Organización de los Estados Americanos

COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE)

DECIMOSEXTO PERÍODO ORDINARIO DE SESIONES
25-26 de febrero de 2016
Washington, D.C.

OEA/Ser.L/X.2.16
CICTE/Dec 1/16
26 febrero 2016
Original: español

DECLARACIÓN

FORTALECIMIENTO DE LA COOPERACIÓN Y DEL DESAROLLO EN LA SEGURIDAD CIBERNETICA Y LA LUCHA CONTRA EL TERRORISMO EN LAS AMÉRICAS

(Aprobado durante la quinta sesión plenaria, celebrada el 26 de febrero de 2016)

DECLARACIÓN

FORTALECIMIENTO DE LA COOPERACIÓN Y DEL DESAROLLO EN LA SEGURIDAD CIBERNETICA Y LA LUCHA CONTRA EL TERRORISMO EN LAS AMÉRICAS

(Aprobado durante la quinta sesión plenaria, celebrada el 26 de febrero de 2016)

LOS ESTADOS MIEMBROS DEL COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE) de la Organización de los Estados Americanos (OEA), reunidos en su Decimosexto Período ordinario de sesiones, celebrado en Washington, D. C., Estados Unidos de América, de 25 al 26 de febrero de febrero de 2016

1. REAFIRMANDO la naturaleza, principios y propósitos del Comité Interamericano contra el Terrorismo (CICTE) y reiterando su más vehemente condena del terrorismo en todas sus formas y manifestaciones, cualquiera sea su origen y manifestación de acuerdo con los principios de la Carta de la Organización de los Estados Americanos, y con la Convención Interamericana contra el Terrorismo, y con pleno respeto a la soberanía de los Estados ,al Estado de derecho y al derecho internacional, incluidos el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho internacional de los refugiados";

2. RECONOCIENDO que la amenaza del terrorismo se ve agravada cuando existen conexiones entre el terrorismo y el tráfico ilícito de drogas, el delito cibernético, el tráfico ilícito de armas, el lavado de activos y otras formas de delincuencia organizada trasnacional, y que tales ilícitos pueden ser utilizados para apoyar y financiar actividades terroristas;

3. REAFIRMANDO todas las Declaraciones adoptadas en los períodos de las sesiones del Comité Interamericano contra el Terrorismo y reconociendo todas las Resoluciones aprobadas en materia de terrorismo por la Asamblea General de la OEA;

4. REAFIRMANDO ASIMISMO la resolución AG/RES. 1939 (XXXIII-O/03) "Desarrollo de una Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética" y reafirmando la resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una Estrategia Interamericana Integral de Seguridad Cibernética: Un Enfoque Multidimensional y Multidisciplinario para la Creación de una Cultura de Seguridad Cibernética"

5. HACIENDO SUYO el marco internacional de combate al terrorismo adoptado por la Organización de las Naciones Unidas a través de las resoluciones de la Asamblea General y del Consejo de Seguridad y de la Estrategia Global contra el Terrorismo;

6. ENFATIZANDO la importancia que los Estados Miembros de la OEA firmen, ratifiquen o adhieran, según sea el caso, y apliquen de manera eficaz la Convención Interamericana contra el Terrorismo, así como los instrumentos universales pertinentes, incluyendo las Convenciones de las Naciones Unidas, las Resoluciones pertinentes del Consejo de Seguridad y del Consejo de Derechos Humanos de las Naciones Unidas y la Estrategia Global de las Naciones Unidas contra el Terrorismo, adoptada por la Asamblea General de dicha organización;

7. DESAROLLANDO una cultura de seguridad cibernética en las Américas adoptando medidas de prevención eficaces para prever, tratar y responder a los ataques cibernéticos, cualquiera sea su origen, y por quien quiera sea cometidos, luchando contra las amenazas cibernéticas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas. Reafirmando nuestro compromiso de desarrollar e implementar una estrategia integral de la OEA sobre seguridad cibernética, utilizando las contribuciones y recomendaciones elaboradas conjuntamente por los expertos de los Estados Miembros y por el Grupo de Expertos Gubernamentales de la REMJA en Materia de Delito Cibernético, el CICTE, la Comisión Interamericana de Telecomunicaciones (CITEL) y otros órganos apropiados, teniendo en cuenta el trabajo que desarrollan los Estados Miembros coordinado con la Comisión de Seguridad Hemisférica;

8. RECORDANDO que los Ministros en Materia de Seguridad Pública de las Américas reunidos en la MISPA V, realizada el 19 y 20 de noviembre de 2015 en Lima, emitieron un pronunciamiento reafirmando su decidido y firme compromiso con la paz y la lucha contra el terrorismo en todas sus formas y manifestaciones;

9. RECONOCIENDO que la lucha contra el terrorismo requiere de sistemas de justicia penal que respeten y protejan los derechos humanos y las libertades fundamentales, para asegurar que las personas que planifiquen, realicen o apoyen actos de terrorismo sean llevados ante la justicia, donde quieran que los mismos se encuentren, y sean sometidos al debido proceso;

10. SUBRAYANDO su apoyo a las víctimas de terrorismo y sus familiares, expresando su solidaridad con ellos, así como la importancia de proporcionarles la asistencia y protección adecuada de acuerdo a la normativa interna de cada Estado;

11. TENIENDO PRESENTE la Declaración "Fortalecimiento de la Seguridad Cibernética en las Américas" aprobada durante la cuarta sesión plenaria del Décimo Segundo Periodo de Sesiones del CICTE , celebrada el 7 de marzo de 2012, así como la Declaración Protección de Infraestructura Crítica ante las Amenazas Emergentes aprobada durante la quinta sesión plenaria del Décimo Quinto Periodo de Sesiones del CICTE, celebrada el 20 de marzo de 2015;

12. TOMANDO NOTA CON SATISFACCIÓN de la amplia labor realizada desde 2004 por la Secretaría del CICTE así como el grupo de trabajo sobre delito cibernético de la REMJA, y CITEL para implementar la mencionada Estrategia Interamericana para Combatir las Amenazas a la Seguridad Cibernética y así como la implementación del Plan de Trabajo del CICTE, el cual incluye el área de Protección de la Infraestructura Crítica y, dentro de ella, el Programa de Seguridad Cibernética;

13. REITERANDO la importancia de continuar implementando dicha Estrategia y la necesidad de fortalecer las alianzas entre todos los actores de la seguridad cibernética;

14. RECONOCIENDO que la libre expresión y la libre circulación de la información, ejercidas de conformidad con las obligaciones y compromisos aplicables de los Estados Miembros contenidos en el marco de los instrumentos internacionales y regionales sobre Derechos Humanos son esenciales para la innovación y el funcionamiento de las redes informáticas que sustentan el crecimiento económico y el desarrollo social;

15. RECONOCIENDO TAMBIÉN que los Estados Miembros utilizan en forma creciente la infraestructura de tecnologías de la información y comunicaciones (TIC), redes, sistemas de información y tecnologías relacionadas, e integradas en la red global de Internet, y que ello aumenta el posible impacto sobre los Estados Miembros de las amenazas a la seguridad cibernética y la explotación de vulnerabilidades relacionadas;

16. CONSIDERANDO, por tanto, que el adecuado desarrollo de capacidades y marcos de seguridad cibernética y de la infraestructura de TIC son fundamentales para la seguridad regional, nacional e individual, así como para el desarrollo socio-económico;

17. CONSCIENTES que los Estados no deberían realizar ni apoyar de forma deliberada actividades en la esfera de las tecnologías de la información y comunicaciones (TIC) contrarias a las obligaciones que le incumben en virtud del derecho internacional que dañaran intencionadamente infraestructuras criticas de otros Estados;

18. RECONOCIENDO la labor realizada por el Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de las Naciones Unidas, y tomando nota de los informes elaborados por dicho Grupo (2010, 2013, 2015);

19. TOMANDO nota de la Resolución A/70/125 de la Asamblea General de las Naciones Unidas con el documento final de la reunión de alto nivel sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad

de la Información, en especial la prioridad dada a la creación de confianza y seguridad en la utilización de las tecnologías de la información y las comunicaciones;

20. CONSCIENTES de la necesidad de continuar fortaleciendo la Secretaría del CICTE en sus funciones de apoyo a los Estados Miembros en aumentar sus capacidades de cooperación para prevenir, combatir y eliminar el terrorismo;

21. RESALTANDO la importancia que revisten las actividades, proyectos y programas desarrollados por el CICTE en las diferentes áreas de trabajo establecidas en sus planes de trabajo anuales, en particular, la realización de talleres, seminarios, reuniones, capacitaciones, cursos especializados y demás actividades, a niveles nacional, subregional y regional;

22. CONSIDERANDO la importancia de que los Estados Miembros cooperen con la inclusión y cooperación de actores claves en el uso del ciberespacio tales como el sector privado, la sociedad civil, la academia, la comunidad técnica, entre otros actores sociales y organismos internacionales;

DECLARAN:

1. Su más enérgica condena al terrorismo y a quien lo apoye, en todas sus formas y manifestaciones, por ser un acto criminal e injustificable**,** bajo cualquier circunstancia, en dondequiera y por quienquiera sea cometido y porque constituye una grave amenaza a la paz y la seguridad internacionales, a la democracia, estabilidad y prosperidad, de los países de la región;

2. Su más firme compromiso de prevenir, combatir y eliminar el terrorismo mediante la más amplia cooperación posible, con pleno respeto a la soberanía de los Estados y en cumplimiento de las obligaciones asumidas en la legislación nacional y el derecho internacional, incluidos el derecho internacional de los derechos humanos, el derecho internacional humanitario y el derecho internacional de los refugiados;

3. Su exhortación a los Estados Miembros que aún no lo hayan hecho a que firmen, ratifiquen o adhieran, según sea el caso, la Convención Interamericana contra el Terrorismo, así como los demás instrumentos jurídicos internacionales pertinentes, y que implementen de una manera efectiva las Resoluciones de la Asamblea General y del Consejo de Seguridad de las Nacionales Unidas en materia de lucha contra el terrorismo;

4. Su compromiso renovado de implementar la Estrategia Interamericana de Seguridad Cibernética, adoptada mediante la resolución AG/RES. 2004 (XXXIV-O/04) en la cual los Estados Miembros reafirmaron su compromiso de desarrollar e implementar una

estrategia integral de la OEA sobre seguridad cibernética, utilizando las contribuciones y recomendaciones elaboradas conjuntamente por los expertos de los Estados Miembros y por el Grupo de Expertos Gubernamentales de la REMJA en Materia de Delito Cibernético, el CICTE, la Comisión Interamericana de Telecomunicaciones (CITEL) y otros órganos apropiados, teniendo en cuenta el trabajo que desarrollan los Estados Miembros, coordinado con la Comisión de Seguridad Hemisférica;

5. La importancia de identificar el Internet como un recurso global disponible para el público para promover un entorno de TIC abierto, seguro, y pacifico entendiendo el Internet y su seguridad como elementos cruciales para el desarrollo de la economía de los Estados Miembros y como factor clave para mejorar la integración de sistemas de información en nuestra región;

6. La importancia de asegurar y reafirmar el respeto integral de los Derechos Humanos en el uso del ciberespacio, consagrados en diversos instrumentos tales como la Declaración Universal de Derechos Humanos, y especialmente aquellos contenidos en la Convención Interamericana de Derechos Humanos para los Estados parte, considerando su interdependencia, igualdad, e indivisibilidad incrementando para ello los espacios de colaboración con la Comisión Interamericana de Derechos Humanos y sus relatorías para asistir en estas tareas;

7. La necesidad de que todos los Estados Miembros continúen sus esfuerzos por establecer y/o fortalecer grupos nacionales de alerta, vigilancia y respuesta ante incidentes cibernéticos, conocidos como Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT);

8. La importancia que los Estados Miembros participen en y fortalezcan la Red de Seguridad Hemisférica de los CSIRT y de Autoridades en Seguridad Cibernética, así como que aumenten el intercambio de información entre los Estados Miembros y la cooperación relacionada con la protección de infraestructura de información crítica, y para la prevención y respuesta a incidentes de ciberseguridad;

9. Su compromiso de instar a las instituciones competentes de aplicación de la ley para que participen en y mantengan actualizada la Red;

10. La importancia de generar marcos y protocolos de cooperación y asistencia entre los Estados Miembros, cuando existan incidentes originados en un Estado Miembro distinto a aquel o aquellos que los sufren;

11. Su compromiso por generar medidas de fomento de la confianza que fortalezcan la paz y la seguridad internacionales y pueden incrementar la cooperación, la transparencia, la previsibilidad y la estabilidad entre los Estados en el uso del ciberespacio, reconociendo las medidas de fomento de la confianza y seguridad como uno de los ejes

de colaboración entre los Estados que aumenten confianza y cooperación y reduzcan el riesgo de conflicto ;

12. La importancia de reforzar la seguridad y la capacidad de recuperación de tecnologías de infraestructura crítica de información y comunicaciones (TIC) ante los riesgos en el ciberespacio, con especial énfasis en las instituciones gubernamentales críticas así como en otros sectores públicos y privados críticos para la seguridad nacional, incluyendo los sistemas de gobierno digital, salud, energético, financiero, de telecomunicaciones y de transporte, entre otros, mediante el uso de medidas físicas y cibernéticas;

13. La importancia de que todos los Estados Miembros establezcan y/o fortalezcan unidades especializadas en prevención, e investigación de incidentes en materia de seguridad cibernética en sus respectivas agencias de aplicación de la ley;

14. Su voluntad de proporcionar asistencia y capacitación para mejorar la seguridad en el uso de las tecnologías de la información y comunicaciones (TIC), e intercambiar las mejores prácticas técnicas, jurídicas y administrativas para tal efecto;

15. La necesidad de establecer procedimientos para la asistencia mutua a la hora de responder a los incidentes, para hacer frente a problemas a corto plazo de seguridad de las redes y prestar su colaboración a los requerimientos que los países miembros recíprocamente se efectúen con la finalidad de investigar y perseguir delitos relacionados con actos terroristas, incluidos los procedimientos para acelerar la asistencia;

16. La importancia de facilitar la cooperación transfronteriza para hacer frente a las vulnerabilidades de las infraestructuras fundamentales que trascienden las fronteras nacionales;

17. Solicitar a la Secretaría del CICTE, para que dentro de su competencia, continúe la labor de fortalecimiento de las capacidades en los Estados Miembros que lo soliciten para la prevención, y respuesta frente al uso de las tecnologías de la información y comunicaciones (TIC), con fines terroristas, respetando los derechos humanos así como su labor de concientización de los usuarios y usuarias de la Internet frente a los riesgos del uso del ciberespacio;

18. Su voluntad de establecer y/o fortalecer programas y campañas de concienciación, especialmente dirigidos hacia los grupos más vulnerables a los delitos cibernéticos;

19. La necesidad de que la Secretaría del CICTE, dentro de su competencia, continúe desarrollando las capacidades de los Estados Miembros que así lo soliciten para luchar contra incidentes e/u actos terroristas, incluyendo iniciativas de prevención, respuesta a incidentes cibernéticos, investigación y análisis de evidencia, cooperación internacional en la respuesta e investigación de los mismos, así como otras actividades

que permitan reforzar las capacidades de las instituciones de aplicación de la ley y de respuesta a incidentes cibernéticos en las Américas;

20. La necesidad de que la Secretaría del CICTE, dentro de su competencia, de conformidad con la Estrategia Interamericana Integral de Seguridad Cibernética del 2004 (la Estrategia de 2004 y su Anexo A), continúe desarrollando los mecanismos de cooperación con otros organismos a instancias internacionales, de manera de realizar acciones coordinadas en la protección y uso del ciberespacio;

21. Su voluntad de continuar desarrollando estrategias nacionales de seguridad cibernética integrales e involucrar a todos los actores y partes interesadas pertinentes en su desarrollo e implementación, incluyendo al sector privado, la academia, la comunidad técnica, y la sociedad civil, y otros actores sociales;

22. La importancia de promover la cooperación entre los sectores público, privado, académico, la comunidad técnica y la sociedad civil y otros actores sociales para fortalecer el resguardo y la protección de dicha infraestructura crítica de información y comunicaciones;

23. Explorar futuras oportunidades para ampliar los esfuerzos del CICTE en construir las capacidades de los Estados Miembros para proteger sistemas de infraestructura de la información y comunicaciones, incluyendo la implementación de programas de desarrollo de capacidades que fortalezcan la seguridad y capacidad de recuperación de las cadenas de suministro global;

24. Alentar a los Estados Miembros a proveer contribuciones voluntarias para fortalecer la capacidad del CICTE para asistir a los Estados Miembros, cuando así se lo solicite, en la implementación de la Estrategia de 2004 y su Anexo A, las declaraciones aprobadas y el Plan de Trabajo;

25. Invitar a los Estados Miembros, Observadores Permanentes y organismos internacionales pertinentes que provean, mantengan o incrementen, según corresponda, sus contribuciones voluntarias de recursos financieros o humanos al CICTE, con el objeto de facilitar el cumplimiento de sus funciones y promover la optimización de sus programas y el alcance de su labor;

26. El interés de crear un fondo de contribución voluntario, mediante el cual los Estados Miembros, Observadores Permanentes y organismos internacionales pertinentes, puedan realizar sus contribuciones voluntarias de recursos financieros con el objeto de incrementar la seguridad cibernética en las Américas, y encomendar a la Secretaría del CICTE presentar un borrador de normas de funcionamiento a la Comisión de Seguridad Hemisférica;

27. Solicitar a la Asamblea General de la OEA para que se instruya a la Secretaría General a, dentro de los recursos asignados en el programa-presupuesto de la OEA, proveer a la Secretaría del CICTE los recursos humanos y financieros necesarios para la implementación del Plan de Trabajo del CICTE, el cual incluye las áreas sobre Controles Fronterizos, Asistencia Legislativa y Combate al Financiamiento del Terrorismo, Protección de Infraestructura Crítica, Fortalecimiento de Estrategias ante Amenazas Terroristas Emergentes y Coordinación y Cooperación Internacional;

28. Encomendar a la Secretaría del CICTE**,** dentro de sus competencias para que apoye el compromiso y los esfuerzos de los Estados Miembros que así lo soliciten en el cumplimiento e implementación de esta Declaración y el Plan de Trabajo del CICTE;