**COMITÉ INTERAMERICANO CONTRA EL TERRORISMO (CICTE)**

TERCERA REUNIÓN DEL GRUPO DE TRABAJO OAS/Ser.L/X.5

SOBRE MEDIDAS DE FOMENTO DE COOPERACIÓN CICTE/GT/MFCC-23/21

Y CONFIANZA EN EL CIBERESPACIO 9 agosto 2021

27 de julio de 2021 Original: inglés

TERCERA REUNIÓN DEL GRUPO DE TRABAJO

SOBRE MEDIDAS DE FOMENTO DE COOPERACIÓN Y CONFIANZA

EN EL CIBERESPACIO

INFORME DEL RELATOR

27 de julio de 2021

Distinguidos jefes de delegación,

distinguidos delegados,

invitados especiales,

señoras y señores:

Quisiera comenzar agradeciéndoles el trabajo y el progreso realizados en nuestra primera reunión virtual del Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio del Comité Interamericano contra el Terrorismo (CICTE). La Delegación de Estados Unidos, en calidad de Relator de esta reunión, se complace en presentar este informe de las intervenciones de hoy.

La Tercera Reunión del Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio se celebró de manera virtual el 27 de julio de 2021. Contó con la participación de 16 delegaciones de Estados Miembros de la Organización de los Estados Americanos (OEA): Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, Estados Unidos, Guatemala, Guyana, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana y Trinidad y Tobago, así como invitados especiales, observadores permanentes y representantes de organizaciones internacionales.

La reunión comenzó con las palabras de apertura de **Carlos Landeros**, representante del Gobierno de Chile y Director Nacional del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) de Chile, en calidad de Presidente del Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio. El señor Landeros señaló la tendencia mundial de ciberataques cada vez más frecuentes y destructivos, que podrían afectar la economía, el sistema democrático y la sociedad de los Estados Miembros, y destacó el alcance multinacional de los riesgos cibernéticos y la necesidad de cooperación práctica en la gestión de riesgos. Presentó un resumen de las medidas de fomento de la confianza (MFC) en el ciberespacio adoptadas por el Grupo de Trabajo y observó que, en la medida en que se aplicaran, ayudarían a consolidar una red de apoyo eficaz en el Hemisferio. Agregó que la finalidad de estas reuniones era fomentar la confianza y la cooperación. Asimismo, se refirió a la importancia de promover la equidad de género en el campo cibernético y puso de relieve el trabajo realizado por el gobierno de Chile al respecto.

**Arthur Weintraub**, Secretario de Seguridad Multidimensional de la OEA, dio la bienvenida a los Estados Miembros en nombre de la Secretaría General y les agradeció su participación en la reunión de hoy. Agradeció a los gobiernos de Chile y México su extraordinario liderazgo en la presidencia y la vicepresidencia del Grupo de Trabajo en 2019 y 2020. Afirmó que las MFC eran instrumentos para contrarrestar los delitos cibernéticos y otras amenazas de ese tipo y fomentar la confianza, la transparencia y la diplomacia. Eso concuerda con la labor del Grupo de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, ambos de las Naciones Unidas. Señaló que el Grupo de Trabajo tenía la capacidad para asistir a los Estados Miembros en sus actividades multilaterales en este ámbito.

Los Estados Miembros que participaron en la videoconferencia aprobaron el proyecto de temario de la reunión, distribuido el 7 de julio de 2021 en el documento CICTE/GT/MFCC-18/21, y el proyecto de calendario, distribuido el 13 de julio de 2021 en el documento CICTE/GT/MFCC-20/21.

**Alison August Treppel**, Secretaria Ejecutiva del CICTE, habló sobre el portal de la red de contactos que la Secretaría del CICTE estaba preparando y sobre la posibilidad de que los integrantes de la red hicieran un ejercicio práctico con el portal. Este trabajo responde a la solicitud de que la Secretaría asista a los Estados Miembros en la aplicación de las tres primeras MFC del Grupo de Trabajo.

**Sofia Hunter**, Oficial del Programa de Ciberseguridad del CICTE/OEA, presentó un panorama del portal. En nombre de la Secretaría del CICTE, explicó los objetivos del portal y presentó un prototipo descriptivo para facilitar la comprensión del formato y el uso. El objetivo principal del portal es aumentar la transparencia y la accesibilidad a fin de que los Estados Miembros puedan intercambiar información, documentos normativos o jurídicos y datos sobre contactos, en consonancia con las MFC del Grupo de Trabajo.

**Kerry-Ann Barrett**,Oficial del Programa de Ciberseguridad del CICTE, invitó a los Estados Miembros a reflexionar sobre la forma en que su gobierno respondería a un incidente cibernético hipotético en la región. Describió un ciberataque hipotético contra un importante aeropuerto regional, también hipotético, e instó a los Estados Miembros a que consideraran las siguientes preguntas: ¿Cómo respondería su organismo a un incidente de este tipo? ¿Tienen planes formales para una respuesta? ¿A qué organismos deben avisar y con quiénes se comunicarían si esos organismos no estuvieran disponibles? Por último, ¿qué papel podrían desempeñar las organizaciones regionales o internacionales? La señora Barrett recalcó la utilidad de tener a mano una lista de contactos, como la que estará en el portal. La Secretaría planea llamar a los Estados Miembros cuando el portal comience a funcionar para comprobar que los datos que contiene sean correctos y pedirá a los Estados Miembros que actualicen los datos cuando los contactos cambien. La Secretaría planea también hacer ejercicios prácticos del uso del portal.

La señora Barrett se refirió al apoyo que la Secretaría del CICTE había proporcionado a los Estados Miembros en los últimos años para la aplicación de las MFC y señaló el mandato dado por los Estados Miembros a la Secretaría de asistirles en el cumplimiento de las 11 normas voluntarias no vinculantes acordadas sobre la base de un informe del Grupo de Expertos Gubernamentales de las Naciones Unidas. Agregó que 16 Estados Miembros de la OEA habían dado a conocer su política pública en materia de ciberseguridad, de acuerdo con una de las MFC del Grupo de Trabajo, y 28 habían proporcionado datos sobre contactos. Como parte de su apoyo técnico al Grupo de Trabajo, el CICTE mantiene la lista de contactos de los Estados Miembros, proporciona orientación informal e información actualizada sobre asuntos relacionados con la aplicabilidad del derecho internacional en el ciberespacio y está estableciendo un portal en la web para administrar los contactos en el ámbito de la política cibernética y ofrecer un repositorio de políticas y leyes regionales en materia de ciberseguridad. La Secretaría planea inaugurar el portal el 1 de octubre de 2021. Asimismo, la Secretaría ha organizado cursos para funcionarios de ministerios de gobierno sobre la aplicabilidad del derecho internacional en el ciberespacio.

A continuación, se ofreció la palabra a los Estados Miembros para que hicieran breves intervenciones sobre la aplicación de las MFC. Intervinieron siete países:

* **Estados Unidos:** La Delegada de Estados Unidos destacó el apoyo de su país a la labor de la OEA y el CICTE en este ámbito y, en particular, al Grupo de Trabajo, y afirmó que Estados Unidos se complacía en seguir proporcionando apoyo financiero para el Grupo de Trabajo, la Secretaría y la creación del portal. Señaló que el gobierno de Biden seguía dando prioridad a la ciberseguridad como imperativo de política y había emitido una nueva orden del Poder Ejecutivo sobre asuntos cibernéticos, documento que Estados Unidos aportaría al Repositorio de Políticas de la OEA. El Departamento de Estado ha ofrecido un curso interno para ciberdiplomáticos de Estados Unidos asignados a la región, con el propósito de fortalecer la red de expertos en la materia preparados para trabajar en estos temas en toda la región y en el resto del mundo. Estados Unidos se comprometió a seguir colaborando con asociados regionales y Estados Miembros de la OEA en temas clave de la ciberdiplomacia en 2022.
* **Chile:** El Delegado de Chile observó que su país se había centrado en la construcción de una estructura para reforzar la respuesta a incidentes cibernéticos por medio de medidas tales como la ampliación de la cooperación a escala internacional con la elaboración de una lista de contactos de confianza y el intercambio de información. Uno de los mecanismos para el intercambio de información es la red CSIRT Américas, que opera bajo la égida del CICTE. Asimismo, el Delegado de Chile explicó el trabajo de su país en el ámbito de la legislación interna sobre ciberseguridad, proceso que lleva mucho tiempo. Una de las tareas legislativas en curso está relacionada con el Convenio de Budapest sobre la Ciberdelincuencia. Otra se refiere a la protección de la infraestructura crítica, área que requiere cooperación entre los sectores público y privado. El Delegado de Chile destacó la importancia de proveer asistencia sobre temas conexos a otros Estados Miembros.
* **México:** El Delegado de México agradeció a Chile y a la Secretaría la convocatoria de la reunión a pesar de las dificultades planteadas por la respuesta mundial a la COVID-19 y recalcó la importancia de celebrar reuniones de este tipo, justamente debido a las circunstancias en que se da esa respuesta. Señaló que México había puesto de relieve cinco elementos en la aplicación de las MFC regionales:
	+ Primero, México ha reafirmado la aplicabilidad del derecho internacional en el ciberespacio, incluso con su participación en este Grupo de Trabajo.
	+ Segundo, al participar en actividades recientes de las Naciones Unidas, México ha contribuido a la acción encaminada a construir y consolidar el marco para el comportamiento responsable de los Estados en el ciberespacio. México está muy entusiasmado al ver que el trabajo de este grupo, que fomenta la confianza en el ciberespacio, también secundará esta labor.
	+ Tercero, es necesario mantener un equilibrio entre la protección y la seguridad en el ciberespacio y la promoción de las innovaciones tecnológicas y los derechos humanos en línea.
	+ El cuarto elemento es el fomento de la participación de otros interesados no gubernamentales.
	+ El quinto elemento consiste en colaborar con organizaciones multilaterales si se produce un incidente.
	+ Sobre la base de estos cinco principios, México ha formado un grupo interinstitucional con el cometido de tomar decisiones sobre la respuesta a incidentes e impulsar la política cibernética. Asimismo, ha promovido los equipos comunitarios de respuesta a emergencias (CERT) y ha trabajado en la formulación de una política integral de ciberseguridad en el ámbito federal y de los estados. México instituyó una semana nacional de la ciberseguridad para fomentar la conciencia al respecto.
	+ El Delegado de México preguntó de qué forma se podía evitar la duplicación de tareas de la iniciativa del portal, el portal de política cibernética del Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) y el nuevo portal de CSIRT Américas. La Secretaría del CICTE dijo que respondería al final de la sesión.
* **Argentina:** El Delegado de Argentina señaló que el fomento de la confianza contribuía a la seguridad internacional y a la estabilidad en el ciberespacio. Destacó la fructífera labor del Grupo de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta, de las Naciones Unidas, que concluyó este año con informes de consenso que apoyan el marco para el comportamiento responsable de los Estados. Argentina, junto con otros Estados de la región, promueve el establecimiento de programas de acción conjunta en el Grupo de Trabajo de Composición Abierta. El Delegado de Argentina recalcó la importancia del intercambio de información para la estabilidad del ciberespacio, así como la utilidad de las organizaciones regionales. Afirmó que su país apoyaba las seis MFC y las había aplicado. En Argentina se ha creado la Dirección Nacional de Ciberseguridad, que contribuye a la formulación de la Estrategia Nacional de Ciberseguridad, actualmente en revisión. Asimismo, se está elaborando un programa de protección de la infraestructura crítica. Argentina da prioridad a la perspectiva de género en el ámbito de la ciberseguridad y se propone fomentar una mayor participación de la mujer en el sector. En Argentina hay un CSIRT nacional encargado de la coordinación y la gestión de incidentes a nivel nacional, que forma parte de CSIRT Américas. Por último, se organizan programas y cursos de aumento de la capacidad para los diplomáticos y los responsables de las políticas del país. Argentina cree que el portal y los ejercicios prácticos serán importantes. El Delegado de Argentina observó que la amenaza de la ciberdelincuencia era un campo prioritario para la cooperación entre Estados Miembros y que su país era signatario del Convenio de Budapest sobre la Ciberdelincuencia.

* **Colombia:** La Delegada de Colombia dijo que su país participaba en el Grupo de Trabajo de Composición Abierta, lo cual Colombia consideraba como su propia medida de fomento de la confianza. Mencionó dos hitos con respecto a la aplicación de las MFC en el ciberespacio. Primero, Colombia ratificó el Convenio de Budapest sobre la Ciberdelincuencia y está trabajando en su implementación. Segundo, se estableció en el país una nueva política, CONPES 3995, la tercera política pública de ciberseguridad, que facilita la determinación de las prioridades nacionales. Colombia está considerando la capacitación en todos los niveles y recibiría con beneplácito directrices de la OEA con respecto a la aplicabilidad del derecho internacional para asistir a los Estados Miembros en su implementación.
* **República Dominicana:** El Delegado de la República Dominicana dijo que el país contaba con una estrategia de ciberseguridad desde 2018 y promovía la interacción entre diversos sectores a fin de fomentar la confianza. El Consejo Nacional de Ciberseguridad está integrado por instituciones que trabajan en los ámbitos de la transformación de políticas públicas, las telecomunicaciones, el ministerio público y la justicia. La República Dominicana está trabajando en la actualización de su ley de 2007 sobre la ciberdelincuencia, y recientemente se terminó de redactar un proyecto de ley cuyo proceso legislativo podría concluir este año. El gobierno también trabajó con el sector privado en la redacción de una ley que abarca todo el ecosistema digital del país, prestando especial atención a la infraestructura crítica. Asimismo, se está avanzando con una ley para proteger los datos. La República Dominicana tiene un plan de trabajo para formular normas orientadas a cada sector de la infraestructura crítica y planea hacer un análisis de riesgos en 2022 a fin de elaborar un catálogo oficial de la infraestructura crítica nacional. En un análisis realizado anteriormente en el país se determinó que varios incidentes cibernéticos estaban relacionados, lo cual suscitó preocupación. Para fortalecer la capacidad operacional con el fin de responder a incidentes, sin limitarse al CSIRT nacional, se están estableciendo CSIRT sectoriales. El CSIRT del sector financiero está bien afianzado; se está gestando un CSIRT para el sector de la defensa, y el año próximo posiblemente le siga uno en el sector de la energía. La República Dominicana tiene una agenda digital para el próximo decenio relacionada con la legislación y la transformación digital, en la cual la ciberseguridad es un tema transversal. Se formulará una estrategia de ciberseguridad actualizada en un plazo de tres años, aproximadamente. El CIRST nacional, el CSIRT del sector financiero y otros CSIRT del país forman parte de CSIRT Américas. El país ha sido seleccionado por el proyecto CyberNet de la Unión Europea para ser sede de un centro regional con la misión de reforzar la ciberseguridad y combatir la ciberdelincuencia. La República Dominicana planea contar con establecimientos de capacitación especializada abiertos a todos los países de América Latina y el Caribe.
* **Ecuador:** El Delegado de Ecuador señaló que, tras el reciente cambio de gobierno, el país estaba trabajando para mantener la ciberseguridad como tema central. Una de las medidas tomadas para aplicar las MFC en el ciberespacio es la creación del Comité Nacional de Ciberseguridad. Asimismo, se aprobó una nueva ley de protección de datos y se están tomando medidas para aplicar el Convenio de Budapest y mejorar las actividades encaminadas a aumentar la capacidad nacional.
* Para concluir las deliberaciones, la Secretaría del CICTE respondió a las preguntas formuladas por el Delegado de México. La Secretaría del CICTE, en calidad de Secretaría Técnica, hace un gran esfuerzo para evitar la duplicación de tareas y coordinar su labor con otras entidades. El UNIDIR y la Organización para la Seguridad y Cooperación en Europa (OSCE) tienen portales, y la Secretaría todavía no ha planeado actividades conjuntas. Su objetivo central es servir a los Estados Miembros y está dispuesta a considerar iniciativas conjuntas más adelante. La Secretaría del CICTE administra el portal técnico y el portal sobre políticas que se están creando, lo cual le permitirá tomar medidas prácticas para facilitar la cooperación y la colaboración entre ambos grupos.

El segmento siguiente consistió en una conversación abierta entre Estados Miembros sobre las enseñanzas y las dificultades de la aplicación de las MFC en el ciberespacio adoptadas por el Grupo de Trabajo. Al respecto, intervinieron dos países:

* **Estados Unidos:** La Delegada de Estados Unidos reflexionó sobre las dificultades de la formulación y la aplicación de una política cibernética. Para facilitar la coordinación entre diversos organismos de la administración pública, es útil contar con mecanismos formales e informales de coordinación cibernética antes que se produzcan incidentes. Asimismo, es importante que se indiquen de antemano en las políticas los puntos fuertes, las facultades o los mandatos de un organismo dado. También es importante que la política y las leyes en materia cibernética sean lo más neutrales posible desde el punto de vista tecnológico, a fin de que no pierdan relevancia con el tiempo como consecuencia de los avances tecnológicos. Otra dificultad es la escasez de recursos y la necesidad de buscar un equilibrio entre las necesidades a corto y a largo plazo. El Departamento de Estado designa un encargado de asuntos cibernéticos en cada embajada en el exterior, con la capacitación necesaria en este campo y preparado para manejar interacciones ciberdiplomáticas.
* **Colombia:** Dos delegados de Colombia intervinieron y propusieron que la OEA convocara una reunión ministerial para abordar el tema de la ciberdiplomacia, aumentar la conciencia y la colaboración en materia de ciberseguridad y armonizar las actividades para aplicar las MFC. En cada embajada, Colombia tiene agregados de defensa que sirven de enlace con diversas instituciones.

La Secretaria Alison Treppel reiteró la disposición de la Secretaría del CICTE para apoyar la aplicación de las MFC y agradeció a los diversos donantes.

Ningún Estado Miembro propuso nuevas MFC en el ciberespacio. La Secretaría invitó a los Estados Miembros a que presentaran propuestas por escrito más adelante.

La parte siguiente de la reunión consistió en las tres alocuciones que se resumen a continuación.

**Duncan Hollis**, profesor de Derecho de la cátedra Laura H. Carnell de la Facultad de Derecho de la Universidad Temple, afirmó en su alocución que los Estados estaban de acuerdo en que el derecho internacional se aplicaba a sus operaciones cibernéticas, pero todavía era poco lo que se sabía acerca de la manera específica en que se aplicaba, principalmente porque la mayoría de los Estados guardaban silencio sobre el tema. Presentó una conceptualización de las expresiones “uso de la fuerza”, “responsabilidad del Estado” y “ataque” en el marco del derecho internacional humanitario y concluyó señalando las dificultades de promover la transparencia en la aplicación del derecho internacional humanitario en el ciberespacio y posibles actividades futuras.

**Dan McBryde**, Asesor Principal de Política del Ministerio de Asuntos Mundiales de Canadá, resumió la evolución y el progreso del Grupo de Expertos Gubernamentales y el Grupo de Trabajo de Composición Abierta desde 2015. Describió las diferencias entre ambos mecanismos, posibles actividades futuras y las 11 normas del comportamiento responsable de los Estados en el ciberespacio, adoptadas por el Grupo de Expertos Gubernamentales en 2015, que constituyen la base de todas las actividades en este ámbito. En opinión de Canadá, no es necesario adoptar normas nuevas, sino concentrarse en la aplicación de las normas existentes. El señor McBryde dijo que Canadá emitiría una declaración para fines de 2022 sobre la forma de aplicar el derecho internacional en el ciberespacio.

**Isaac Morales**, Coordinador de Seguridad Multidimensional en la Secretaría de Relaciones Exteriores de México, habló sobre la propuesta de México y otros países de realizar una encuesta nacional sobre la aplicación de la resolución 70/237 de la Asamblea General de las Naciones Unidas. Esta iniciativa voluntaria facilitaría la aplicación de políticas, la detección de dificultades y la coordinación de la asistencia técnica para distintos países. El señor Morales dijo que México podría responder a cualquier pregunta sobre la encuesta e invitó a todos los Estados Miembros a participar en la iniciativa. El señor Morales recalcó la importancia de las consultas multilaterales y las organizaciones regionales para la seguridad en el ciberespacio.

La Secretaria Alison Treppel agradeció a los tres oradores y confirmó que el material presentado durante las alocuciones se enviaría a los Estados Miembros. Concluyó la parte de la reunión moderada por la Secretaría del CICTE y cedió la palabra nuevamente a Chile.

A continuación, los Estados Miembros abordaron el lugar y la fecha de la Cuarta Reunión del Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio. Los delegados señalaron lo siguiente:

* Chile propuso celebrar la reunión siguiente durante el primer semestre de 2022, de forma presencial, en Chile, si las condiciones lo permiten.
* Estados Unidos secundó la propuesta de Chile de celebrar una reunión presencial en 2022 si las condiciones lo permiten.
* Colombia aceptó la propuesta de Chile y propuso un formato híbrido que permita la participación virtual o presencial.
* México recalcó la importancia de la flexibilidad con respecto al formato de las reuniones futuras.
* Costa Rica apoyó la necesidad de flexibilidad con las fechas y la modalidad de la próxima reunión.

La Cancillería de Chile presentó un proyecto de texto para incluir en la resolución ómnibus y ofreció la palabra a los Estados Miembros que quisieran intervenir.

* Colombia propuso eliminar el tercer párrafo y destacó la importancia de celebrar la próxima reunión de una manera flexible e híbrida.
* México puso de relieve la necesidad de escribir siglas tales como “GGE” en inglés o de escribir el nombre completo para evitar confusiones.
* Estados Unidos propuso dividir el cuarto párrafo en dos partes para destacar la idea de que el Grupo de Trabajo estaba de acuerdo en reunirse otra vez.
* Colombia expresó preocupación por el uso de la palabra “articuladas” y propuso reemplazarla con “contenidas”.
* México se refirió a la propuesta de Estados Unidos y argumentó que dividir el cuarto párrafo en dos partes implicaría repetir una sección ya mencionada en otro párrafo. En vista de la importancia de tener un número reducido de párrafos, México propuso mantener la propuesta de Chile con la adición de las modificaciones solicitadas por Estados Unidos.
* Estados Unidos aceptó mantener los cuatro párrafos y propuso continuar las conversaciones en la reunión del CICTE.

En el punto siguiente, elección de autoridades, se ofreció la palabra para la presentación de candidaturas.

Canadá y Argentina propusieron a México para que ocupara la presidencia. El señor Landeros les agradeció la presentación de la candidatura y felicitó a la Delegación de México por su elección por aclamación. Agradeció a México que aceptara esta importante misión y que se ofreciera a encabezar las actividades regionales para mejorar la cooperación, la transparencia, la previsibilidad y la estabilidad y reducir los riesgos de interpretación errónea, escalada y conflicto que pudieran surgir del uso de las TIC.

México agradeció a todas las delegaciones la elección para presidir el Grupo de Trabajo y subrayó que continuaría trabajando sobre las bases sentadas por Chile y fomentaría la cooperación en el Grupo de Trabajo.

Chile propuso a Estados Unidos para que ocupara la vicepresidencia. El señor Landeros aprovechó la oportunidad para felicitar a la Delegación de Estados Unidos por su elección por aclamación.

El señor Landeros cedió la palabra a Estados Unidos para que presentara el informe del Relator y lo sometiera a la aprobación del Grupo de Trabajo. Estados Unidos presentó una reseña de las intervenciones realizadas durante la reunión y dijo que se distribuiría un informe formal en breve.

Como nadie más pidió la palabra, el señor Landeros agradeció los comentarios de las delegaciones y clausuró la Tercera Reunión del Grupo de Trabajo sobre Medidas de Fomento de Cooperación y Confianza en el Ciberespacio.

CICTE01414S04