Actualización de la ONU: avances relacionados con la cibernética

Informe sobre debates relacionados con la cibernética en las Naciones Unidas

Veni Markovski
Alexey Trepykhalin
3 de junio de 2021
GE-009

ÍNDICE

Introducción

Este documento brinda una actualización sobre los debates dentro de los diferentes grupos de la Asamblea General de las Naciones Unidas (AGNU) en los que se discuten cuestiones relativas a la ciberseguridad. Incluye actualizaciones sobre las deliberaciones que tuvieron lugar en el primer Grupo de Trabajo de Composición Abierta (OEWG), el Grupo de Expertos Gubernamentales (GGE) y el Comité Especial de Expertos de Composición Abierta (AHC[1]) entre el 1 de julio de 2020 y el 3 de junio de 2021.

Este documento es parte de una serie periódica de informes que brindan una reseña general de las actividades que se llevan a cabo en la ONU y que son pertinentes al ecosistema de Internet y la misión de la ICANN.[2] El monitoreo de dichas actividades demuestra el compromiso y la responsabilidad del equipo de Participación Gubernamental y de las Organizaciones Intergubernamentales (GE) de la organización de la ICANN de mantener informada a la comunidad de la ICANN en general sobre cuestiones de importancia para la Internet global, única e interoperable y su sistema de identificadores únicos.[3]

Actualización sobre el Grupo de Trabajo de Composición Abierta (OEWG)

Desde la publicación que realizó la organización de la ICANN sobre los debates relacionados con la cibernética en la ONU en julio de 2020, el OEWG tuvo tres rondas más de consultas informales ese año (del 29 de septiembre al 1 de octubre, del 17 al 19 de noviembre, y del 1 al 3 de diciembre). Durante estas consultas, la Secretaría del OEWG recibió diversos comentarios y aportes de los Estados miembros como parte del proceso formal y de organizaciones no gubernamentales como parte de las consultas informales que inició la Presidencia del OEWG.

A continuación, el equipo de GE de la organización de la ICANN resume solo los aportes al OEWG que se relacionan con la misión de la ICANN. La siguiente es una lista de dichos aportes ordenados por fecha.

---

[1] En las dos actualizaciones anteriores, utilizamos la abreviatura OECE; sin embargo, en la sesión inaugural del Comité, nos dimos cuenta de que los Estados miembros de la ONU utilizan otra abreviatura, AHC, para Comité Especial. Por ende, para que haya uniformidad, la organización de la ICANN adaptó el texto en consecuencia. El nombre completo de este comité es “Comité Especial Encargado de Elaborar una Convención Internacional Integral sobre la Lucha Contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos”.

[2] Consulte los informes anteriores del equipo de GE aquí: https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en Esta y todas las demás direcciones URL incluidas en las notas al pie y en los apéndices se obtuvieron el 3 de junio de 2021.

[3] “Plan Operativo y Financiero de la ICANN”, pág. 47, organización de la ICANN, diciembre de 2020, https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf

2 de julio de 2020, República de Finlandia: “También queremos extender nuestro firme apoyo a la propuesta realizada por los Países Bajos sobre la protección de la integridad y la disponibilidad del núcleo público de Internet y sus sugerencias concretas respecto del alcance de las normas sobre infraestructura crítica (13f y 13g)”.[4]

19 de noviembre de 2020, República Islámica de Irán: “Estas sanciones digitales [unilaterales] han afectado la inversión en infraestructuras de TIC, así como el acceso a tecnologías digitales, recursos digitales como los IP y el sistema del DNS y las redes, y no solo constituyen barreras para lograr los objetivos nacionales de desarrollo relacionados con las TIC, sino que también violan los derechos humanos”.[5]

19 de enero de 2021, Reino de los Países Bajos: “‘Los agentes estatales y no estatales no deberían realizar ni permitir deliberadamente actividades que perjudiquen de forma intencional y sustancial la disponibilidad general o la integridad del núcleo público de Internet y, por consiguiente, la estabilidad del ciberespacio’ [sería] una orientación para la implementación de la recomendación 13(f) del GGE de la ONU de 2015 y, por lo tanto, se incluiría también dentro del ámbito de aplicación de la recomendación 13(g) del GGE de la ONU de 2015”.[6]

19 de febrero de 2021, República de Eslovenia: “También queremos respaldar los pedidos realizados por los Países Bajos para poner mayor énfasis en la protección del núcleo público de Internet”.[7]

19 de febrero de 2021, República Federal de Alemania: “Sugerencia de incluir una referencia a las amenazas al núcleo público de Internet, como también se mencionó en el párrafo 50 del Borrador Preliminar, en la sección sobre amenazas existentes y potenciales”.[8]

Del 19 al 22 de febrero de 2021, Reino de los Países Bajos: “Con el transcurso de los años, las operaciones cibernéticas en contra de la integridad, el funcionamiento y la

---

[4] “Declaraciones de la República de Finlandia”, 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, consultas informales virtuales, 19 de junio y 2 de julio de 2020, https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-finland-19-june-and-2-july-2020.pdf

[5] “‘Documento previo al borrador preliminar’ revisado del informe del OEWG, tercera reunión oficiosa virtual del OEWG, intervención de la delegación de la República Islámica de Irán, 19 de noviembre de 2020, “Creación de capacidades”, https://front.un-arm.org/wp-content/uploads/2020/11/iran-intervention-on-capacity-building-19-nov-2020.pdf

[6] “Documento oficioso que incluye propuestas de texto específicas en relación con el tema de la agenda ‘Reglas, normas y principios’ a partir de presentaciones escritas de las delegaciones”, versión al 18 de enero de 2021, https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Non-paper-rules-norms-and-principles-19-01-2021.pdf

[7] 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, reunión virtual oficiosa (18, 19 y 22 de febrero de 2021), Eslovenia, declaración, 19 de febrero de 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Slovenia-19-February-2021-FINAL.pdf

[8] Comentarios de Alemania sobre el Borrador Preliminar del OEWG, 19 de febrero de 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Germany-Written-Contribution-OEWG-Zero-Draft-Report_clean.pdf

disponibilidad de Internet han demostrado ser una amenaza real y verosímil. Esto se mencionó como 'núcleo público' en el documento previo al borrador preliminar del OEWG. Dado que buscamos lograr el consenso, nos contactamos con los países que habían manifestado inquietudes durante nuestros debates anteriores y formulamos una nueva redacción que parece responder a esas inquietudes. El nuevo texto dice lo siguiente: 'la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet'".[9]

23 de febrero de 2021, Reino Unido: "Expresamos nuestro agradecimiento a los Países Bajos por trabajar con nosotros y con otros con el fin de perfeccionar la propuesta sobre el 'núcleo público' y recibimos con agrado la inclusión del texto en cuestión".[10]

25 de febrero de 2021, Reino de los Países Bajos: "En consonancia con el texto sobre la protección del núcleo público que se incluyó en el documento previo al borrador preliminar, teniendo en cuenta la convergencia en la redacción exacta, proponemos lo siguiente. Nos gustaría proponer cambiar la formulación de la última oración del párrafo 21 sobre 'integridad, funcionamiento y disponibilidad' por la [necesidad de proteger] 'la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet'".

"Además, desearíamos mencionar la importancia de la 'protección de la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet' en la parte de conclusiones y recomendaciones de la sección sobre reglas, normas y principios".[11]

3 de marzo de 2021, Comisión Global sobre la Estabilidad del Ciberespacio (GCSC): "Si bien la Comisión se sintió muy complacida de notar que en el informe anterior sobre el documento previo al borrador preliminar se consideraron varias de las recomendaciones de la GCSC, lamentamos que muchas de estas recomendaciones no se hayan incluido en el borrador preliminar o en el primer borrador actual. Esto se aplica particularmente a la norma para proteger el núcleo público de Internet, que creemos que ha sido bien recibida por muchos Estados, así como por la sociedad civil y los observadores del sector privado".[12]

8 de marzo de 2021, República Islámica de Irán: "Las plataformas y corporaciones transnacionales como la ICANN deberían tener que rendir cuentas".[13]

---

[9] Declaración de su excelencia Nathalie Jaarsma, Reino de los Países Bajos, ante las Naciones Unidas (18,19 y 22 de febrero de 2021), https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-informals-intervention-Feb-2021.pdf

[10] Comentarios del Reino Unido respecto del Borrador Preliminar del Informe del OEWG sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, 23 de febrero de 2021, https://front.un-arm.org/wp-content/uploads/2021/02/UK-submission-to-OEWG-ICTs-zero-draft-002.pdf

[11] Países Bajos: propuestas presentadas por escrito al Borrador Preliminar del OEWG, febrero de 2021, https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-written-comments-to-zero-draft.pdf

[12] Comentarios de la GCSC sobre el Primer Borrador del Informe Sustantivo del Grupo de Trabajo de Composición Abierta, 3 de marzo de 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Submission-to-OEWG-First-Draft-Report-March-2021.pdf

[13] Primera reunión: 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, tercer período de sesiones sustantivo (del 8 al 12 de marzo de 2021), TV web de la ONU, 8 de marzo de 2021 (comienza en 1:29:40) https://media.un.org/en/asset/k1o/k1obxycc3u

8 de marzo de 2021, Cybersecurity Tech Accord: “El reciente hackeo a SolarWinds ha puesto de manifiesto que ninguna organización debería sentirse inmune frente a un adversario decidido y con suficientes recursos. Asimismo, demostró hasta qué punto los agentes maliciosos descaradamente avanzados están dispuestos a socavar la confianza en los procesos esenciales y el núcleo público de Internet al llevar a cabo un ataque”.[14]

El 9 de marzo de 2021, la República Federal de Alemania respaldó el nuevo texto de compromiso: “... en particular, sobre el núcleo público de Internet”.[15]

El 9 de marzo de 2021, una coalición de nueve organizaciones de la sociedad civil recomendó que el informe del OEWG “... haga referencia a la necesidad de que todos los agentes protejan la disponibilidad básica y la integridad de la Internet global, lo que incluye no interferir con el núcleo público de Internet”.[16]

10 de marzo de 2021, República Popular China: “Los Estados deberían participar en la administración y la distribución de los recursos internacionales de Internet en igualdad de condiciones”.[17]

El 12 de marzo de 2021, la GCSC manifestó su “pesar por el hecho de que el término ‘núcleo público’ no estaba reflejado en el borrador final del informe del OEWG”.[18]

Además de la publicación del informe final del OEWG, el presidente del OEWG publicó un resumen de la Presidencia, que incluía el texto anterior sobre el núcleo público propuesto por los Países Bajos el 19 de enero.[19]

---

[14] Respuesta de Cybersecurity Tech Accord al Informe Sustantivo del OEWG de la ONU [PRIMER BORRADOR], https://front.un-arm.org/wp-content/uploads/2021/03/Tech-Accord-OEWG-response-March-2021-FINAL.pdf

[15] Tercera reunión: 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, tercer período de sesiones sustantivo (del 8 al 12 de marzo de 2021), TV web de la ONU, 9 de marzo de 2021 (comienza en 38:20) https://media.un.org/en/asset/k13/k13uzdidth

[16] “Aporte conjunto de la sociedad civil acerca del Primer Borrador del Informe del OEWG sobre las TIC”, depositario de documentos del OEWG, 9 de marzo de 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Joint-CS-feedback-on-first-draft-1.pdf

[17] 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, tercer período de sesiones sustantivo, del 8 al 12 de marzo de 2021, resumen de la Presidencia del OEWG, documento de la sala de conferencias, 10 de marzo de 2021, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

[18] Declaración de la GCSC sobre el borrador final del informe sustantivo del Grupo de Trabajo de Composición Abierta de la ONU, 12 de marzo de 2021, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Statement-OEWG-Multistakeholder-Consultation-Final-Draft-Report-March-2021.pdf

[19] 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, tercer período de sesiones sustantivo, del 8 al 12 de marzo de 2021, resumen de la Presidencia, documento de la sala de conferencias, 10 de marzo de 2021, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

Con la nueva redacción acordada entre los Estados miembros, en los puntos 18 y 26, el texto de compromiso del informe final del OEWG de 2021 dice lo siguiente:

"18. Los Estados concluyeron que las actividades maliciosas de las TIC pueden tener consecuencias económicas, sociales, humanitarias y relacionadas con la seguridad potencialmente devastadoras para la infraestructura crítica (CI) y la infraestructura crítica de información (CII) en las que se sustentan servicios esenciales para el público. Si bien es prerrogativa de cada Estado determinar qué infraestructura designa como crítica, dicha infraestructura puede incluir instalaciones médicas, servicios financieros, energía, agua, transporte y saneamiento. También son motivo de preocupación real, y cada vez mayor, las actividades maliciosas de las TIC contra la CI y la CII que menoscaban la confianza en los procesos políticos y electorales y las instituciones públicas o que afectan la disponibilidad general o la integridad de Internet. Es posible que dicha infraestructura sea propiedad del sector privado, o que este la gestione o la maneje, o puede que se comparta o se transmita en red con otro Estado o esté gestionada por distintos Estados. Por ello, puede ser necesaria la cooperación entre Estados o entre los sectores público y privado para proteger su integridad, funcionamiento y disponibilidad".[20]

"26. Si bien coincidieron en la necesidad de proteger toda la infraestructura crítica (CI) y la infraestructura crítica de información (CII) que sustentan los servicios esenciales para el público, además de esforzarse por garantizar la disponibilidad general y la integridad de Internet, los Estados también concluyeron que la pandemia de COVID-19 ha acentuado la importancia de proteger la infraestructura de salud, incluso las instalaciones y los servicios médicos, mediante la implementación de normas que aborden la infraestructura crítica, tales como aquellas afirmadas por consenso mediante la resolución 70/237 de la Asamblea General de la ONU".[21]

La delegación de los Países Bajos, en sus comentarios sobre el informe por consenso del OEWG, señaló que "los Países Bajos reciben con agrado la inclusión de la disponibilidad general y la integridad de Internet, aquello que consideramos como el núcleo público de Internet".[22]

Actualización sobre el Grupo de Expertos Gubernamentales (GGE)

[20] 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, Informe Sustantivo Final, documento de la sala de conferencias, 10 de marzo de 2021, A/AC.290/2021/CRP.2, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
[21] 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, Informe Sustantivo Final, documento de la sala de conferencias, 10 de marzo de 2021, A/AC.290/2021/CRP.2.
[22] Novena reunión: 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, tercer período de sesiones sustantivo (del 8 al 12 de marzo de 2021), TV web de la ONU, 12 de marzo de 2021, (comienza en 35:23), https://media.un.org/en/asset/k1r/k1rf2exuhz

El 28 de mayo de 2021, se adoptó el informe por consenso del GGE.[23] Varios puntos del informe son relevantes para la comunidad de la ICANN, dentro del contexto global de las deliberaciones relacionadas con la cibernética en la ONU que hemos observado en los últimos años. Los puntos citados que se enumeran a continuación (en algunos casos citados en forma parcial) se extraen de la *Copia Anticipada del Informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional* y la "Carta de Transmisión" del informe.[24]

Punto 10: "La actividad perjudicial de las TIC contra la infraestructura crítica que proporciona servicios a nivel nacional, regional o mundial, que fue debatida en informes anteriores del GGE, se ha vuelto un problema cada vez más grave. Genera especial preocupación la actividad maliciosa de las TIC que afecta la infraestructura crítica de información, la infraestructura que proporciona servicios esenciales al público, la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet y las entidades del sector de la salud".

Punto17: "El Grupo también tomó nota de la propuesta de China, Kazajistán, Kirguistán, la Federación Rusa, Tayikistán y Uzbekistán respecto de un código de conducta internacional para la seguridad de la información (véase A/69/723)".[25]

Punto 44: "Como se señala en la norma 13(g), los Estados deberían tomar medidas adecuadas para proteger su infraestructura crítica. A este respecto, cada Estado determina qué infraestructuras o sectores considera críticos dentro de su jurisdicción, de conformidad con las prioridades nacionales y los métodos de categorización de la infraestructura crítica".

Punto 45: "La infraestructura crítica también puede hacer referencia a aquellas infraestructuras que suministran servicios en varios Estados, como la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet".

Punto 48: "La designación de una infraestructura o sector como infraestructura crítica por parte de un Estado puede ser de utilidad para proteger dicha infraestructura o sector. Además de determinar las infraestructuras o los sectores de infraestructura que considera críticos, cada Estado determina las medidas estructurales, técnicas, organizacionales, legislativas y normativas necesarias para proteger su infraestructura crítica y restablecer la funcionalidad en caso de que se produzca un incidente".

---

[23] Mensaje de Twitter del Departamento de Estado de EE. UU., 28 de mayo de 2021, https://twitter.com/State_Cyber/status/1398314450743091201?s=20

[24] Copia anticipada, Informe del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional y Carta de Transmisión, 28 de mayo de 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

[25] Anexo a la carta dirigida al Secretario General con fecha del 9 de enero de 2015 de los representantes permanentes de China, Kazajistán, Kirguistán, la Federación Rusa, Tayikistán y Uzbekistán ante las Naciones Unidas [Original: chino y ruso], código internacional de conducta para la seguridad de la información, A/69/723, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement

Punto 49: “Algunos Estados actúan como hospedadores de infraestructuras que suministran servicios a nivel regional o internacional. Las amenazas de las TIC a esas infraestructuras podrían tener efectos desestabilizadores. Los Estados que participan en esa clase de acuerdos podrían alentar la cooperación transfronteriza con operadores y propietarios de infraestructuras competentes a fin de mejorar las medidas de seguridad de las TIC otorgadas a esa infraestructura y fortalecer los procesos y procedimientos complementarios existentes, o bien elaborar nuevos, para detectar y mitigar los incidentes de TIC que afecten dicha infraestructura”.

Punto 63: “Además, y en consulta con los agentes relevantes de la industria y otros del ámbito de la seguridad de las TIC, los Estados pueden, de acuerdo con las normas técnicas internacionales pertinentes, elaborar pautas e incentivos en relación con la notificación y gestión responsable de las vulnerabilidades y los respectivos roles y responsabilidades de las diferentes partes interesadas en los procesos de elaboración de informes, los tipos de información técnica que se divulgará o compartirá públicamente, incluido el intercambio de información técnica sobre incidentes de TIC que son graves, y la forma de manejar los datos sensibles y garantizar la seguridad y confidencialidad de la información”.

Punto 79: “El diálogo mediante consultas e instancias de participación bilaterales, subregionales, regionales y multilaterales puede promover el entendimiento entre los Estados, fomentar mayor confianza y contribuir a una cooperación más estrecha entre ellos para mitigar los incidentes de TIC y, a la vez, reducir los riesgos de errores de percepción y escalonamiento. Otras partes interesadas, tales como el sector privado, el sector académico, la sociedad civil y la comunidad técnica, pueden contribuir significativamente a facilitar dichas consultas e instancias de participación”.

Punto 87: “El Grupo destaca la importancia de la cooperación y la asistencia en el área de seguridad de las TIC y creación de capacidades, así como su importancia para todos los elementos del mandato del Grupo. Una mayor cooperación, junto con una asistencia y una creación de capacidades más eficaces en el área de seguridad de las TIC que involucren a otras partes interesadas, tales como el sector privado, el sector académico, la sociedad civil y la comunidad técnica, pueden ayudar a los Estados a aplicar el marco para el comportamiento responsable de los Estados al hacer uso de las TIC. Resultan vitales para subsanar las brechas existentes dentro y entre los Estados en materia de cuestiones técnicas, jurídicas y de política que son relevantes para la seguridad de las TIC. Asimismo, pueden contribuir a cumplir otros objetivos de la comunidad internacional, tales como los Objetivos de Desarrollo Sostenible (ODS)”.

Punto 95: “El Grupo también identificó posibles áreas para trabajos futuros, que incluyen, a mero modo enunciativo: [...] (d): ‘Identificar mecanismos que faciliten la participación de otras partes interesadas esenciales, incluidos el sector privado, el sector académico, la sociedad civil y la comunidad técnica, en los esfuerzos dirigidos a implementar el marco de comportamiento responsable, donde corresponda’”.

Actualización sobre el Comité Especial de Expertos de Composición Abierta (AHC)

El AHC tenía programado comenzar su trabajo en agosto de 2020, pero, debido a la pandemia de COVID-19, su primer período de sesiones de organización se llevó a cabo del 10 al 12 de mayo de 2021.[26] Desde la publicación del documento con fecha de julio de 2020 de la organización de la ICANN, se dieron a conocer algunos aportes nuevos en la página web del AHC.[27] En la primera reunión de su período de sesiones de organización, celebrada el 10 de mayo de 2021, el AHC eligió al Presidente del Comité, a su Relator y a 13 Vicepresidentes, que representan a diferentes regiones geográficas.[28] El AHC no logró alcanzar consenso sobre las modalidades de organización de sus reuniones futuras durante el tiempo asignado y el Presidente anunció que continuarán con consultas informales.[29]

El 26 de mayo de 2021, en su 71.ª reunión plenaria, la Asamblea General de la ONU adoptó, sin votación, el texto de la resolución A/RES/75/282 "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos".[30] Los documentos establecieron dos sedes para los períodos de sesiones del AHC: Viena y la ciudad de Nueva York. Se celebrarán siete períodos de sesiones en total y la sede de estos períodos de sesiones rotará entre Viena y la ciudad de Nueva York. El primero y el último período de sesiones se llevarán a cabo en la ONU en la ciudad de Nueva York. Las decisiones del AHC sobre cuestiones sustantivas sin aprobación por consenso se tomarán por mayoría de dos tercios de los representantes presentes con derecho a voto.

La resolución también alienta al presidente del AHC a llevar adelante consultas entre períodos de sesiones para solicitar aportes de una gama diversa de partes interesadas sobre la elaboración del proyecto de convención.

---

[26] Las reuniones del período de sesiones de organización del AHC pueden verse en los siguientes enlaces:
Primera reunión: https://media.un.org/en/asset/k1v/k1vgo4a624 (La segunda reunión no se llevó a cabo porque todas las cuestiones organizacionales se resolvieron durante la primera reunión)
Tercera reunión: https://media.un.org/en/asset/k1z/k1zsp4exqc
Cuarta reunión: https://media.un.org/en/asset/k12/k12bsxlcak
Quinta reunión: https://media.un.org/en/asset/k1m/k1ma80pf1p
Sexta reunión: https://media.un.org/en/asset/k1m/k1m0si6d6n

[27] "Comité Especial establecido en virtud de la resolución 74/247 de la Asamblea General", UNODC, https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

[28] El período de sesiones de organización del Comité Especial se celebró en Nueva York, del 10 al 12 de mayo de 2021. Resultados de las elecciones del Comité Especial https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

[29] Sexta reunión, Comité Especial Encargado de Elaborar una Convención Internacional Integral sobre el Ciberdelito, TV web de la ONU, 12 de mayo de 2021, (comienza en 3:24:34) https://media.un.org/en/asset/k18/k18lkzt0og

[30] Resolución adoptada por la Asamblea General el 26 de mayo de 2021, "75/282. Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", Distr.: 1 de junio de 2021, A/RES/75/282, https://undocs.org/a/res/75/282

Conclusión

El equipo de GE seguirá monitoreando los debates en el AHC y el nuevo OEWG, que realizarán su labor desde 2021 hasta 2025. Este OEWG celebró su primera reunión de organización el 1 de junio de 2021, en la que eligió al representante permanente de Singapur ante la ONU como Presidente.[31]

Las actualizaciones sobre el trabajo del OEWG, el GGE y el AHC, así como otras publicaciones del GE, se pueden consultar en la página web del GE de la organización de la ICANN.[32]

[31] 1 de junio, primera reunión: https://media.un.org/en/asset/k1o/k1oa2ngbsc
1 de junio, segunda reunión: https://media.un.org/en/asset/k14/k1443my9hu
[32] Página web del GE, sitio web de la ICANN: https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en

Apéndice

OEWG. Informe Final Sustantivo: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

OEWG. Resumen de la Presidencia: 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, tercer período de sesiones sustantivo, del 8 al 12 de marzo de 2021
https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

OEWG. Grabación en video de la tercera reunión sustantiva, del 8 al 12 de marzo de 2021

8 de marzo de 2021
Día 1: primera reunión
https://media.un.org/en/asset/k1o/k1obxycc3u

Día 1: segunda reunión
https://media.un.org/en/asset/k18/k1893g1q0h

9 de marzo de 2021
Día 2: tercera reunión
https://media.un.org/en/asset/k13/k13uzdidth

Día 2: cuarta reunión
https://media.un.org/en/asset/k1h/k1huoxryeo

10 de marzo de 2021
Día 3: quinta reunión
https://media.un.org/en/asset/k1d/k1d4e06j0x

Día 3: sexta reunión
https://media.un.org/en/asset/k1m/k1mqlxrfv4

11 de marzo de 2021
Día 4: la séptima y la octava reunión no se celebraron. Se dedicó el día a debates bilaterales y consultas con las capitales.

12 de marzo de 2021
Día 5: novena reunión
https://media.un.org/en/asset/k1r/k1rf2exuhz**}**

Día 5: décima reunión (El sitio web de la ONU no brinda un enlace a la grabación de esta sesión).

Día 5: decimoprimera reunión, sesión final del OEWG (adopción del informe sustantivo por consenso) https://media.un.org/en/asset/k1p/k1prn29un6