Organisation des
États Américains

COMITÉ INTERAMÉRICAIN CONTRE LE TERRORISME (CICTE)

SEIZIÈME SESSION ORDINAIRE
25 et 26 février 2016
Washington, D.C.

OEA/Ser.L/X.2.16
CICTE/Dec 1/16
26 février 2016
Original: espagnol

DÉCLARATION

RENFORCEMENT DE LA COOPERATION ET DU DEVELOPPEMENT EN MATIERE DE SECURITE CYBERNETIQUE ET DE LUTTE CONTRE LE TERRORISME DANS LES AMERIQUES

(Approuvée à la cinquième séance plénière, tenue le 26 février 2016)

DÉCLARATION

RENFORCEMENT DE LA COOPERATION ET DU DEVELOPPEMENT EN MATIERE DE SECURITE CYBERNETIQUE ET DE LUTTE CONTRE LE TERRORISME DANS LES AMERIQUES

(Approuvée à la cinquième séance plénière, tenue le 26 février 2016)

LES ÉTATS MEMBRES DU COMITÉ INTERAMÉRICAIN CONTRE LE TERRORISME (CICTE) de l'Organisation des États Américains (OEA), réunis à l'occasion de leur Seizième Session ordinaire, tenue à Washington, D.C. (États-Unis d'Amérique) les 25 et 26 février 2016,

1. RÉAFFIRMANT la nature, les principes et les objectifs du Comité interaméricain contre le terrorisme (CICTE) et réitérant leur plus véhémente condamnation du terrorisme sous toutes ses formes et manifestations, quelle qu'en soit l'origine et la manifestation, conformément aux principes énoncés dans la Charte de l'Organisation des États Américains et à la Convention interaméricaine contre le terrorisme, et dans le respect total de la souveraineté des États, de l'état de droit et du droit international, notamment le droit international humanitaire, le droit international relatif aux droits humains et le droit international des réfugiés;

2. RECONNAISSANT que la menace terroriste est aggravée lorsqu'il existe des liens entre le terrorisme et le trafic illicite de drogues, la cybercriminalité, le trafic illicite d'armes, le blanchiment des avoirs ainsi que d'autres formes de délinquance transnationale organisée et que ces actions illicites peuvent être utilisées pour appuyer et financer des activités terroristes;

3. RÉAFFIRMANT toutes les déclarations adoptées lors des sessions du Comité interaméricain contre le terrorisme et ayant présentes à l'esprit toutes les résolutions adoptées par l'Assemblée générale de l'OEA dans le domaine du terrorisme;

4. RÉAFFIRMANT ÉGALEMENT la résolution AG/RES. 1939 (XXXIII-O/03) « Élaboration d'une stratégie interaméricaine pour combattre les menaces à la cybersécurité » ainsi que la résolution AG/RES. 2004 (XXXIV-O/04) « Adoption d'une stratégie interaméricaine intégrée pour combattre les menaces à la cybersécurité : une approche multidimensionnelle et multidisciplinaire de la création d'une culture de cybersécurité »;

5. FAISANT SIENS le cadre international de lutte contre le terrorisme adopté par l'Organisation des Nations Unies par l'intermédiaire des résolutions de l'Assemblée générale et du Conseil de sécurité ainsi que de la Stratégie antiterroriste mondiale;

6. SOULIGNANT l'importance pour les États membres de l'OEA de signer ou ratifier la Convention interaméricaine contre le terrorisme ou d'y adhérer, selon le cas, et de l'appliquer d'une manière efficace, ainsi que les instrument juridiques universels pertinents, notamment les conventions des Nations Unies, les résolutions pertinentes du Conseil de sécurité des

Nations Unies et du Conseil des droits de l'homme des Nations Unies, et la Stratégie antiterroriste mondiale des Nations Unies adoptée par l'Assemblée générale de cette Organisation ;

7. ENGAGÉ dans le développement d'une culture de cybersécurité dans les Amériques en adoptant des mesures et des préventions efficaces pour anticiper, traiter et répondre aux attaques cybernétiques quels qu'en soient l'origine et les auteurs, en combattant les menaces et la délinquance cybernétiques, en qualifiant comme délits passibles de poursuites pénales les attaques contre le cyberespace, en protégeant les infrastructures critiques et en sécurisant les réseaux de système. Réaffirmant notre engagement à élaborer et mettre en œuvre une stratégie intégrée de l'OEA sur la sécurité cybernétique, en utilisant les contributions et les recommandations mises au point conjointement par les experts des États membres et par le Groupe d'experts gouvernementaux de la REMJA sur les délits cybernétiques, le CICTE, la Commission interaméricaine des télécommunications (CITEL) ainsi que d'autres organes appropriés, en tenant compte des travaux que mènent les États membres avec la coordination de la Commission sur la sécurité continentale;

8. RAPPELANT que les ministres responsables de la sécurité publique des Amériques, réunis dans le cadre de la MISPA V, qui s'est tenue les 19 et 20 novembre 2015 à Lima, ont émis une déclaration dans laquelle ils réaffirmaient leur appui ferme et résolu à la paix et à la lutte contre le terrorisme sous toutes ses formes et manifestations;

9. RECONNAISSANT que la lutte contre le terrorisme exige des systèmes de justice pénale qui respectent et protègent les droits humains et les libertés fondamentales afin de s'assurer que les personnes qui planifient, commettent ou appuient des actes de terrorisme sont traduites en justice, où qu'elles puissent se trouver, et soumises à une procédure judiciaire;

10. SOULIGNANT leur soutien aux victimes du terrorisme et à leurs proches, ils expriment leur solidarité à leur égard ainsi que l'importance de leur fournir l'assistance et la protection appropriée, en accord avec les normes internes de chaque État;

11. AYANT PRÉSENTES À L'ESPRIT la Déclaration « Renforcement de la sécurité cybernétique dans les Amériques », approuvée à la quatrième séance plénière de la Douzième session du CICTE, tenue le 7 mars 2012, ainsi que la Déclaration « Protection des infrastructures face aux menaces émergentes », approuvée à la cinquième séance plénière de la Quinzième session du CICTE, tenue le 20 mars 2015;

12. PRENANT NOTE AVEC SATISFACTION de l'ampleur de la tâche accomplie depuis 2004 par le Secrétariat du CICTE, le Groupe de travail de la REMJA sur la cybersécurité et la CITEL, afin de mettre en œuvre la Stratégie interaméricaine pour combattre les menaces contre la sécurité cybernétique, de même que le Plan de travail du CICTE, lequel inclut le domaine de la protection des infrastructures critiques, et au sein de celui-ci, le Programme de sécurité cybernétique;

13. RÉITÉRANT qu'il est important de continuer à mettre en application la stratégie précitée et qu'il est nécessaire de renforcer les partenariats avec tous les acteurs intervenant en matière de sécurité cybernétique;

14. RECONNAISSANT que la libre expression et la libre circulation de l'information, exercées en conformité avec les obligations et les engagements applicables aux États membres en vertu des instruments internationaux et régionaux relatifs aux droits humains sont essentiels pour l'innovation et pour le fonctionnement des réseaux informatiques sur lesquels s'appuient la croissance économique et le développement social;

15. RECONNAISSANT ÉGALEMENT que les États membres utilisent de plus en plus l'infrastructure des technologies de l'information et de la communication (TIC), les réseaux, les systèmes d'information et les technologies connexes et intégrées dans le réseau mondial de l'Internet et que cela accroît l'impact que pourraient avoir sur les États membres les menaces contre la sécurité cybernétique ainsi que l'exploitation des vulnérabilités qui y sont associées;

16. CONSIDÉRANT par conséquent que le renforcement adéquat des capacités et des cadres de sécurité cybernétique, ainsi que de l'infrastructure des TIC est fondamental pour la sécurité régionale, nationale et individuelle de même que pour le développement socio-économique;

17. CONSCIENTS que, dans le domaine des technologies de l'information et de la communication (TIC), les États ne devraient réaliser ni appuyer délibérément des activités qui sont en contradiction avec les obligations qui leur incombent en vertu du droit international, qui endommageraient intentionnellement des infrastructures critiques d'autres États;

18. RECONNAISSANT LA VALEUR du travail accompli par le Groupe d'experts gouvernementaux de l'ONU chargé d'examiner les progrès de la téléinformatique dans le contexte de la sécurité internationale et prenant acte des rapports élaborés par ce Groupe (2010, 2013, 2015);

19. PRENANT acte de la résolution A/70/125 de l'Assemblée générale des Nations Unies et du document final de la réunion de haut niveau sur l'examen général de la mise en œuvre des résultats du Sommet mondial sur la société de l'information, en particulier l'importance accordée à l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et des communications;

20. CONSCIENTS de la nécessité de continuer à renforcer le Secrétariat du CICTE dans ses fonctions d'appui aux États membres qui améliorent leurs capacités de coopération afin de prévenir, combattre et éliminer le terrorisme;

21. SOULIGNANT l'importance qu'ont les activités, les projets et les programmes mis en œuvre par le CICTE dans les différents domaines de travail établis dans ses plans de travail annuels, notamment la réalisation d'atelier, de séminaires, de réunions, d'actions de formation, de cours spécialisés et d'autres activités, aux niveaux national, sous régional et régional;

22. CONSIDÉRANT qu'il est important que les États membres coopèrent par l'inclusion et la collaboration des acteurs clés dans l'utilisation du cyberespace, notamment ceux du secteur

privé, de la société civile, du monde universitaire, de la communauté technique, qui figurent au nombre des acteurs sociaux et des organismes internationaux;

DÉCLARENT :

1. Qu'ils condamnent de la manière la plus énergique terrorisme et toute personne qui l'appuie, quelles qu'en soient les formes et manifestations parce qu'il constitue un acte criminel et injustifiable, quelles qu'en soient les circonstances, le lieu et l'auteur, et parce qu'il constitue une grave menace contre la paix et la sécurité internationales, la démocratie, la stabilité et la prospérité des pays de la région;

2. Qu'ils s'engagent de la manière la plus résolue à prévenir, combattre et éliminer le terrorisme moyennant une coopération la plus large possible, dans le respect total de la souveraineté des États et conformément aux obligations qui leur incombent en vertu de la législation nationale et du droit international, notamment le droit international relatif aux droits humains, le droit international humanitaire et le droit international des réfugiés;

3. Qu'ils exhortent les États membres qui ne l'auraient pas encore fait, à signer ou ratifier la Convention interaméricaine contre le terrorisme et les autres instruments internationaux pertinents ou d'y adhérer, selon le cas, et de mettre en œuvre de manière effective les résolutions de l'Assemblée générale et du Conseil de sécurité des Nations Unies relatives à la lutte contre le terrorisme;

4. Qu'ils renouvèlent leur engagement de mettre en application la Stratégie interaméricaine de sécurité cybernétique, adoptée par la résolution AG/RES. 2004 (XXXIV-O/04) [US: dans laquelle les États membres ont réaffirmé leur engagement à élaborer et mettre en œuvre une stratégie intégrée de l'OEA sur la sécurité cybernétique, en utilisant les contributions et les recommandations mises au point conjointement par les experts des États membres et par le Groupe d'experts gouvernementaux de la REMJA sur les délits cybernétiques, le CICTE, la Commission interaméricaine des télécommunications (CITEL) ainsi que d'autres organes appropriés, en tenant compte des travaux que mènent les États membres avec la coordination de la Commission sur la sécurité continentale;

5. Qu'il est important d'identifier l'Internet comme étant un bien public mondial destiné à promouvoir un environnement des TIC ouvert à tous, sûr et pacifique, étant entendu que l'Internet et sa sécurité sont des éléments cruciaux pour le développement de l'économie des États membres et un facteur clé pour l'amélioration de l'intégration des systèmes d'information dans notre région;

6. Qu'il est important de garantir et de réaffirmer le respect intégral des droits de l'homme dans l'utilisation du cyberespace, tels que consacrés dans divers instruments, comme la Déclaration universelle des droits de l'homme, et en particulier tels qu'ils énoncés dans la Convention américaine relative aux droits de l'homme pour les États parties, en tenant compte de leur indépendance, de leur égalité, et de leur indivisibilité, en étendant à cet effet les espaces de collaboration de la Commission interaméricaine des droits de l'homme et de ses rapporteurs afin qu'ils apportent leur aide à la réalisation de ces tâches;

7. Qu'il est nécessaire que tous les États membres continuent leurs efforts destinés à créer et/ou renforcer des groupes nationaux d'alerte, de surveillance et d'intervention en cas d'incidents cybernétiques, lesquels sont connus sous le nom d'Équipes d'intervention en cas d'incidents liés à la sécurité cybernétique (CSIRT, selon les sigles en anglais);

8. Qu'il est important que les États membres participent au Réseau sur la sécurité continentale des CSIRT et des autorités responsables de la sécurité cybernétique et qu'ils les renforcent et qu'il est également important qu'ils accroissent les échanges d'informations entre eux ainsi que la coopération pour la protection des infrastructures d'information critiques et la prévention des incidents en matière de sécurité cybernétique ainsi que pour les interventions quand ces incidents se produisent;

9. Qu'ils s'engagent à exhorter les institutions responsables de l'application de la loi à participer au Réseau et à l'actualiser;

10. Qu'il est important de mettre au point des cadres et des protocoles de coopération et d'assistance entre les États membres en cas d'incidents ayant leur origine dans un État membre différent de celui ou de ceux qui subissent ces incidents;

11. Qu'ils s'engagent à élaborer des mesures d'encouragement de la confiance de nature à renforcer la paix et la sécurité internationales et qui soient susceptibles d'accroître la coopération, la transparence, la prévisibilité et la stabilité entre les États dans l'utilisation du cyberespace, car ils reconnaissent les mesures de renforcement de la confiance et de la sécurité comme étant l'un des axes de la collaboration entre les États, qui renforcent la confiance et la coopération et réduisent le risque de conflit;

12. Qu'il est important de renforcer la sécurité et la résilience des technologies des infrastructures critiques de l'information et de la communication (TIC) face aux risques existant dans le cyberespace, en privilégiant tout particulièrement les institutions gouvernementales critiques ainsi que d'autres secteurs publics et privés cruciaux pour la sécurité nationale, y compris, entre autres, les systèmes d'administration en ligne, de santé, d'énergie, des finances, des télécommunications et des transports, moyennant la mise en application de mesures physiques et cybernétiques;

13. Qu'il est important que tous les États membres créent et/ou renforcent des unités spécialisées dans la prévention et l'investigation d'incidents de cybersécurité au sein de leurs institutions chargées de mettre la loi en application;

14. Qu'ils sont déterminés à fournir l'assistance et la formation visant à améliorer la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC) et à échanger à cet effet les pratiques techniques, juridiques et administratives les plus performantes;

15. Qu'il est nécessaire de mettre en place des procédures d'entraide afin de faire face aux incidents, d'affronter les problèmes à court terme de sécurité des réseaux, et collaborer aux demandes que les pays membres s'adresseront réciproquement pour mener une enquête sur les infractions liées aux actes terroristes et les poursuivre, notamment des procédures visant à accélérer la prestation de l'aide;

16. Qu'il est important de faciliter la coopération transfrontalière afin de faire face aux vulnérabilités des infrastructures fondamentales qui dépassent les frontières nationales;

17. Qu'ils demandent au Secrétariat du CICTE de continuer, dans la limite de ses compétences, ses activités de renforcement des capacités dans les États membres qui en font la demande pour la prévention et l'intervention face à l'utilisation des technologies de l'information et de la communication (TIC) à des fins terroristes, dans le respect des droits humains, ainsi que ses activités de sensibilisation des utilisateurs de l'Internet aux risques liés à l'utilisation du cyberespace;

18. Qu'ils sont déterminés à mettre en place et/ou à renforcer des programmes et des campagnes de sensibilisation, ciblés plus spécialement sur les groupes les plus vulnérables aux délits cybernétiques;

19. Qu'il s'avère nécessaire que le Secrétariat du CICTE, dans la limite de ses compétences, continue de renforcer les capacités des États membres qui font une demande en ce sens afin de lutter contre les incidents et/ou actes terroristes, notamment par des initiatives concernant la prévention des incidents cybernétiques, l'intervention quand ils se produisent, l'investigation et l'analyse des preuves, la coopération internationale pour l'intervention et les enquêtes en cas de tels incidents ainsi que d'autres activités permettant de renforcer les capacités des institutions responsables de mettre la loi en application et d'intervenir en cas d'incidents cybernétiques dans les Amériques;

20. Qu'il est nécessaire que le Secrétariat du CICTE, dans la limite de ses compétences, conformément à la Stratégie interaméricaine intégrée de sécurité cybernétique adoptée en 2004 (la Stratégie de 2004 et son Annexe A) continue de développer des mécanismes de coopération avec d'autres instances ou organismes internationaux, de sorte à mettre en œuvre des activités coordonnées en matière de protection et d'utilisation du cyberespace;

21. Qu'ils veulent continuer à mettre au point des stratégies nationales intégrées de sécurité cybernétique et à faire participer à leur élaboration et à leur mise en œuvre tous les acteurs et les parties pertinentes concernées notamment le secteur privé, le monde universitaire, la communauté technique, la société civile, ainsi que d'autres acteurs sociaux;

22. Qu'il est important de promouvoir la coopération entre les secteurs public, privé, universitaire, la communauté technique, la société civile, et d'autres acteurs sociaux afin de renforcer la sécurité et la protection de ces infrastructures critiques d'information et de communication;

23. Qu'il faut étudier les possibilités futures d'élargir les initiatives du CICTE visant à renforcer les capacités dans les États membres dans le but de protéger les systèmes d'infrastructures de l'information et de la communication, y compris la mise en œuvre de programmes de renforcement des capacités de nature à renforcer la sécurité et la résilience des chaînes d'approvisionnement mondiales;

24. Qu'ils encouragent les États membres à verser des contributions volontaires pour renforcer la capacité du CICTE à aider les États membres, qui en font la demande, à mettre en œuvre la Stratégie de 2004 et son Annexe A, ainsi que les déclarations adoptées et le Plan de travail;

25. Qu'ils invitent les États membres, les Observateurs permanents et les organismes internationaux pertinents à verser, maintenir ou augmenter, selon le cas, leurs contributions volontaires au CICTE, sous la forme de ressources financières ou humaines, afin de lui faciliter l'exécution de ses attributions et de promouvoir l'optimisation de ses programmes et le rayon d'action de ses activités;

26. Qu'ils sont intéressés à créer un fonds de contributions volontaires, par l'intermédiaire duquel les États membres, les Observateurs permanents et les organismes internationaux pertinents, pourront effectuer des contributions volontaires sous forme de ressources financières afin d'améliorer la sécurité cybernétique dans les Amériques et qu'ils recommandent au Secrétariat du CICTE de présenter à la Commission sur la sécurité continentale un avant-projet sur les normes de fonctionnement de ce fonds;

27. Qu'ils demandent à l'Assemblée générale de l'OEA de charger le Secrétariat général de fournir au Secrétariat du CICTE, sur les crédits alloués dans le Programme-budget, les ressources humaines et financières dont il a besoin pour mettre en œuvre le Plan de travail du CICTE, lequel comprend notamment les domaines des Contrôles frontaliers, de l'Assistance juridique et de la Lutte contre le financement du terrorisme, de la Protection des infrastructures critiques, du Renforcement des stratégies face aux menaces terroristes émergentes et de la Coordination et coopération internationales;

28. Qu'ils recommandent au Secrétariat du CICTE, dans les limites de ses compétences, de soutenir l'engagement et les initiatives des États membres qui en font la demande pour respecter et mettre en application cette Déclaration et le Plan de travail du CICTE.