privé pour mettre en place un ensemble pratique de mesures conjointes.

32. Pour assurer le suivi de la stratégie adoptée par les États-Unis, un groupe de travail interorganisations sur la répression de la criminalité liée à l'identité, constitué en 2008, a organisé des réunions mensuelles et séances d'information animées par des chercheurs du secteur privé. Un groupe de travail international sur la criminalité liée à l'identité a également été créé avec la participation du Canada, des États-Unis et du Royaume-Uni. Quelques-unes des recommandations formulées par le groupe restreint ont également été prises en compte. D'une manière générale, l'orateur était d'avis que, même si on ne pouvait s'en satisfaire, la lutte contre la criminalité liée à l'identité dans la situation actuelle était plus efficace depuis qu'avaient été adoptées les mesures politiques susmentionnées. Par conséquent, il est essentiel que l'on évalue régulièrement le chemin parcouru.

33. M. John Unsworth a présenté les travaux menés par le Ministère de l'intérieur du Royaume-Uni sur la criminalité liée à l'identité. Le Bureau national du renseignement sur la fraude s'est vu confié la mise à jour de l'évaluation faite en 2010 dans ce domaine. Les travaux ont été menés en partenariat avec toutes les forces nationales de détection et de répression, des partenaires privés et les départements du Ministère de l'intérieur. La collecte d'informations complètes sur les questions pertinentes reste un enjeu important et pour ce faire, il s'avère crucial d'établir des relations avec d'autres secteurs. Même si le public est de plus en plus sensibilisé à la menace, beaucoup reste à faire en matière de protection. Il existe aussi un lien entre la criminalité liée à l'identité et d'autres infractions, la criminalité organisée en l'occurrence. M. Unsworth a indiqué que, selon l'évaluation, près de 1,8 millions de personnes sont victimes de vol d'identité

chaque année (une personne toutes les 20 secondes). Mais une bonne partie de ces infractions ne sont probablement pas signalées. Autre conséquence, environ 2,5 milliards de crédits d'impôt sont indûment versés en raison de pratiques frauduleuses.

34. M. Unsworth a fait observer que, parce qu'ils se focalisent souvent sur l'infraction finale, les services de détection et de répression pourraient manquer de cibler directement les infractions liées à l'identité commises aux premiers stades de l'activité criminelle. Le Ministère de l'intérieur reconnaît qu'une approche multisectorielle et des mesures plus rationnelles s'imposent pour faire face à la menace que pose cette forme de criminalité. Dans ce contexte, une stratégie multisectorielle a été élaborée par le Conseil de mise en œuvre de la stratégie de lutte contre la criminalité liée à l'identité, qui poursuit des objectifs à différents niveaux: assurer l'intégrité des documents (donner aux entreprises et au secteur public plus de moyens pour vérifier et authentifier les informations d'identification, en ligne ou en personne); renforcer les mesures de détection et de répression (cibler efficacement les ressources pour porter un coup aux activités criminelles perpétrées dans la création, le vol et la diffusion d'identités fausses ou d'emprunt); promouvoir la prévention (communiquer aux secteurs public et privé les données recueillies sur les fausses identités afin d'empêcher la commission d'autres infractions); et promouvoir des programmes de formation (sensibiliser les personnes et les entreprises pour leur permettre de se protéger elles-mêmes). Cette stratégie fait constamment l'objet d'un suivi pour faciliter son application.

35. À l'issue des présentations, les participants sont convenus que l'existence et la mise en œuvre de stratégies nationales visant à prévenir et à combattre la criminalité liée à l'identité pourraient jouer un rôle considérable dans l'attention portée à ce phénomène et dans l'affectation et l'utilisation efficace des ressources qui lui sont consacrées, dans le cadre d'efforts coordonnés de lutte contre la criminalité en général, de la poursuite d'objectifs d'intérêt public et de la défense des activités et des intérêts du secteur privé. Ces stratégies peuvent aussi jouer un rôle important au niveau international, pour ce qui est de clarifier les politiques, les législations et les stratégies mises en œuvre par chaque pays et de servir de base de discussions ou de négociations sur la coordination et la coopération entre États Membres. Cet aspect est particulièrement important en ce qui concerne la criminalité liée à l'identité parce qu'il touche un grand nombre de fonctions et d'intérêts sécuritaires, économiques et personnels et parce que les problèmes de criminalité liée à l'identité se posent pour la plupart en ligne et dans les systèmes numériques. Les participants sont convenus que si les modalités de ces stratégies pourraient différer d'un État Membre à l'autre, une liste-clef de leurs éléments constitutifs pourrait à tout le moins être établie pour que chaque État puisse s'en inspirer lorsqu'il envisagera d'élaborer sa propre stratégie.

36. À cet égard, les participants ont examiné le contenu d'une brève esquisse des éléments à inclure dans les stratégies nationales relatives à la prévention, aux enquêtes, aux poursuites et à la condamnation concernant la criminalité liée à l'identité. Cette esquisse a été établie par le Secrétariat sur la base du document élaboré par le Rapporteur (voir par. 27 ci-dessus) et des débats sur les exemples de pratiques nationales mentionnés au titre du point de l'ordre du jour y relatif. Le groupe restreint a fait, sur la structure et le contenu de l'esquisse, certaines propositions qui, telles que finalement convenues, sont jointes au présent rapport

(voir appendice II). Le groupe restreint a également décidé que le document élaboré par le Rapporteur soit amélioré et actualisé puis soumis, en tant que document de séance, à la Commission à sa vingt-deuxième session. La Commission voudra peut-être examiner l'esquisse et le document de séance en tant qu'outils d'orientation et inviter en outre les États Membres à communiquer au Secrétariat leurs points de vue sur la question d'une stratégie nationale contre la criminalité liée à l'identité.

D. Travaux d'autres organisations internationales et intergouvernementales

37. MM. Christopher Hornek et Paul Picard ont présenté les activités de l'OSCE dans le domaine de la gestion de l'identité. Les différents départements de l'OSCE abordent le problème selon des perspectives différentes: le Bureau des institutions démocratiques et des droits de l'homme (BIDDH) sous l'angle de la migration (enregistrement des faits d'état civil et des populations) ou des élections (bases de données d'électeurs), le Bureau du Coordonnateur des activités économiques et environnementales sous l'angle de la bonne gouvernance et de la gestion des migrations, etc. Cependant, le service chargé en priorité de ces questions est le Département contre les menaces transnationales, et plus particulièrement l'Unité d'action contre le terrorisme. L'OSCE concentre ses activités sur les aspects pratiques de la délivrance et de l'administration des documents, du renforcement de la gestion de l'identité, de la promotion du remplacement par des documents de meilleure qualité, notamment par la promotion des normes de l'Organisation de l'aviation civile internationale (OACI), et de la détection des faux documents dans le cadre des contrôles aux frontières.

38. L'OSCE a pris également part aux activités de divers groupes de travail chargés de cette question et a mené à bien plus de 55 projets depuis 2003, pour certains en coopération avec l'OACI, Interpol, l'Organisation internationale pour les migrations (OIM), l'Union européenne et l'Organisation internationale de normalisation (ISO). Elle met en œuvre des projets à long terme en République de Moldova, au Tadjikistan, en Ouzbékistan et au Kirghizistan. Par ailleurs, le Répertoire de clés publiques de l'OACI a été brièvement présenté. Il est disponible gratuitement sur Internet, mais le téléchargement de documents reste payant. En conclusion, l'accent a été mis sur les difficultés qu'il restait à résoudre pour améliorer la gestion de l'identité et mettre à niveau les contrôles aux frontières.

39. M. Jae Sung Lee a présenté les travaux réalisés par la Commission des Nations Unies pour le droit commercial international (CNUDCI) dans le domaine de la gestion de l'identité. La CNUDCI a joué un rôle précurseur dans l'élaboration de normes internationales relatives au commerce électronique dont s'inspirent les législations nationales. À cet égard, des indicateurs de fraude commerciale ont été adoptés en 2008. Avec l'utilisation croissante de communications électroniques dans le commerce international, pratiquement tous les groupes de travail de la CNUDCI examinent des questions s'y rapportant dans les délibérations relatives à leurs domaines respectifs. Bien qu'ils se concentrent sur l'aspect relatif à la facilitation du commerce de la gestion de l'identité, ils n'ont pas adopté de texte spécifique sur la question. À sa réunion d'octobre 2012, le Groupe de travail IV sur le commerce électronique a examiné les questions liées à la gestion de l'identité. Il a élaboré une

loi type sur le commerce électronique, qui décrit dans ses grandes lignes la gestion de l'identité, et une autre sur les signatures électroniques. Le groupe a en outre examiné la notion de système de gestion de l'identité, son modèle économique, les processus auxquels il fait appel, ses acteurs principaux et ses avantages potentiels. Les systèmes de gestion de l'identité ont été conçus pour permettre l'identification et l'authentification des utilisateurs cherchant à accéder aux services, en vue de promouvoir la confiance dans le commerce électronique. Un colloque tenu en 2011 a abouti à un large consensus sur l'utilité de la gestion de l'identité pour faciliter les transactions électroniques transfrontières. Il a été suggéré alors que la CNUDCI serait en excellente position pour travailler sur les aspects juridiques transnationaux de la gestion de l'identité. Ses travaux permettraient aussi de préciser le champ d'application des dispositions sur les signatures électroniques figurant dans ses textes, et faciliteraient le traitement de la gestion de l'identité dans le cadre d'autres sujets pouvant l'intéresser. Le Groupe de travail IV a donc été chargé d'examiner la question de la gestion de l'identité pour ce qui se rapporte aux documents transférables électroniques. Il est intéressant de noter que l'équipe juridique spéciale sur la gestion de l'identité de l'American Bar Association a soumis, en vue de son examen éventuel par le Groupe de travail, un document qui présentait la question de la gestion de l'identité dans son ensemble, son rôle dans le commerce électronique, ainsi que les questions juridiques connexes et les obstacles rencontrés.

40. La CNUDCI s'attache actuellement à suivre les diverses initiatives relatives à la gestion de l'identité, en vue de mieux définir les termes d'un futur mandat éventuel du groupe de travail. Par ailleurs, elle collabore avec l'Union européenne à l'élaboration d'une proposition de "Règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur". Entre autres activités qu'elle a eu à mener, on peut citer les suivantes: création d'une plate-forme d'interopérabilité pour les identités électroniques à l'échelle européenne (Secure Identity Across Borders Linked); coopération avec l'OIM sur les questions relatives à la gestion des frontières; coopération avec l'OASIS (Organization for the Advancement of Structured Information Standards) sur le commerce des identités; et mise en place d'un programme paneuropéen en ligne de passation des marchés publics.

E. Assistance technique domaines d'intervention: mesures législatives, gestion de l'identité et prévention de la criminalité liée à l'identité

41. Le groupe restreint a rappelé les précédents mandats dans lesquels un appel était lancé pour que soit apportée une assistance technique dans le domaine de la criminalité liée à l'identité (voir par. 7 et 8 de la résolution 2009/22 du Conseil économique et social) et fait le bilan des activités menées dans ce domaine, conformément à ses orientations et recommandations. À cet égard, il a été fait référence aux principales conclusions des délibérations antérieures du groupe restreint, notamment à l'élaboration de rapports de recherche sur les approches en matière d'incrimination, les questions de victimisation et les partenariats public-privé. Il a été fait mention notamment du manuel sur la criminalité liée à l'identité (Handbook on Identity-related Crime, disponible uniquement en anglais), qui comprend un guide complet destiné aux professionnels de la coopération

internationale en matière de lutte contre la criminalité liée à l'identité (voir par. 2 ci-dessus).

42. Dans ses débats sur d'autres questions d'assistance technique, le groupe restreint a rappelé que la plupart des activités qui seraient menées dans ce domaine dans l'avenir dépendraient des ressources disponibles, tant pour la préparation des supports d'assistance technique que pour la mise en œuvre effective des projets. Le groupe restreint s'est en outre accordé à reconnaître l'intérêt d'activités conjointes et de synergies entre les secteurs public et privé dans ce domaine. À cet égard, la prévention de la criminalité liée à l'identité, sous toutes ses formes, à savoir prévention sociale (éducation, sensibilisation), prévention situationnelle (faire face aux risques spécifiques de la victimisation ou former le personnel chargé de la détection de la criminalité liée à l'identité) et prévention technique (élaboration de mesures de sécurité techniques visant à garantir l'intégrité des documents), était un domaine qui se prêterait particulièrement bien à des initiatives communes.

43. Par ailleurs, le groupe est convenu qu'il était nécessaire de suivre une approche ciblée et de définir des domaines prioritaires si l'on souhaitait que les activités menées dans le cadre de l'assistance technique portent leurs fruits. De l'avis général, les mesures législatives étaient un domaine prioritaire et d'une importance cruciale. À cet égard, il a été convenu que l'assistance technique devrait être axée, avant tout, sur l'élaboration de cadres juridiques adéquats et adaptés à la lutte contre la criminalité liée à l'identité. Il s'agissait d'aider les États Membres à définir de nouvelles infractions, ou à actualiser celles déjà visées, pour combattre l'abus et la falsification d'identité à des fins criminelles, et sur la mise en place des outils et des instruments juridiques nécessaires pour mener efficacement des poursuites et des enquêtes en matière de lutte contre la criminalité liée à l'identité.

44. Compte tenu de ce qui précède, il a été convenu que l'élaboration d'une législation type sur la criminalité liée à l'identité pourrait s'avérer particulièrement utile aux États Membres qui souhaitaient pouvoir s'appuyer sur un ensemble de dispositions type pour structurer des mesures juridiques efficaces. M. Gercke a porté à l'attention du groupe restreint un modèle établi par ses soins, énumérant une liste de points à prendre en compte pour l'élaboration d'une législation type. M. Gercke a rappelé qu'il serait impossible d'incriminer efficacement les abus liés à l'identité en tant que tels sans un système unifié de gestion de l'identité. Pour cette raison, l'esquisse de législation type proposée sur la criminalité liée à l'identité (voir appendice I) comprend également des aspects de nature administrative, en rapport avec le programme relatif à la gestion de l'identité. Les États Membres souhaitant s'appuyer sur cette esquisse de législation type pourront ainsi définir eux-mêmes le champ d'application de leur cadre juridique, en gardant à l'esprit que les aspects relatifs à la gestion de l'identité pourront également être traités dans le contexte plus large d'une stratégie nationale en matière de criminalité liée à l'identité.

F. Engagement du secteur privé dans le développement et la fourniture d'une assistance technique: partenariats public-privé

45. Les représentants de la BBA (British Bankers Association) ont présenté les travaux menés par leur association pour lutter contre la criminalité financière, ainsi que leur coopération actuelle avec le secteur public. La BBA représente

200 institutions financières présentes dans 60 pays. Dans ce cadre, elle gère sept comités sur la criminalité financière, dont l'un concentre ses activités sur la fraude. Ces comités sont des organes de décision dont la tâche est notamment de communiquer des informations au gouvernement sur des questions de fond. La BBA transmet également au gouvernement les avis et préoccupations du secteur bancaire concernant par exemple l'échange, au sein de ce secteur, d'informations sur les opérations suspectes ou les difficultés posées par l'accroissement de la mobilité internationale de la clientèle. Le budget considérable consacré au problème, les efforts déployés pour la sécurisation des systèmes et le recrutement de personnel qualifié, issu pour une grande part des services de détection et de répression, sont autant de preuves de l'engagement du secteur bancaire dans la lutte contre la criminalité financière.

46. Les représentants de la BBA ont souligné l'importance des synergies entre secteurs public et privé et de la coopération entre ses membres et les services de détection et de répression, notamment pour ce qui était de la communication d'informations sur les moyens de détecter les opérations suspectes. La BBA joue en outre un rôle dans la stratégie nationale de lutte contre la fraude, et participe activement à d'autres initiatives public-privé, notamment à des campagnes de sensibilisation en ligne. De telles synergies sont fondamentales compte tenu du fait que la criminalité financière évolue constamment et que les nouveaux problèmes qu'elle pose ne pourront être surmontés que grâce à un engagement mutuel des deux secteurs. De même, une coopération pourrait être très utile dans le domaine de la lutte contre le blanchiment d'argent, ce domaine étant l'un des plus problématiques aux yeux des membres de la BBA. Il a été noté que les informations communiquées par le secteur privé pouvaient être d'une aide précieuse pour le développement d'un cadre législatif et politique relatif à la criminalité financière et au blanchiment d'argent. Le rôle de la communauté internationale dans la lutte contre la criminalité financière a également été souligné.

47. Les représentants de la BBA ont par ailleurs insisté sur le fait que la sensibilisation du public constituait un facteur déterminant. D'après leur expérience, les systèmes bancaires étaient bien protégés et n'étaient pas directement piratés. En revanche, les courriels des clients présentaient des vulnérabilités qui étaient souvent exploitées par les pirates pour accéder aux dossiers bancaires sous couvert de légitimité. Ils ont également fait valoir la diversité de la communauté bancaire. Par exemple, dans leur lutte contre la criminalité liée à l'identité, les banques d'affaires et les banques de détail auront probablement des intérêts divergents.

48. En réponse à une question soulevée par M. Gilberto Martins de Almeida concernant les nouveaux risques que pouvait engendrer l'utilisation croissante de nouveaux systèmes tels que le paiement par téléphone portable, M. Matthew Allen a fait valoir qu'il fallait prendre en compte les potentielles insuffisances d'autres secteurs, tels que ceux de la vente au détail ou des télécommunications, dans l'évaluation des risques liés à la criminalité financière. Certes, tous les nouveaux produits ne présentent pas le même niveau de risque, mais l'utilisation accrue de moyens technologiques comme le paiement par téléphone portable dans les pays en développement, par exemple, reste une gageure. La communauté internationale pourrait également avoir un rôle à jouer dans la lutte contre ce risque.

49. M. Sébastien Saillard a présenté les travaux de la société RESOCOM du Reso-Club. RESOCOM, qui se spécialise dans la lutte contre la criminalité liée à

l'identité, a développé des services Web qui permettent de vérifier l'authenticité des documents d'identification et des passeports de tous les pays. Plus de 2 millions de documents auraient été contrôlés par la société en 2011.

50. RESOCOM est l'un des membres fondateurs du Reso-Club, réseau dont l'objectif est de promouvoir des échanges et de bonnes pratiques entre professionnels des secteurs public et privé en matière de lutte contre la criminalité liée à l'identité. L'association Reso-Club organisera en octobre 2013 à Paris son Troisième forum européen sur la lutte contre la criminalité liée aux documents d'identité et d'identification. L'association s'emploie par ailleurs à élaborer des projets d'assistance aux victimes de la criminalité liée à l'identité.

51. À la lumière des présentations ci-dessus, le groupe restreint a débattu de l'élaboration d'un document décrivant et faisant la synthèse des expériences volontaires de partenariats public-privé menées à l'échelle internationale, pour montrer leur importance. Le groupe a autorisé par ailleurs la compilation dans un document d'expériences de partenariats public-privé réussies en matière de lutte contre la criminalité liée à l'identité dans différentes régions du monde. Un document regroupant de courtes descriptions de chacune de ces expériences (avantages, exprimés en chiffres et en statistiques), sans analyse argumentative/éditoriale, sera présenté dans un document de séance à la Commission pour la prévention du crime et la justice pénale à sa vingt-deuxième session.

52. Le groupe restreint a ensuite autorisé le Secrétariat à recueillir des informations plus complètes, notamment des exemples de cas pratiques, auprès des entités du secteur privé représentées à la réunion par l'intermédiaire de la BBA et du Reso-Club, sur les questions suivantes: les incidences de la criminalité liée à l'identité sur ces entités; la production de données quantitatives (chiffrées) et/ou qualitatives, y compris les évaluations et les opinions portant sur certains moyens de faire face aux problèmes que pose cette forme de criminalité; les types d'initiatives ou de mesures qui ont été prises par les entités du secteur privé pour améliorer la prévention de la criminalité liée à l'identité; les mesures qui ont été prises pour faire en sorte que les clients ne soient pas victimes de cette criminalité; les types de formations, s'il en existe, offertes aux employés et aux agents chargés de la détection des infractions liées à l'identité; les effets bénéfiques du renforcement des partenariats public-privé dans la prévention et la lutte contre la criminalité liée à l'identité; et les domaines dans lesquels les synergies entre les autorités et les institutions financières ou autres entités du secteur privé pourraient permettre d'engranger des résultats tangibles et probants.

G. Présentation d'exemples représentatifs de projets universitaires comportant des aspects relatifs à la prévention et à la détection de la criminalité liée à l'identité

53. L'exposé présenté au groupe restreint par M. Nikos Passas, aidé de ses collègues de l'université Northeastern de Boston (États-Unis) qui ont pris part à la réunion en téléconférence, a porté sur plusieurs projets élaborés – ou en cours d'élaboration à l'université et comportant des aspects relatifs à la prévention et à la détection de la criminalité liée à l'identité. Quelque peu comparable à une

opération d'infiltration dans le domaine de la cybercriminalité, le premier projet consistait à diffuser des données sur un réseau criminel pour comprendre le fonctionnement de la cyber-économie clandestine. "Mediascan", le second projet, s'adresse aux banques et aux institutions financières, avec comme objectif de détecter et suivre les opérations suspectes et irrégulières, qui s'appuient souvent sur l'usage impropre d'informations d'identification. Le troisième projet est axé sur l'analyse des pratiques en matière de dissimulation ou d'utilisation malveillante des identités dans le contexte des paiements informels et du blanchiment de capitaux fondé sur les activités commerciales.

H. Autres questions

54. M. Knopjes a présenté "Fidelity", un projet de l'Union européenne visant à déterminer les insuffisances et les vulnérabilités auxquelles le passeport électronique était soumis au cours de son cycle de vie, et à élaborer des solutions techniques et des recommandations en réponse à ces problèmes. D'une durée de 4 ans, ce projet réunit 19 partenaires (PME, secteur professionnel, utilisateurs finaux, universitaires) et consiste principalement à déterminer les SWOT (forces, faiblesses, menaces, opportunités) du passeport électronique pendant son cycle de vie. M. Knopjes a décrit différents problèmes survenant à diverses étapes du cycle de vie du passeport électronique, notamment lors du processus de délivrance (sécurité des certificats de naissance et des autres preuves d'identité) ou au moment de la révocation et de la destruction des puces. Il a été question de la gestion des certificats, de l'application des mesures de protection des données personnelles tout au long du processus et de la vérification de la qualité des données biométriques. L'orateur a fait observer qu'il devenait urgent d'établir des normes internationales minimales pour les certificats de naissance (voir ci-après) et les autres preuves d'identité si l'on souhaitait améliorer le niveau d'intégrité des documents d'identité.

55. De plus, M. Knopjes a fait un exposé sur les problèmes de sécurité posés par les documents sources, ceux-ci constituant la première forme d'identification à la naissance. Délivrés sous la responsabilité des autorités, ces documents posent souvent des problèmes de sécurité car il n'existe ni normes ni critères les régissant. L'orateur a appelé l'attention sur l'absence de normes internationales et la méconnaissance des documents sources des autres pays. Il n'existe actuellement sur ces documents aucune base de données dans laquelle les autorités pourraient puiser des informations sur les modèles en circulation, et les connaissances sur la question sont limitées. Par conséquent, il existe un risque que des documents sources contrefaits soient utilisés pour obtenir des cartes d'identité ou des passeports sécurisés valides.

56. Dans le même ordre d'idées, M. Knopjes a proposé une définition pratique de la gestion de l'identité en tant que système caractérisé par une philosophie, une politique et des instruments permettant aux autorités de gérer les identités de tous les citoyens. À cet égard, un tableau de l'infrastructure d'identité a été présenté au groupe restreint, afin d'illustrer les quatre phases du cycle de vie du document (création, utilisation et contrôle simultané, fin de vie). Pour chacune de ces phases, des explications techniques ont été fournies concernant les questions d'enregistrement, la procédure suivie et les compétences requises.

IV. Conclusions et recommandations sur les mesures à prendre

57. À la dernière session de la réunion, le 18 janvier 2013, le Président du groupe restreint a récapitulé comme suit les principales conclusions des délibérations:

a) Élaboration d'une esquisse de législation type sur la criminalité liée à l'identité; et

b) Élaboration d'une liste de contrôle des éléments stratégiques à prendre en compte dans le développement de stratégies nationales en matière de prévention, d'enquêtes, de poursuites et de sanctions concernant la criminalité liée à l'identité.

Ces deux conclusions sont annexées au présent rapport.

58. Le Président a en outre noté que le groupe restreint proposait un cadre concret détaillant les mesures à prendre, en particulier pour la période entre la clôture de sa sixième réunion et la vingt-troisième session de la Commission. À cet égard, le groupe restreint a fait des recommandations sur la suite à donner aux points suivants:

a) Mise à jour du document descriptif sur l'élaboration d'un cadre énumérant les éléments de base d'une stratégie nationale en matière de prévention, d'enquêtes, de poursuites et de sanctions relatives à la criminalité liée à l'identité; et présentation de ce document, pour examen à la Commission, sous forme de document de séance, à sa vingt-deuxième session;

b) Élaboration d'un document descriptif regroupant les expériences de partenariats public-privé réussies en matière de lutte contre la criminalité liée à l'identité dans différentes régions du monde; et présentation de ce document, pour examen, sous forme de document de séance, à la Commission à sa vingt-deuxième session;

c) Constitution d'un recueil d'informations sur la criminalité liée à l'identité issues du secteur privé, conformément aux conseils et orientations mentionnés plus haut (voir par. 52);

d) Élaboration d'une législation type sur la criminalité liée à l'identité, à partir de l'esquisse annexée au présent rapport. Pour ce qui est de la méthodologie à suivre, il a été considéré que l'initiative du Secrétariat de réunir, sous réserve que des fonds extrabudgétaires soient disponibles, un groupe spécial d'experts chargés de cette tâche était le moyen le plus approprié de mener à bien ce travail d'élaboration; et

e) Recueil auprès des États Membres de plus amples informations sur l'élaboration et la mise en œuvre de stratégies et de programmes nationaux de prévention et de lutte contre la criminalité liée à l'identité.

Appendice I

Esquisse de législation type sur la criminalité liée à l'identité

1. Définition

Cette section pourrait contenir des définitions des termes les plus importants. En dehors des termes "identité", "moyen d'identification", "possession", "utilisation" et "transfert", la section consacrée aux définitions pourrait également contenir des définitions de termes techniques.

2. Droit pénal matériel

La loi type pourrait contenir des dispositions de droit pénal détaillées sur la criminalité liée à l'identité en ligne et hors ligne (usurpation d'identité/fraude à l'identité). Des dispositions spécifiques ou des peines aggravantes pourraient être prévues pour des infractions spécifiques (par exemple: falsification de codes d'accès au domaine militaire). La loi type pourrait également contenir des dispositions de droit pénal incriminant des actes préparatoires tels que la production, la vente, l'importation, l'exportation ou la possession d'outils utilisés dans la contrefaçon des passeports.

3. Droit procédural

En théorie, la loi type pourrait contenir tout un ensemble de règles procédurales permettant à un pays qui ne disposerait pas d'une législation adéquate en matière de cybercriminalité de lutter efficacement contre la criminalité en ligne liée à l'identité. Néanmoins, ces règles risquent de faire double emploi avec d'autres initiatives et de donner lieu à des conflits. Il serait donc préférable qu'elles s'appliquent uniquement aux questions liées à l'identité. Les règles relatives au gel, à la saisie et à la confiscation des avoirs et/ou des informations liées à l'identité en seraient un exemple.

4. Preuve électronique

Certaines dispositions pourraient viser la recevabilité des preuves spécifiques à la criminalité liée à l'identité. L'obligation de remettre des dossiers à la victime pourrait également être prise en compte dans ces dispositions.

5. Questions urgentes

La législation type pourrait contenir des dispositions prévoyant des mesures d'urgence en cas d'infractions liées à l'identité constatées dans des affaires en cours. Les cas d'"interdiction de l'accès au rapport de solvabilité" (voir "Droit procédural" ci-avant) en seraient un exemple.

6. Obligations en matière de communication d'informations et de notification

La législation type pourrait contenir des dispositions en vertu desquelles les entreprises victimes d'infractions liées à l'identité (concernant les données de la clientèle) seraient tenues de signaler ces infractions aux services de détection et de répression. De plus, la législation type pourrait contenir des obligations de notification au titre desquelles les entreprises devraient aviser les clients que leurs données ont été obtenues illégalement. La législation type pourrait également

contenir des dispositions prévoyant la mise en place de mécanismes de communication de l'information (par exemple: des sites Web consacrés au dépôt des plaintes).

7. Protection des informations liées à l'identité

La législation type pourrait prévoir une interdiction d'utiliser certaines informations liées à l'identité, de même que des obligations de conserver ces informations en maintenant certaines normes de protection (exemple: chiffrement) et des normes techniques de suppression/destruction des informations liées à l'identité.

8. Statistiques

La loi type pourrait contenir des dispositions établissant certaines prescriptions en matière de communication d'informations afin de permettre le recueil de données statistiques par la police.

Appendice II

Liste de contrôle des éléments stratégiques à prendre en compte pour l'élaboration de stratégies nationales en matière de prévention, d'enquêtes, de poursuites et de sanctions concernant la criminalité liée à l'identité

La présente liste de contrôle rappelle brièvement les parties prenantes, les éléments fondamentaux et la procédure qu'un État peut choisir de suivre pour élaborer sa stratégie nationale en matière de prévention, d'enquêtes, de poursuites et de sanctions concernant la criminalité liée à l'identité.

A. Parties prenantes ou participants à prendre en compte dans une stratégie nationale

- Le secteur public (entités publiques chargées de l'infrastructure, des documents ou des systèmes d'identité, institutions chargées de la politique et plus généralement de la législation en la matière, organismes chargés des enquêtes, des poursuites, de la prévention de la criminalité, etc.);
- Le secteur privé (par exemple: représentants des secteurs des finances, de la vente et de l'informatique);
- Les organisations régionales et internationales.

B. Éléments fondamentaux d'une stratégie nationale

- Évaluation des menaces comprendre la nature et l'ampleur du problème ou de la situation;
- Collecte, diffusion et analyse des informations pertinentes sur le problème;
- Définition des priorités et coordination entre le secteur public et le secteur privé;
- Éléments législatifs incrimination, détection et répression, coopération internationale et mesures non pénales/administratives;
- Capacités d'enquête, de détection et de répression;
- Éléments nécessaires aux interventions rapides destinées à troubler le déroulement des infractions liées à l'identité et à leur marquer un coup d'arrêt;
- Composantes de la prévention du crime: prévention sociale (programmes de formation, sensibilisation); prévention situationnelle (diffusion d'informations auprès de groupes particulièrement exposés à des risques de victimisation spécifiques de victimisation ou en situation de détecter et de mettre fin aux infractions liées à l'identité); prévention technique (mesures de sécurité visant à garantir l'intégrité des documents et des systèmes);
- Assistance aux victimes;
- Formation des enquêteurs, des agents des services de détection et de répression et des autres employés et agents concernés, y compris dans le secteur privé;

- Coopération entre les secteurs public et privé dans la mise en œuvre de la stratégie.

C. Procédure d'élaboration et de mise à jour permanente d'une stratégie nationale

- Consacrer les ressources nécessaires à la mise en œuvre;
- Mener des consultations initiales à tous les niveaux du secteur public, ainsi qu'avec le secteur privé;
- Mettre en place des mécanismes permanents de coordination verticale (en particulier dans les États fédéraux);
- Mener des consultations et travailler en coordination avec les parties concernées à l'échelle internationale, selon qu'il convient;
- Veiller à organiser des consultations permanentes entre les parties concernées;
- Évaluer le succès et la pérennité de la mise en œuvre de la stratégie.