Actualización de las Naciones Unidas: Avances Relacionados con el Ciberespacio

Actualización de las Naciones Unidas: Avances Relacionados con el Ciberespacio en el Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso (OEWG), el Comité Especial de Expertos de Composición Abierta para la Elaboración de un Convenio Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, el Pacto Digital Mundial y otros debates relacionados con las Naciones Unidas.

GE-014
15 de diciembre de 2023

ICANN

ÍNDICE

Introducción

El presente documento ofrece información actualizada sobre las deliberaciones de la Asamblea General de las Naciones Unidas (AGNU), donde se debaten cuestiones relacionadas con el ciberespacio. Incluye actualizaciones sobre los debates del segundo Grupo de Trabajo de Composición Abierta (OEWG)[1] y del Comité Especial de Expertos de Composición Abierta (AHC)[2] del 4 de junio de 2021 al 2 de septiembre de 2023, así como debates más recientes sobre el Pacto Digital Mundial en 2023.

Como parte de una serie periódica de informes, este documento ofrece una visión general de las actividades que tienen lugar en las Naciones Unidas y que son relevantes para el ecosistema de Internet y para la misión de la Corporación para la Asignación de Nombres y Números en Internet.[3] El seguimiento de estas actividades demuestra el compromiso y la responsabilidad del equipo de Participación Gubernamental y Organizaciones Intergubernamentales (GE) de la organización de la ICANN (org) de mantener informada a la comunidad de la ICANN en general sobre cuestiones de importancia para la Internet mundial, única e interoperable y su sistema de identificadores únicos.[4]

[1] Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso (OEWG), https://meetings.unoda.org/meeting/57871/statements

[2] Comité Especial de Expertos de Composición Abierta para la Elaboración de un Convenio Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos,https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[3] Ver informes anteriores de GE en este enlace: https://www.icann.org/en/government-engagement/publications Este y todos los demás URL de las notas a pie de página y los apéndices se obtuvieron el [insertar] de agosto de 2023.

[4] "Planes Operativos y Financieros de la ICANN", p. 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

Novedades del OEWG

Primera sesión sustantiva[5]

9 de diciembre de 2021

China: "El actual sistema de distribución y gestión de los recursos críticos de Internet es desequilibrado e injusto". [...] "Los Estados deben participar en la gestión y distribución de los recursos internacionales de Internet en pie de igualdad, y construir un sistema de gobernanza mundial de Internet de multilateralismo, democracia y transparencia".[6]

12 de diciembre de 2021

China: "los Estados tienen derecho a ejercer, de conformidad con los principios y normas de derecho internacional universalmente reconocidos, la jurisdicción personal, territorial y de protección necesaria y razonable sobre actividades específicas en materia de TIC fuera de sus territorios que tengan una conexión genuina y sustancial con los Estados, así como sobre las instalaciones, entidades, datos e información pertinentes relacionados con las TIC. Para ejercer su jurisdicción, un Estado puede solicitar la asistencia de otros Estados y regiones en un espíritu de autocontrol, cortesía y reciprocidad".
[...]
"Manifestación de la soberanía en la capa física. Los Estados tienen jurisdicción sobre la infraestructura física y los servicios básicos de las TIC dentro de sus territorios. Los Estados tienen derecho a adoptar las medidas necesarias para mantener la seguridad de la infraestructura física de acuerdo con la legislación nacional y conforme al derecho internacional. Los Estados tienen derecho a participar en la gestión de la infraestructura mundial de Internet y en la cooperación internacional al respecto". [...] "Manifestación de la soberanía en la capa lógica. Los Estados pueden promulgar o adoptar de forma independiente las normas o reglamentos técnicos pertinentes, manteniendo al mismo tiempo la interoperabilidad de Internet de conformidad con sus obligaciones en virtud del derecho internacional".[7]

Contexto: En un reciente libro blanco que publicó la Oficina de Información del Consejo de Estado de la República Popular China, cabe citar los siguientes puntos sobre la gobernanza y los recursos críticos de Internet:

"Capítulo III, Punto 3: Participación activa en la gobernanza del ciberespacio
China ha participado activamente en el funcionamiento de las organizaciones mundiales de Internet. Ha participado activamente en las actividades de plataformas y organizaciones como la Corporación para la Asignación de Nombres y Números en Internet (ICANN). Ha apoyado la reforma del mecanismo de gobernanza de la ICANN para aumentar la representación de los

[5] Las citas de las sesiones del OEWG y el AHC incluyen declaraciones escritas y orales
[6] Opiniones de China sobre la aplicación del principio de soberanía en el ciberespacio, 9 de diciembre de 2021, pág. 1, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf
[7] Opiniones de China sobre la aplicación del principio de soberanía en el ciberespacio, 12 de diciembre de 2021, págs. 1 y 4, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

países en desarrollo y poner más recursos de información de Internet bajo una gestión mundial concertada. China también ha participado en las actividades de la Internet Society (ISOC), el Grupo de Trabajo en Ingeniería de Internet (IETF) y la Junta de Arquitectura de Internet (IAB). Ha desempeñado una función constructiva facilitando el intercambio entre comunidades, promoviendo la I+D técnicos y su aplicación, y participando estrechamente en la formulación de las normas y reglas pertinentes".
[...]

Capítulo IV, Punto 5: 5. Mantener la seguridad y estabilidad del sistema de gestión de recursos básicos de Internet
El sistema de gestión de los recursos básicos de Internet es la piedra angular de su funcionamiento. Debe garantizarse que las instituciones que albergan los sistemas de gestión operen con plena credibilidad y no supongan una amenaza para los dominios de alto nivel de ningún país solo por las exigencias jurisdiccionales de algún otro país. China aboga por que se garantice la disponibilidad y confiabilidad de los recursos básicos de Internet, que deben ser utilizados por todos los países y gestionados conjuntamente y distribuidos equitativamente por la comunidad internacional, de modo que los sistemas tecnológicos para los recursos, incluido el sistema de nombres de dominio, sean seguros, estables y resilientes. Debe existir la garantía de que los servicios no se interrumpirán o cancelarán debido a cualquier factor político o humano. China aboga por que los gobiernos, las autoridades industriales y las empresas trabajen conjuntamente para acelerar el uso de la tecnología y las aplicaciones IPv6".[8]

[8] Xinhua, China publica un libro blanco sobre la comunidad con un futuro compartido en el ciberespacio, 7 de noviembre de 2022
https://english.www.gov.cn/archive/whitepaper/202211/07/content_WS636894aac6d0a757729e2973.html

14 de diciembre de 2021

Portugal: "Un férreo esfuerzo de cooperación internacional en relación a la resiliencia de las infraestructuras críticas nacionales de todos los Estados miembros de las Naciones Unidas y del núcleo de Internet que los une a todos en consonancia con los derechos humanos, el derecho internacional y según los más altos parámetros es esencial para disuadir los ciberataques por debajo del umbral del conflicto armado".[9]

China: "El futuro de Internet no debe ni puede estar controlado por un puñado de países. Formar pequeños círculos ideológicamente excluyentes y aferrarse al monopolio de las TIC y a la armonía del ciberespacio solo obstaculizará los esfuerzos multilaterales para promover la ciberseguridad. Ciertos países han intentado lanzar la llamada "alianza por el futuro de Internet", que no es más que el ejemplo de los intentos de dividir Internet, procurar el monopolio tecnológico y la hegemonía del ciberespacio y suprimir el desarrollo científico y tecnológico de otros países solo para servir a su propia agenda geopolítica. Afirman construir una Internet abierta, pero en realidad están atizando la confrontación y dividiendo Internet, lo que va totalmente en contra del espíritu de paz, seguridad, apertura y cooperación de Internet y del interés común de la comunidad internacional".[10]

"Mientras tanto, en consonancia con los atributos de las TIC y las necesidades de [la] situación cambiante, deberíamos debatir la formulación de nuevas normas. La seguridad de los datos es un nuevo desafío importante al que se enfrentan todos los países. Sobre la base del mandato de la resolución, las partes mantendrán debates en profundidad sobre cuestiones como el flujo transfronterizo de datos, la seguridad de la cadena de suministro y la protección de la información personal, y estudiarán las respuestas adecuadas. La Iniciativa Global sobre Seguridad de Datos de China podría servir de base preliminar para el debate".[11]

Contexto: En la misma declaración, se critican las iniciativas de otros países y se propone una "Iniciativa sobre Seguridad de Datos" propia de China que "podría servir de base preliminar para el debate".

España: "Si no logramos ponernos de acuerdo sobre una normativa mundial en el seno de las Naciones Unidas, las actuales tensiones geopolíticas podrían conducir a una fragmentación del ciberespacio en varias áreas de influencia con certificación de normas y especificidades técnicas incompatibles entre sí".[12]

---

[9] UN Web TV, 3.ª reunión plenaria, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Primera sesión sustantiva, 14 de diciembre de 2021, https://media.un.org/en/asset/k11/k11eljcg88 (comienza en 1:14:20)

[10] UN Web TV, 3.ª reunión plenaria, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Primera sesión sustantiva, 14 de diciembre de 2021, https://media.un.org/en/asset/k11/k11eljcg88 (comienza en 1:50:40)

[11] Declaración del Consejero Wu Jianjian, Jefe de la Delegación China en el Intercambio General de Puntos de Vista de la Primera Sesión Sustantiva del Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y de su Uso, 14 de diciembre de 2021, https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-3rd-plenary-meeting_General-Exchange-of-Views_DEC-14-AM_ENG.pdf

[12] UN Web TV, 4.ª reunión plenaria, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Primera sesión sustantiva, 14 de diciembre de 2021, https://media.un.org/en/asset/k1b/k1b55qgp81 (comienza en 4:30)

China: "El ciberespacio corre el riesgo de fragmentarse. El Secretario General de las Naciones Unidas, Guterres, advirtió durante la Asamblea General de este año que el mundo corre el riesgo de dividirse en dos con dos conjuntos de normas en conflicto. Lo mismo ocurre con el ciberespacio".[13]

República Islámica de Irán: “Esto requiere un enfoque más global de las amenazas en el ámbito de la seguridad de la información que aborde no solo la infraestructura digital, sino también el contenido y la información en sí. Algunos ejemplos de amenazas urgentes y desafiantes, existentes y potenciales, a las que se enfrentan los Estados son los siguientes: (1) monopolio y hegemonía en la gobernanza de Internet..."[14]

Contexto: No hay pruebas de ningún "monopolio y hegemonía" en la gobernanza de Internet. La gobernanza de Internet se ha debatido ampliamente en la CMSI y durante las negociaciones de la CMSI+10 en la Asamblea General de las Naciones Unidas, y no se ha llegado a dicha conclusión en la Agenda de Túnez de la CMSI ni en el Documento de Resultados de la CMSI+10.

15 de diciembre de 2021

Países Bajos: "Algunos ejemplos de desafíos existentes y amenazas potenciales a los que se enfrenta la comunidad mundial incluyen las operaciones cibernéticas contra la integridad, el funcionamiento y la disponibilidad de Internet, tal como se menciona en el acervo. Esta infraestructura técnica esencial para la disponibilidad general o la integridad de Internet, o el núcleo público, fue mencionada como infraestructura crítica tanto en los informes anteriores del OEWG y del GGE (norma 13f). Esta infraestructura técnica esencial para el funcionamiento general de Internet también necesita protección contra las tendencias a controlarla en una forma que socave la integridad o disponibilidad de Internet. Estas tendencias proceden de un amplio abanico de actores. En particular, el modelo de gobernanza de Internet, que se basa en la gobernanza multilateral, no debería verse socavado en modo alguno. El sector privado, la sociedad civil, la comunidad técnica y otras partes interesadas son indispensables para el funcionamiento de Internet".[15]

República Islámica de Irán: “En nuestra opinión una reforma significativa de la actual gobernanza de Internet, un acceso abierto, justo y no discriminatorio de los Estados a las tecnologías de la información y la comunicación y una cadena de suministro de ciberseguridad

[13] UN Web TV, 4.ª reunión plenaria, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Primera sesión sustantiva, 14 de diciembre de 2021, https://media.un.org/en/asset/k1b/k1b55qgp81 (comienza en 1:56:42)
[14] UN Web TV, 4.ª reunión plenaria, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Primera sesión sustantiva, 14 de diciembre de 2021, https://media.un.org/en/asset/k1b/k1b55qgp81 (comienza en 2:35:20)
[15] UN Web TV, 5.ª reunión plenaria, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Primera sesión sustantiva, 15 de diciembre de 2021, https://media.un.org/en/asset/k1r/k1royetcr4 (comienza en 39:42), también aquí: Declaración de S.E Nathalie Jaarsma, Embajadora en Misión Especial para Políticas de Seguridad y Cibernética, 15 de diciembre de 2021, https://documents.unoda.org/wp-content/uploads/2021/12/21.12.15-Netherlands-Statement-on-Threats-OEWG-in-the-Field-of-Information-and-Telecommunications-in-the-Context-of-Internat.pdf

confiable son requisitos esenciales de un comportamiento responsable de los Estados en el entorno de las TIC".[16]

Contexto: El Grupo de Trabajo de las Naciones Unidas sobre Gobernanza de Internet (WGIG) elaboró esta definición de Gobernanza de Internet: "La gobernanza de Internet es el desarrollo y la aplicación de principios, normas, reglas, procedimientos para la toma de decisiones y programas compartidos por parte de los gobiernos, el sector privado y la sociedad civil —en sus respectivos roles—, que dan forma a la evolución y el uso de Internet".[17] Por consiguiente, no se refiere a los temas de la declaración. El estado actual de la gobernanza de Internet se debate cada año en el Foro de Gobernanza de Internet (IGF), que es el lugar adecuado para dichos debates porque está abierto a cualquier persona interesada en participar. El futuro de la gobernanza de Internet se debatirá durante la CMSI+20 en 2025, en la Asamblea General de las Naciones Unidas.

India: "Tenemos que debatir las obligaciones para no realizar ni permitir conscientemente ataques al núcleo público de Internet. Eso incluye: enrutamiento de paquetes y elementos de reenvío, sistemas de nombres y números, mecanismos criptográficos de seguridad e identidad, medios de transmisión, software y centros de datos".[18]

16 de diciembre de 2021

Costa Rica: "Las prácticas y lecciones recomendadas también podrían extraerse de la comunidad técnica, dado que los CERT han dirigido comunidades que se basan en relaciones de confianza para intercambiar información con el fin de responder a eventos relacionados con las TIC. Podemos extraer lecciones sobre la importancia de ir más allá de la mera enumeración de nombres en un directorio, sino más bien convocar reuniones o realizar ejercicios para crear confianza y relaciones dentro de la red".[19]

17 de diciembre de 2021

República Islámica de Irán: "El OEWG debe abordar las principales fuentes de desconfianza en el entorno de las TIC, en particular el monopolio en la gobernanza de Internet, el anonimato, las ciberestrategias ofensivas, la creación de una imagen hostil y la xenofobia que conducen a medidas coercitivas unilaterales, y la falta de responsabilidad de las empresas y plataformas privadas y de sus Estados nacionales por las actividades extraterritoriales. Por ejemplo, el

[16] UN Web TV, 6.ª reunión plenaria, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Primera sesión sustantiva, 15 de diciembre de 2021, https://media.un.org/en/asset/k1r/k1rnexulnt (comienza en 50:35)
[17] Informe del Grupo de Trabajo de las Naciones Unidas sobre Gobernanza de Internet, junio de 2005, punto 10, https://www.wgig.org/docs/WGIGREPORT.pdf
[18] UN Web TV, 6.ª reunión plenaria, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Primera sesión sustantiva, 15 de diciembre de 2021, https://media.un.org/en/asset/k1r/k1rnexulnt (comienza en 1:48:55)
[19] UN Web TV, 8.ª reunión plenaria, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Primera sesión sustantiva, 16 de diciembre de 2021, https://media.un.org/en/asset/k1y/k1yzr8yhb1 (comienza en: 57:20), también aquí: Misión Permanente de Costa Rica ante las Naciones Unidas, declaración, 16 de diciembre de 2021, https://documents.unoda.org/wp-content/uploads/2021/12/Final-Costa-Rica-CBMs-1612021-SP-EN.pdf

punto de partida es llevar a cabo una gobernanza de Internet multilateral, justa y transparente".[20]

Contexto: No hay pruebas de ningún "monopolio en la gobernanza de Internet". La gobernanza de Internet está definida en la Agenda de Túnez de la CMSI y todas las partes interesadas, incluidos los gobiernos, participan en ella. Tampoco existe un consenso probado para un nuevo modelo multilateral de gobernanza de Internet. Así lo afirmó Alemania el 28 de marzo de 2022 (Consultar la cita a continuación).

[20] Presentación para la primera sesión sustantiva, Irán (República Islámica de), 17 de diciembre de 2022, págs. 8-9, https://documents.unoda.org/wp-content/uploads/2021/12/Irans-submission-to-first-substantive-session_13-17-Dec-21.pdf

Segunda sesión sustantiva

28 de marzo de 2022

Subsecretario General de las Naciones Unidas, Izumi Nakamitsu: "Es universalmente reconocido: la participación de múltiples partes interesadas es esencial en el ámbito de la seguridad de las TIC, donde los actores privados poseen y gestionan gran parte de la infraestructura relevante".[21]

EE. UU.: "Este proceso [del OEWG] hoy aquí [...] pertenece a todos los estados miembros que procuran preservar la estabilidad en el ciberespacio, pertenece a todas las partes interesadas que se benefician de una Internet abierta, interoperable, segura y confiable para todos..."[22]

Alemania: "Internet no es propiedad ni está bajo el control de los Estados. Es un dominio público gestionado y promovido por un conjunto muy complejo y eficiente de agentes que representan a la industria, la sociedad civil y los gobiernos. La participación en este Grupo de Trabajo de Composición Abierta debería reflejar plenamente esta realidad".[23]

España: "Vemos la verdadera amenaza de la fragmentación dentro de esferas que podrían afectar las especificaciones técnicas que podrían terminar siendo totalmente incompatibles entre sí. No podemos permitir que esto ocurra porque afectará directamente a todos nuestros países".[24]

29 de marzo de 2022

Federación Rusa: “Por ejemplo, existe la posibilidad absolutamente real de que todo un país quede aislado de los sistemas de comunicaciones internacionales, en particular de Internet, o del sistema interbancario de transporte de información y de realización de pagos, SWIFT. No es una amenaza teórica; es lo que le está sucediendo a mi país. La experiencia demuestra que la tecnología permite llevar a cabo esta amenaza, ya que estos sistemas son gestionados por un país o un grupo muy reducido de países. Por ende, tomando como ejemplo Internet, sería la corporación para la gestión de los nombres de dominio y las direcciones IP, la ICANN. Se trata de una organización internacional sin fines de lucro que, de hecho, está totalmente controlada

[21] UN Web TV, (1.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 29 de marzo de 2022, https://media.un.org/en/asset/k1h/k1hhzc7i5z (comienza en 6:27)
[22] UN Web TV, (1.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 29 de marzo de 2022, https://media.un.org/en/asset/k1h/k1hhzc7i5z (comienza en 35:00)
[23] UN Web TV, (1.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 29 de marzo de 2022, https://media.un.org/en/asset/k1h/k1hhzc7i5z (comienza en 1:13:55), y también aquí: Declaración de Alemania en el OEWG de marzo, tema 3 del orden del día, 22 de abril de 2022, pág. 3, https://documents.unoda.org/wp-content/uploads/2022/04/German-Statement-at-the-March-2022-OEWG-Agenda-Item-3.pdf)
[24] UN Web TV, (1.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 29 de marzo de 2022, https://media.un.org/en/asset/k1h/k1hhzc7i5z (comienza en 1:52:38)

por los Estados Unidos de América. Estas condiciones hacen que cualquier país... ¡cualquiera! ...sea vulnerable a las decisiones políticas de dicho país".[25]

Contexto: La ICANN no está en condiciones de "interrumpir" (detener, cerrar, etc.) Internet en ningún país. Esto se afirma de manera clara en una carta con fecha del 2 de marzo de 2022, dirigida por el Presidente y Director Ejecutivo de la ICANN en respuesta al Viceprimer Ministro de Ucrania.[26] El Registro Regional de Internet para Europa, Oriente Medio y partes de Asia Central, Centro de Coordinación de Redes RIPE (RIPE NCC) expresó una postura similar en una publicación con fecha del 10 de marzo de 2022.[27] Esto también se constató el 5 de abril de 2022, cuando la Sra. Fiona Alexander[28] expresó: "La Federación Rusa estaba mejor protegida en el modelo de múltiples partes interesadas que en el sistema de las Naciones Unidas". De modo que mientras el ministro ucraniano pedía tanto a RIPE como a la ICANN que le quitaran sus recursos de Internet, ambos dijeron "no".[29] Pero en marzo de 2022, en la Asamblea Mundial de Normalización de las Telecomunicaciones de la UIT, el gobierno ruso fue despojado de las posiciones de liderazgo en los grupos de estudio a petición de Ucrania.[30] Por lo tanto, aunque la Federación Rusa participa en la ICANN, quiere que sea asumida por la UIT o sustituida. Me pareció irónico que el modelo de múltiples partes interesadas protegiera mejor al pueblo de Rusia y a Internet que el sistema de las Naciones Unidas, en el que el gobierno ruso fue despojado de su rol".[31] El 6 de abril de 2022, la Casa Blanca publicó una hoja informativa sobre las sanciones de Estados Unidos, el G7 y la UE a Rusia, en la que afirma que el acceso a Internet no es un objetivo de las sanciones.[32]

Malasia: "A este respecto [nosotros] podríamos considerar que es necesario centrarse en medidas rápidas y efectivas por parte del proveedor de alojamiento y las entidades encargadas del cumplimiento de la ley, los proveedores de servicios de Internet, los registradores de

[25] UN Web TV, (3.ª reunión) Grupo de trabajo de composición abierta sobre la seguridad de las tecnologías de la información y las comunicaciones y de su uso 2021-2025, Segunda sesión sustantiva, 29 de marzo de 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (comienza en 51:05)

[26] Carta de Göran Marby, Presidente y Director Ejecutivo de la Corporación para la Asignación de Nombres y Números en Internet (ICANN) a Mykhailo Fedorov, Viceprimer Ministro, Ministro de Transformación Digital de Ucrania, 2 de marzo de 2022, https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

[27] RIPE NCC, Respuesta de RIPE NCC a la solicitud del Gobierno ucraniano, 10 de abril de 2022, https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[28] En la actualidad, Fiona Alexander es una distinguida estratega política residente en la Escuela de Servicio Internacional y una distinguida becaria en el Laboratorio de Gobernanza de Internet de la American University. Durante casi 20 años, Fiona trabajó en la Administración Nacional de Telecomunicaciones e Información (NTIA) del Departamento de Comercio de los Estados Unidos, donde fue Administradora Asociada de Asuntos Internacionales.

[29] Respuesta de RIPE NCC a la solicitud del Gobierno de Ucrania, Carta del Viceprimer Ministro de Ucrania a RIPE NCC (PDF), Respuesta del Director General de RIPE NCC (PDF), Ámsterdam, 10 de marzo de 2022, https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[30] Cuenta oficial de Twitter de la Misión Permanente de Ucrania para la oficina de las Naciones Unidas en Ginebra, 9 de marzo de 2022, https://twitter.com/UKRinUNOG/status/1501658319932600326, Sitio web de la Misión Permanente de la República Checa para la oficina de las Naciones Unidas en Ginebra, 9 de marzo de 2022, https://www.mzv.cz/mission.geneva/en/specialized_agencies/international_telecommunication_union/russia_s_military_aggression_against.html

[31] Fiona Alexander, seminario web de ITIF, Gobernanza de Internet durante Tiempos de Guerra y Conflictos, 5 de abril de 2022, (comienza en 58:57), https://itif.org/events/2022/04/05/internet-governance-during-times-war-and-conflict

[32] La Casa Blanca, Sala de Prensa, HOJA INFORMATIVA: Estados Unidos, el G7 y la UE Imponen Costos Severos e Inmediatos a Rusia, 6 de abril de 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/factsheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/

nombres de dominio en el bloqueo y retirada de sitios maliciosos a nivel del proveedor de alojamiento, especialmente aquellos que afectan a la infraestructura crítica de información".[33]

Países Bajos: "Las iniciativas que dañan la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet, también denominada núcleo público de Internet, incluyen las operaciones cibernéticas que tienen como objetivo la infraestructura física y lógica central de Internet, o las organizaciones que son fundamentales para el enrutamiento, los nombres y los números a nivel mundial, como los registros regionales de Internet, la ICANN y los grandes puntos de intercambio de Internet. También incluyen las que introducen normas y protocolos de Internet que socavan el carácter abierto e interoperable de Internet. Para profundizar aún más en nuestra comprensión técnica del núcleo público, los Países Bajos iniciarán actividades sobre el núcleo público para ahondar nuestra comprensión técnica conjunta entre esta comunidad del Grupo de Trabajo de Composición Abierta".[34]

República Islámica de Irán: "Sin perjuicio de los riesgos derivados del monopolio existente en la gobernanza de Internet y de la necesidad de una nueva arquitectura, esta cuestión aún no se ha debatido eficazmente en el sistema de las Naciones Unidas desde la Cumbre Mundial sobre la Sociedad de la Información (CMSI) celebrada en Túnez en 2005 (artículos 29 a 82 de la Agenda de Túnez para la Sociedad de la Información). Es lamentable que el Foro de Gobernanza de Internet (IGF) se niegue a debatir esta cuestión y la remita al OEWG, mientras que el OEWG considera que está fuera de su mandato debatir la gobernanza de Internet y la remite al IGF. Como consecuencia, la comunidad internacional no ha sido capaz de alcanzar un consenso sobre la gobernanza mundial de Internet que elimine el actual monopolio sobre la gobernanza de Internet. La comunidad internacional debe esbozar en breve, en el seno del OEWG, una solución mejor para la gobernanza de Internet que proteja la estabilidad y la seguridad del entorno de las TIC".[35]

Contexto: También en este caso, como a principios de semana, Irán afirma que existe un "monopolio en la gobernanza de Internet", opinión que no se sustenta en hechos. Además, Irán afirma que es necesaria "una nueva arquitectura", pero no está claro cuál sería esa "nueva arquitectura". Sin embargo, la cuestión de las mejoras de la arquitectura de cooperación digital se abordó en la Hoja de Ruta para la Cooperación Digital del Secretario General de las Naciones Unidas. En 2022, el Secretario General de las Naciones Unidas creó el Grupo de Liderazgo de Alto Nivel del IGF, un órgano de múltiples partes interesadas para apoyar y fortalecer el IGF.[36] Además, todas las cuestiones relacionadas con la gobernanza de Internet se han debatido desde 2003 en el marco de la CMSI y de la revisión de la CMSI+10, así como, en varias ocasiones, en el IGF. Irán afirma que el IGF "se niega a debatir esta cuestión", pero el

[33] UN Web TV, (3.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 29 de marzo de 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (comienza en 1:18:48)
[34] UN Web TV, (3.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 29 de marzo de 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (comienza en 1:26:20)
[35] UN Web TV, (3.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 29 de marzo de 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (comienza en 1:35:05), y también aquí: Declaración de la Delegación de la República Islámica de Irán ante la segunda sesión sustantiva del Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y de su Uso, 29 de marzo de 2022, pág. 3, https://documents.unoda.org/wp-content/uploads/2022/03/1-Introductory-Remarks-Existing-and-Potential-Threats.pdf
[36] Consultar también, Naciones Unidas, Panel de Alto Nivel del Secretario General sobre la Cooperación Digital, https://www.un.org/es/sg-digital-cooperation-panel

IGF debate activamente todas las cuestiones que los participantes han planteado en forma de propuestas, que han sido aceptadas por el Grupo Asesor de Múltiples Partes Interesadas del IGF. La gobernanza de Internet es mundial, y se describe y explica correctamente en los documentos de la CMSI.[37]

Francia: “Mi delegación desea llamar la atención del Grupo sobre las amenazas a la naturaleza libre e interoperable del ciberespacio. En el contexto de la atención internacional, podríamos ver un creciente aislamiento del ciberespacio [...] incluso en los niveles más profundos. [...] Nunca se han impuesto sanciones con respecto al acceso de los Estados a los niveles más profundos de Internet. Pero esta tentación se discute cada vez más y es muy peligrosa. Esta fragmentación conlleva riesgos no solo para los respectivos derechos humanos, para la libre circulación de la información, el crecimiento económico, sino cada vez más para la estabilidad internacional. En efecto, si tenemos varias Internets diferentes, los Estados podrían decidir llevar a cabo actividades malévolas si consideran que podrían hacerlo protegiendo la Internet precaria, y tener otra además de esa. Nuestro grupo debe tenerlo en cuenta y debe dirigir el camino para redoblar nuestros esfuerzos para preservar la arquitectura del ciberespacio libre, que sea singular, abierto, estable, seguro y universalmente accesible".[38]

30 de marzo de 2022

Países Bajos: “Para los Países Bajos, la protección del núcleo público incluye respetar su modelo de gobernanza de múltiples partes interesadas y evitar la incorporación de normas y protocolos que socaven la naturaleza abierta e interoperable de Internet. En este contexto, y como reacción a lo que se sugirió ayer, me gustaría destacar que el rol de las organizaciones de múltiples partes interesadas, como la ICANN y los Registros Regionales de Internet, es garantizar la coordinación técnica de Internet y trabajar para mantener una Internet única, global e interoperable, que siga funcionando en todo momento y sea accesible para todos...”[39]

Federación Rusa: "Todos los Estados deberían desempeñar la misma función en la gobernanza internacional de Internet y asumir la misma responsabilidad por la misma".[40]

Contexto: No existen pruebas de que los Estados no desempeñen una "función equitativa en la gobernanza internacional de Internet", ni de que no "tengan la misma responsabilidad" al respecto.

---

[37] Carta conjunta del Panel de Liderazgo y el Grupo Asesor de Múltiples Partes Interesadas a los cofacilitadores del Pacto Digital Mundial, "El Foro de Gobernanza de Internet de las Naciones Unidas está preparado para aceptar las responsabilidades derivadas de la revisión periódica y el seguimiento multisectorial del Pacto Digital Mundial", 16 de octubre de 2023., https://www.intgovforum.org/en/filedepot_download/24/26649

[38] UN Web TV, (3.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025, 3.ª reunión, 29 de marzo de 2022, https://media.un.org/en/asset/k1l/k1l7rcax4f (comienza en 15:07)

[39] UN Web TV, (5.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 30 de marzo de 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (comienza en 1:00:07)

[40] UN Web TV, (5.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 30 de marzo de 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (comienza en 1:10:18) y también aquí: Declaración del Jefe de la Delegación de la Federación Rusa, V. Shin, 30 de marzo de 2022, pág. 3, https://documents.unoda.org/wp-content/uploads/2022/03/Russia-OEWG-statement-3-30.03.2022-Eng.pdf)

China: “Ningún país debería sabotear la infraestructura crítica de otros Estados con TIC, ni participar en la destrucción o el robo de datos importantes de dicha infraestructura. Los Estados deben mejorar la legislación sobre la protección de la infraestructura crítica de información (CII)" [...]. "A partir del 1 de septiembre de 2021 entró en vigencia, en China, el reglamento sobre la protección de la seguridad de la infraestructura crítica de información. Según el reglamento, la infraestructura crítica de información se define como redes y sistemas de información importantes de industrias y sectores clave, como los servicios públicos de telecomunicaciones e información, energía, transporte, obras hidráulicas, finanzas, servicio público, gobierno electrónico y defensa, ciencia y tecnología. Y existen otras redes y sistemas de este tipo cuya afectación, pérdida de funcionamiento o violación de datos puede poner en grave peligro la seguridad nacional, la economía nacional y los intereses públicos. China celebra los exhaustivos debates dentro del OEWG sobre la definición y protección de la infraestructura crítica conforme al principio de soberanía"".[41]

Portugal: "La manipulación de las IP en el contexto de ataques contra el núcleo de Internet o contra la integridad de los procesos electorales también puede ser fundamental".[42]

Singapur: “Un ejemplo de infraestructura crítica podrían ser los sistemas de infraestructura técnica esenciales para la disponibilidad general o la integridad de Internet".[43]

Federación Rusa: “En la fase actual del desarrollo de las TIC, identificar inequívocamente el origen de la actividad perjudicial no parece posible sin una reforma en profundidad de los protocolos de funcionamiento de la red mundial de comunicaciones y sin organizar la necesaria cooperación entre Estados. En este sentido, el establecimiento de un mecanismo claro de cooperación entre los organismos estatales autorizados en la línea de la cooperación CERT-a-CERT es muy relevante".[44]

Contexto: No hay pruebas de que dicha "reforma en profundidad de [Internet]" sea necesaria para el propósito declarado. En todo el mundo existen innumerables casos delictivos en los que las fuerzas de seguridad pudieron identificar el origen de la actividad descrita.[45]

---

[41] UN Web TV, (5.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 30 de marzo de 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (comienza en 1:57:29)

[42] UN Web TV, (5.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 30 de marzo de 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (comienza en 2:06:50)

[43] UN Web TV, (5.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 30 de marzo de 2022, https://media.un.org/en/asset/k1g/k1gu15nuh2 (comienza en 2:36:05)

[44] UN Web TV, (6.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 30 de marzo de 2022, https://media.un.org/en/asset/k1j/k1jpaw8mgf (comienza en 34:40)

[45] Consultar el Informe del Ministerio del Interior de la Federación Rusa (MVD) sobre el Estado de la Delincuencia en Rusia en el Período Comprendido entre Enero y Noviembre de 2022, pág. 3, punto 9. https://d-russia.ru/wp-content/uploads/2022/12/mvd_22_11_.pdf o el Informe del FBI de 2022 sobre la delincuencia en Internet, pág. 8, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf o Delitos en India, Ministerio del Interior, Oficina Nacional de Registros de Delitos, India, TABLA 9A.2 Delitos cibernéticos - Casos de la Ley de TI (por tipología de delito y por Estado/UT) - 2021, https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/post/1679661922TABLE9A2.pdf

31 de marzo de 2022

Canadá: ""Por ejemplo, en la OSCE abogamos por las CBM 4, junto con Kazajstán.
Su objetivo es promover el intercambio de información sobre enfoques nacionales para garantizar una Internet abierta, segura e interoperable.
Esperamos que este trabajo contribuya a proteger la disponibilidad general y la integridad de Internet, un objetivo compartido por los Países Bajos y otros países que lo han mencionado esta semana".[46]

República Islámica de Irán: "Las medidas de fomento de la confianza en el ciberespacio (TCBM) se incorporarán a un entorno de TIC para hacer frente a las principales fuentes de desconfianza en el entorno de las TIC, en particular el monopolio en la gobernanza de Internet, el anonimato, las estrategias cibernéticas y políticas ofensivas, la creación de una imagen hostil y la xenofobia, las medidas coercitivas unilaterales y la falta de responsabilidad de las empresas privadas, así como de las plataformas y sus respectivos Estados por las actividades extraterritoriales".

Creemos que el punto de partida es llevar a cabo una gobernanza de Internet multilateral, justa y transparente. En nuestra opinión, el monopolio (en la gestión) y el anonimato (de personas y cosas) son las principales fuentes de desconfianza en Internet, lo que hace necesarias las CBM pertinentes. Lo primero y más importante es abordar las deficiencias y desventajas del actual sistema de gobernanza de Internet con vistas a hacer realidad la tan esperada gobernanza justa de Internet".[47]

Tercera sesión sustantiva

25 de julio de 2022

Subsecretario General, Izumi Nakamitsu: "Agradezco las propuestas relacionadas con el fortalecimiento de la protección de la infraestructura crítica y de la infraestructura crítica de la información, incluida la mejora de las interacciones con las partes interesadas en este tema. Esto está en consonancia con la petición del Secretario General de dar prioridad a las medidas que mejoren la protección de la infraestructura crítica, incluido el sector de la salud".[48]

Además: “He recalcado repetidamente la importancia de la participación de las partes interesadas de manera inclusiva y sostenida, dada la naturaleza única de las TIC y la función

[46] UN Web TV, (7.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 31 de marzo de 2022, https://media.un.org/en/asset/k1i/k1iykegjsm (comienza en 22:40)
[47] UN Web TV, (7.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Segunda sesión sustantiva, 31 de marzo de 2022, https://media.un.org/en/asset/k1i/k1iykegjsm (comienza en 31:50), y también aquí: Declaración del Sr. Heidar Ali Balouji, Primer Consejero, Misión Permanente de la República Islámica de Irán ante las Naciones Unidas, 31 de marzo de 2022, pág. 1, https://documents.unoda.org/wp-content/uploads/2022/03/4-CBMs.pdf
[48] UN Web TV, (1.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (comienza en 5:53)

central que desempeñan las entidades no gubernamentales en la gestión de muchos recursos de las TIC".[49]

Unión Europea: "La lista incluye también elementos controvertidos. En primer lugar, la propuesta de acordar la terminología y la lista de infraestructura crítica es un ejemplo de propuesta que, según nuestra experiencia, no permitiría un debate consensuado entre los Estados. Según la experiencia adquirida en anteriores contextos multilaterales y regionales, estos debates se consideran divisivos, lentos y podrían sugerir, en el caso de la lista de infraestructura crítica, que se trata de objetivos aceptables".[50]

China: "En efecto, en lo que respecta a la tendencia del entorno de las TIC a tornarse cada vez más dividido, creo que otros colegas aquí presentes son conscientes de esta tendencia y realidad. El Secretario General de las Naciones Unidas, Guterres, en dos debates generales sucesivos de la Asamblea General de las Naciones Unidas, ha recordado a la comunidad internacional la amenaza de una creciente fragmentación del entorno de las TIC y el ciberespacio. Por lo tanto, la fragmentación del entorno de las TIC tiene directa relación con nuestras deliberaciones. Consecuentemente, si este mundo se divide o fragmenta en diferentes partes, entonces no se aplicaría un único conjunto de normas. Ergo nos resultaría imposible llegar a un consenso sobre la implementación o aplicabilidad de las normas internacionales. Por no hablar de las medidas de fomento de la confianza. Así que espero que, en la parte de amenazas existentes y potenciales, incluyamos algunas deliberaciones sobre cómo abordar el problema más importante, más prominente en el entorno de las TIC en este momento".[51]

España: **"**En cuanto a las ciberamenazas, proponemos que el informe las describa reflejando los problemas existentes en el ciberespacio y los problemas que implican para el funcionamiento de la sociedad digital, los ciudadanos particulares y el funcionamiento de las instituciones estatales a través de la técnica y el establecimiento de normas. Se debe asegurar la protección efectiva de los datos personales así como la propiedad intelectual en los intercambios transfronterizos e internacionales. En Europa, tenemos un Reglamento General de Protección de Datos que establece altos niveles de estabilidad y seguridad en el intercambio de datos. Cuanto más seguras sean estas garantías de protección, mayor será la protección y la disposición de los ciudadanos y las empresas para intercambiar datos".[52]

Brasil: "Por último, en cuanto a las interfaces, en el informe hay una interrelación con el tema de la gobernanza de Internet cuando hablamos de los riesgos de fragmentación y de garantizar la disponibilidad y la integridad: celebramos la consideración de esta inquietud en el informe,

[49] UN Web TV, (1.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (comienza en 7:54)
[50] UN Web TV, (1.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (comienza en 2:07:34)
[51] UN Web TV, (1.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (comienza en 2:26:14)
[52] UN Web TV, (1.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1u/k1uo46thhm (comienza en 2:41:52)

pero nos gustaría ser conscientes del espacio propicio para debatir cuestiones más generales sobre la gobernanza de Internet".[53]

Federación Rusa: “Es fundamental reflejar en la versión preliminar inicial del informe las medidas sobre accesibilidad de funcionamiento seguro y estable de Internet con el énfasis en la soberanía de los Estados en su respectivo espacio nacional de información. Y asegurar la participación igualitaria de los Estados en la gestión de esta red".[54]

Contexto: La participación de los Estados en la gobernanza de Internet es una cuestión que se ha debatido y resuelto durante la CMSI. La Internet mundial consiste en miles de redes conectadas que son propiedad y están gestionadas de forma independiente, algunas de ellas por gobiernos. No hay pruebas de que los estados no tengan derecho a "participar en igualdad de condiciones... en la gestión de esta red".

Federación Rusa: "En cuanto al fortalecimiento de la interacción con sujetos no gubernamentales en el negocio de la seguridad de las TIC, vemos una ventaja en escuchar la opinión de aquellas partes interesadas que tienen responsabilidad directa en la defensa del objeto de la infraestructura crítica, incluida la Infraestructura crítica de información, siendo sus protagonistas. Dicho diálogo debería tener lugar teniendo en cuenta la función clave de los gobiernos nacionales en esta cuestión".[55]

Camerún: "Creemos que es importante apoyar a los Estados en toda su capacidad para cubrir las brechas, así como para abordar los problemas con las direcciones IP".[56]

Países Bajos: "Agradecemos la referencia a la disponibilidad general y la integridad de Internet. Como punto editorial, solicitaría que este concepto se reflejara en consonancia con los informes del OEWG y el GGE de 2021. En estos informes, se hace referencia al concepto como: "la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet".[57]

27 de julio de 2022

Pakistán: "Pakistán apoyó firmemente la idea de las CBM y recomendó además medidas que insten a aumentar la cooperación entre los respectivos CERTS de los estados miembros que

[53] UN Web TV, (2.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1a/k1a978izhq (comienza en 7:52) y también aquí: Comentarios de la delegación de Brasil sobre el informe preliminar de progreso (secciones: introducción, amenazas, normas), 27 de julio de 2022, pág. 2, https://documents.unoda.org/wp-content/uploads/2022/07/Brazil-part-1.pdf

[54] UN Web TV, (2.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1a/k1a978izhq (comienza en 27:10)

[55] UN Web TV, (2.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1a/k1a978izhq (comienza en 27:45)

[56] UN Web TV, (2.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1a/k1a978izhq (comienza en 43:42)

[57] UN Web TV, (2.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 25 de julio de 2022, https://media.un.org/en/asset/k1a/k1a978izhq (comienza en 1:31:53)

se ocupan de la investigación o las solicitudes correspondientes de los protocolos de Internet y de resolver los impedimentos técnicos en el ámbito de la ciberatribución".[58]

Primer Informe Anual sobre el Progreso Logrado del Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021–2025

El primer informe anual sobre el progreso logrado del OEWG resumió las opiniones, los debates y las propuestas que se plantearon en la sesión del OEWG en 2021-2022. En este sentido, sirvió como documento de consenso para allanar el camino hacia los debates de 2023.[59]

8 de agosto de 2022

El Primer Informe sobre el Progreso Logrado del OEWG: "Preocupa especialmente la actividad maliciosa de las TIC que afecte a la infraestructura crítica de información, las infraestructuras que prestan servicios esenciales al público, las infraestructuras técnicas esenciales para la disponibilidad general o la integridad de Internet y las entidades del sector de la salud".

Contexto: La redacción anterior se extrajo del informe del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2021.[60]

Primer Informe sobre el Progreso Logrado del OEWG: “Los Estados podrían reforzar la coordinación y la cooperación entre los Estados y las partes interesadas, incluidas las empresas, las organizaciones no gubernamentales y el sector académico. Los Estados señalaron que las partes interesadas ya están desempeñando un papel importante a través de asociaciones con los Estados con fines de capacitación, investigación y facilitación del acceso a Internet y los servicios digitales".[61] [62]

---

[58] UN Web TV, (5.ª reunión) Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Tercera sesión sustantiva, 27 de julio de 2022, https://media.un.org/en/asset/k10/k100qzajqy (comienza en 8:35)

[59] Informe del Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Informes finales, 22 de agosto de 2022, https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports

[60] Informe del GGE de 2021, A/76/135, resolución consensuada de la AG 76/19, 14 de julio de 2021, párrafo 10, https://documents.un.org/prod/ods.nsf/xpSearchResultsM.xsp

[61] Primer Informe Anual sobre el Progreso Logrado del Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021–2025, 8 de agosto de 2022, pág. 13, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/454/03/PDF/N2245403.pdf?OpenElement

[62] Representantes de la Federación Rusa y Ucrania bloquearon la participación de algunas entidades no gubernamentales en el trabajo del OEWG. Un total de 32 organizaciones fueron excluidas de la lista de acreditación# propuesta para las sesiones del OEWG porque los Estados miembros habían llegado antes a un consenso sobre las modalidades de participación de las entidades no gubernamentales. El consenso indicaba específicamente que las entidades no acreditadas por el Consejo Económico y Social de las Naciones Unidas (ECOSOC) podrán participar en los trabajos del OEWG con arreglo al principio de no objeción. Ucrania se opuso a la participación de cinco organizaciones de Rusia. Rusia se opuso a la participación de 10 organizaciones de EE. UU.,

Consultas informales

El Presidente del OEWG convocó varias consultas informales en el período entre sesiones. Las citas que figuran a continuación se han extraído del material publicado en el sitio web del OEWG.

El 7 de diciembre de 2022, Rusia presentó la siguiente declaración en las consultas informales del OEWG: "En la fase actual de desarrollo de las TIC, no es posible identificar de forma confiable e inequívoca el origen de una actividad maliciosa sin reformar a fondo los protocolos de la red mundial de comunicaciones y organizar la necesaria cooperación entre estados. Teniendo esto en cuenta, se hace especialmente necesario el establecimiento de mecanismos claros de interacción entre los organismos estatales competentes".[63]

Contexto: La Federación Rusa no ha aportado pruebas de que sea necesario "reformar en profundidad los protocolos" de Internet para lograr el objetivo descrito. Los protocolos comunes de Internet, como el Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP), permiten las comunicaciones entre dispositivos. El Grupo de Trabajo en Ingeniería de Internet (IETF) es responsable del conjunto TCP/IP. Cualquier cambio en el conjunto TCP/IP es gestionado por el IETF, que está abierto a todo aquel al que le interese participar.

En la misma presentación, Rusia agregó: “No existen normas universalmente reconocidas en el ámbito de la lucha contra el uso de las TIC con fines terroristas y delictivos, la represión de la difusión de contenidos ilegales y falsificaciones y la internacionalización de la gobernanza de Internet".[64]

Contexto: Existen documentos universalmente reconocidos, ya mencionados: la Agenda de Túnez de la CMSI y el Documento de Resultados de la CMSI+10, que explican y afirman el modelo multisectorial de gobernanza de Internet como resultado de un esfuerzo verdaderamente internacional.

Cuarta sesión sustantiva[65]

El 7 de marzo de 2023, Singapur expresó lo siguiente: “También recordamos las propuestas del anexo del resumen del Presidente sobre la protección de la infraestructura técnica esencial para la disponibilidad general o la integridad de Internet. Dicha infraestructura técnica sugiere que el DNS (Sistema de Nombres de Dominio) o los puntos de intercambio de Internet son

cuatro organizaciones del Reino Unido, tres organizaciones internacionales, dos organizaciones de Alemania y una organización, respectivamente, de Australia, Finlandia, Francia, Irlanda, Nigeria, España, Suiza y Uganda.

[63] Declaración del representante de la Federación Rusa en la reunión informal entre sesiones del Grupo de Trabajo de Composición Abierta sobre la Seguridad de las TIC y de su Uso 2021-2025, Nueva York, 7 de diciembre de 2022, pág. 1, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf

[64] Declaración del representante de la Federación Rusa en la reunión informal entre sesiones del Grupo de Trabajo de Composición Abierta sobre la Seguridad de las TIC y de su Uso 2021-2025, Nueva York, 7 de diciembre de 2022, pág. 2, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf

[65] Algunas de las declaraciones durante la cuarta sesión sustantiva del OEWG contenían citas repetitivas que ya se han citado en nuestro informe de actualización.

importantes tanto para los Estados desarrollados como para los que están en vías de desarrollo, dada la creciente dependencia de todos los Estados en las tecnologías basadas en las TIC. Estamos a favor de continuar el debate en el seno del OEWG sobre las posibles medidas que puedan adoptarse para garantizar la disponibilidad o la integridad de Internet".[66]

Quinta sesión sustantiva

El 27 de julio de 2023, Portugal habló, entre otras cosas, de los cuatro puntos que no se incluyeron en el informe anual del OEWG: "…3. La reafirmación de que los servicios esenciales y la infraestructura crítica deberían estar siempre fuera de los límites de la actividad cibernética maliciosa, 4. El reconocimiento de la función esencial de todas las partes interesadas, incluida la plataforma tecnológica, en todos los pilares del marco, concretamente en ... la protección de la infraestructura crítica..."[67]

El 28 de julio de 2023, Rusia citó la declaración de la cumbre Rusia-África sobre las TIC[68] y realizó la siguiente afirmación: "Tomamos nota de la necesidad de reforzar la coordinación entre la Federación Rusa y los Estados africanos en las organizaciones internacionales del sistema de las Naciones Unidas en lo que respecta a los servicios postales y la UIT. En particular, en lo que respecta a la elaboración de documentos para el desarrollo de las TIC. Nos guiamos por el hecho de que debe desarrollarse el Programa de Túnez para la Sociedad de la Información. Fue adoptado en 2005 en el Foro de la CMSI. Apoyamos la creación de un sistema internacional equilibrado para gestionar Internet bajo los auspicios de las Naciones Unidas, a fin de evitar cualquier limitación política unilateral o interés comercial y garantizar la seguridad y estabilidad de la infraestructura crítica de la información de la red mundial".[69]

Contexto: No hay pruebas de que se haya producido alguna limitación que amenace la "seguridad y estabilidad de la infraestructura crítica de la información de la red mundial". Además, no hay pruebas de que el sistema internacional existente para gestionar Internet no sea equilibrado, o necesite pasar a estar bajo los auspicios de alguna organización intergubernamental, incluida Naciones Unidas. De hecho, la Federación Rusa participa en ese mismo sistema como miembro del Comité Asesor Gubernamental de la ICANN.[70]

El 28 de julio de 2023, el OEWG adoptó el 2.º informe preliminar anual sobre el progreso logrado.[71] El informe contiene el siguiente texto:

---

[66] UN Web TV, (3.ª reunión) Grupo de Trabajo de Composición Abierta sobre Tecnologías de la Información y la Comunicación (TIC) - Cuarta sesión sustantiva, 7 de marzo de 2023, (comienza en 2:11:30), https://media.un.org/en/asset/k1a/k1ah2cv3gr

[67] UN Web TV, (8.ª reunión) Grupo de Trabajo de Composición Abierta sobre Tecnologías de la Información y la Comunicación (TIC) - Quinta sesión sustantiva, 27 de julio de 2023, (comienza en 2:11:52), https://media.un.org/en/asset/k1n/k1ngmoogyi

[68] Declaración de la Segunda Cumbre Rusia-África sobre Cooperación en el Ámbito de la Seguridad de la Información Internacional, 28 de julio de 2023, apartado 7, http://en.kremlin.ru/supplement/5975

[69] UN Web TV, (10.ª reunión) Grupo de Trabajo de Composición Abierta sobre Tecnologías de la Información y la Comunicación (TIC) - Quinta sesión sustantiva, 28 de julio de 2023, (comienza en 11:00), https://media.un.org/en/asset/k1s/k1san5j55u

[70] ICANN | GAC, Comité Asesor Gubernamental, https://gac.icann.org/

[71] Informe del Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025, Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025, informes finales, 1 de agosto de 2023, https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports

“Los Estados también resaltaron que las actividades maliciosas de las TIC contra la infraestructura crítica y la infraestructura crítica de información que socavan la confianza en los procesos políticos y electorales, las instituciones públicas, o que afectan a la disponibilidad general o a la integridad de Internet, son también una preocupación real y creciente. Los Estados expresaron su especial preocupación por las actividades maliciosas relacionadas con las TIC cuyo objetivo es interferir en los asuntos internos de los Estados”.[72]

"Los Estados subrayaron la importancia de la protección de la Infraestructura Crítica (CI) y de la Infraestructura Crítica de Información (CII). Los Estados destacaron que la actividad de las TIC que daña intencionadamente la CI o CII o que perjudica, de otro modo, el uso y el funcionamiento de la CI o CII para la prestación de servicios al público puede tener efectos en cascada a nivel nacional, regional y mundial. Plantea un elevado riesgo de daño a la población y puede ser un proceso de escalada. Por lo tanto, los Estados subrayaron la necesidad de seguir reforzando las medidas para proteger todas las CI y CII frente a las amenazas relacionadas con las TIC y propusieron incrementar los intercambios de prácticas recomendadas en materia de protección de la CI y CII, lo que incluye el intercambio de políticas nacionales, y de recuperación tras incidentes de TIC que afecten la CI y CII. En este sentido, los Estados recordaron la Resolución 58/199 de la Asamblea General sobre la "creación de una cultura mundial de ciberseguridad y protección de la infraestructura crítica de información" y el anexo que la acompaña. Los Estados también propusieron apoyar a los países en desarrollo y a los Estados pequeños, en su identificación de CI y CII nacionales, cuando así lo soliciten".[73]

El Informe Anual sobre el Progreso Logrado también contiene la siguiente recomendación: "En las sesiones sexta, séptima y octava del OEWG, los Estados también deberán llevar a cabo debates centrados en: (a) el fortalecimiento de las medidas para proteger la CI y CII de las amenazas relacionadas con las TIC, lo que incluye los intercambios sobre prácticas recomendadas para detectar, defenderse o responder y recuperarse de los incidentes con relación a las TIC, y para apoyar a los países en desarrollo y a los Estados pequeños en su identificación de las CI y CII nacionales, cuando se solicite; y (b) una mayor cooperación y asistencia para garantizar la integridad de la cadena de suministro y evitar el uso de funciones ocultas perjudiciales".[74]

[72] Grupo de Trabajo de Composición Abierta sobre la Seguridad de las Tecnologías de la Información y la Comunicación y en su Uso 2021-2025. Quinta sesión sustantiva, Nueva York del 24 al 28 de julio de 2023. Segundo Informe Anual sobre el Progreso Logrado, pág. 6, https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/227/59/PDF/N2322759.pdf?OpenElement

[73] Ibidem, pág. 8

[74] Ibidem, pág. 9

Comité Ad Hoc de las Naciones Unidas para la Elaboración de un Convenio Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos (AHC)[75]

Primera sesión (presentaciones relacionadas con la primera sesión del AHC)[76]

29 de junio de 2021

Federación Rusa: "Por 'Infraestructura crítica de información' se entenderá un conjunto de instalaciones de infraestructura crítica de información y redes de telecomunicaciones utilizadas para interconectar instalaciones de infraestructura crítica de información; n) El término 'instalaciones de infraestructura crítica' significará los sistemas de información y las redes de información y comunicaciones de las autoridades públicas y sistemas de información y sistemas automatizados de control de procesos que operan en los sectores de defensa, sanidad, educación, transporte, comunicaciones, energía, banca y finanzas, nuclear y otros ámbitos importantes de la vida del Estado y de la sociedad".[77]

8 de noviembre de 2021

Interpol: “El acceso a la información crítica de registración de nombres de dominio (datos de WHOIS) es limitado para los organismos encargados del cumplimiento de la ley en el entorno normativo actual. Para ayudar a los organismos encargados del cumplimiento de la ley de todo el mundo a afrontar este desafío fundamental, INTERPOL ha diseñado y puesto en marcha la prueba piloto de un nuevo portal restringido que proporciona acceso automatizado a la información sobre la registración de dominios a entidades encargadas del cumplimiento de la ley debidamente autorizadas. Una vez concluida con éxito la fase piloto del sistema, INTERPOL está integrando esta solución en sus capacidades policiales a escala mundial con

[75] Este capítulo contiene citas de las 6 sesiones del AHC, y su estructura tiene el objetivo de ilustrar las contribuciones efectuadas durante las sesiones primera y segunda. Las citas de la tercera sesión también incluyen debates grabados que tuvieron lugar en el pleno del AHC. Las sesiones cuarta y quinta dieron lugar a la publicación del texto preliminar, que se tituló "documento consolidado de negociación", y en la sexta sesión se redactó el "texto preliminar del convenio". Este capítulo incluye citas relevantes de estos documentos. Consultar aquí: Comité Ad Hoc para la Elaboración de un Convenio Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, Reuniones del Comité Ad Hoc: Sesiones, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[76] Primera sesión del Comité Ad Hoc, Nueva York, del 28 de febrero al 11 de marzo de 2022, Presentaciones de Estados miembros relacionadas con la primera sesión del Comité Ad Hoc, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html

[77] Convenio de las Naciones Unidas sobre la Lucha contra la Utilización de las Tecnologías de la Información y la Comunicación con Fines Delictivos. Versión preliminar, traducción no oficial, Documento presentado por la Federación Rusa relativo a la primera sesión del Comité Ad Hoc, 29 de junio de 2021, pág. 6, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf

los acuerdos jurídicos necesarios para ampliar el grupo de operadores privados participantes y abrir el sistema a los países miembros".[78]

Segunda sesión (presentaciones relacionadas con la segunda sesión del AHC)[79]

7 de abril de 2022

Federación Rusa (en nombre de Bielorrusia, Burundi, China, Nicaragua y Tayikistán): “Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para ordenar: [...] (b) A un proveedor de servicios que ofrezca sus servicios en el territorio de ese Estado parte que presente la información sobre los suscriptores que esté en posesión o bajo el control de ese proveedor de servicios”. [...] "A los efectos del presente artículo, se entenderá por "información sobre los suscriptores" toda información que obre en poder de un proveedor de servicios relativa a los suscriptores a sus servicios, distinta de los datos sobre tráfico o sobre contenidos, a partir de la cual sea posible establecer: "b) La identidad del suscriptor, las direcciones postales o de otro tipo, los números de teléfono y otros números de acceso, incluidas las direcciones IP y la información de facturación y pago, disponibles en el contrato o acuerdo de servicio; c) La información relativa a la ubicación de los equipos de información y telecomunicaciones que tenga relación con el contrato o acuerdo de servicio".[80]

8 de abril de 2022

Brasil: “i) ‘Datos del suscriptor’ significa cualquier dato informático, recopilado en el curso normal de la actividad de un proveedor de servicios, relativo al nombre, fecha de nacimiento, dirección postal o geográfica, datos de facturación y pago, identificadores del dispositivo, número de teléfono o dirección de correo electrónico, o cualquier otra información, como la dirección IP utilizada en el momento en que se creó una cuenta, que pueda servir para identificar al abonado o cliente, así como el tipo de servicio prestado y la duración del contrato con el proveedor de servicios, que no sean datos de tráfico o de contenido".[81]

República Islámica de Irán: “el convenio debe especificar y estipular obligaciones y regulaciones en cuanto a la cooperación del sector privado, proveedores de servicios y otras

[78] Contribución de INTERPOL a la Elaboración de un Convenio Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos. Documento presentado por Interpol relativo a la primera sesión del Comité Ad Hoc, 8 de noviembre de 2021, pág. 6, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf

[79] Segunda sesión del Comité Ad Hoc, Viena, del 30 de mayo al 10 de junio de 2022, Presentaciones relacionadas con la segunda sesión del Comité Ad Hoc, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html

[80] Documento presentado por la Federación Rusa también en nombre de Bielorrusia, Burundi, China, Nicaragua y Tayikistán relativo a la segunda sesión del Comité Ad Hoc, 7 de abril de 2022, pág. 13, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_E.pdf

[81] Propuesta de Brasil sobre los capítulos iniciales de un convenio sobre ciberdelitos de las Naciones Unidas, documento presentado por Brasil relativo a la segunda sesión del Comité Ad Hoc, 8 de abril de 2022, pág. 2, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Brazil_Contribution_E.pdf

entidades similares con los organismos encargados del cumplimiento de la ley, en particular los sectores y proveedores con alcance mundial o significativo a nivel internacional".[82]

Japón: "La ciberseguridad y la gobernanza de Internet no deberían abordarse en este convenio. Por ejemplo, las siguientes medidas tendrían un efecto paralizador sobre la actividad económica legítima e impedirían el desarrollo de la tecnología, e irían más allá del mandato del Comité Ad Hoc:

- establecer normas de seguridad en el marco de este convenio;
- imponer a las personas jurídicas y físicas la obligación de cumplir dichas normas o imponer sanciones por la infracción de las mismas; o
- responsabilizar a las personas jurídicas, a sus representantes o a los creadores de software que involuntariamente hayan participado en ciberdelitos cometidos por otros actores sin ser conscientes de ello".[83]

9 de abril de 2022

Canadá: Sugirió definir "datos informáticos" como "cualquier representación de hechos, información o conceptos en una forma adecuada para su procesamiento en un sistema informático, incluido un programa adecuado para hacer que un sistema informático realice una función". Esta definición incluiría todo tipo de datos: datos de contenido (el mensaje propiamente dicho), programas informáticos, datos de tráfico, información sobre suscriptores, contraseñas y códigos de conexión. Según la misma contribución, por "datos de tráfico" se entenderá "cualquier dato informático para identificar, activar o configurar un dispositivo relativo a la creación, transmisión o recepción de una comunicación por medio de un sistema informático, generado por un sistema informático que forme parte de la cadena de comunicación, que indique el origen, destino o finalización de la comunicación, la ruta, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente". Esta definición incluye, tanto para los servicios de telefonía como para los de Internet, los datos necesarios para la marcación, el enrutamiento y el direccionamiento o la señalización, por ejemplo: números de teléfono, fecha y hora de una llamada (y otros elementos de los registros de datos de llamadas), el origen y el destino de los mensajes (como el origen, destino o finalización de la comunicación, la ruta, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente, correo electrónico o mensajes de texto), así como las direcciones IP y los datos relativos al protocolo utilizado".[84]

12 de abril de 2022

Vietnam: Sugirió definir el Ciberespacio como "una red de infraestructura de tecnología de la información (TI) que incluye redes de telecomunicaciones, Internet, redes informáticas,

---

[82] Documento presentado por la República Islámica de Irán relativo a la segunda sesión del Comité Ad Hoc, 8 de abril de 2022, pág. 4, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Islamic_Republic_of_Iran_contribution.pdf

[83] Japón, Contribución sobre Criminalización, Disposiciones Generales, y Medidas Procesales y Cumplimiento de la Ley, Documento presentado por Japón relativo a la segunda sesión del Comité Ad Hoc, 8 de abril de 2022, págs. 5 y 6, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Japan_Contribution.pdf

[84] Canadá, Documento presentado del texto preliminar y contribuciones sobre los capítulos y disposiciones específicos que se examinarán durante la segunda sesión del Comité Ad Hoc, a saber, sobre criminalización, disposiciones generales y medidas procesales y cumplimiento de la ley, 9 de abril de 2022, pág. 1, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Canada_Contribution.pdf

sistemas de comunicación, sistemas de procesamiento y control de la información, bases de datos".[85]

13 de abril de 2022
México: “México considera que deben agregarse otras disposiciones de carácter general sobre los siguientes temas: [...] el reconocimiento del núcleo público de Internet y la relevancia del enfoque de neutralidad de la red para los propósitos del convenio".[86]

14 de abril de 2022:
Sudáfrica: "Cada Estado parte mantendrá un registro con información identificable de todos los registradores de nombres de dominio, criptoactivos y comerciantes de criptoactivos dentro de su jurisdicción, de conformidad con los principios fundamentales de su derecho interno, y proporcionará dicha información a las autoridades competentes con fines de investigación y probatorios".[87]

Tercera sesión (presentaciones relacionadas con la tercera sesión del AHC)[88]

29 de agosto de 2022

República Islámica de Irán: “Las entidades privadas, como los proveedores de servicios, incluso en el ámbito de los nombres de dominio, tienen una función especialmente importante en la lucha contra los delitos cometidos mediante la utilización de las TIC. Habida cuenta del rampante uso indebido con intención delictiva de los servicios prestados, sigue siendo vital la cooperación de dichas entidades con los organismos encargados del cumplimiento de la ley y su verificación de antecedentes en este ámbito, especialmente las entidades con un alcance y actividades significativos a nivel internacional. En este sentido, el Convenio debería establecer normas y obligaciones en materia de cooperación efectiva de estas entidades con los organismos encargados del cumplimiento de la ley. Asimismo, dichas entidades deberían respetar las especificidades económicas, sociales, jurídicas y culturales de los Estados".[89]

China: "Los Estados no podrán, en infracción de las leyes del Estado donde se almacenan los datos, recopilar directamente los datos almacenados en estados extranjeros, de empresas o

[85] Documento presentado por Vietnam para la segunda sesión del Comité Ad Hoc, 12 de abril de 2022, pág. 1, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Vietnam_Contribution.pdf
[86] Contribución del Gobierno de México para consideración del Comité Ad Hoc en su segunda sesión sustantiva, 13 de abril de 2022, pág. 3, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Mexico_Contribution.pdf
[87] Contribución de Sudáfrica sobre las disposiciones relativas a la criminalización, disposiciones generales y medidas procesales y cumplimiento de la ley, 14 de abril de 2022, pág. 13, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/South_Africas_contribution.pdf
[88] Tercera sesión del Comité Ad Hoc del 29 de agosto al 9 de septiembre de 2022, Nueva York, Presentaciones relacionadas con la tercera sesión del Comité Ad Hoc, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_third_session/main.html
[89] UN Web TV, (1.ª reunión) Tercera sesión. Comité Ad Hoc para Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, 29 de agosto de 2022, (comienza en 1:08:56), https://media.un.org/en/asset/k1x/k1xh926qrt

individuos o por medios técnicos pasando por alto las medidas de protección de seguridad de la red".[90]

Canadá: "Aunque Canadá no se opone a la inclusión del artículo 32 del Convenio de Budapest, opinamos que podría ser difícil llegar a un consenso sobre un artículo de este tipo, dados los ajustados plazos con los que trabajamos para este Convenio y dado que dicho artículo fue el resultado de largos debates".[91]

Contexto: El Artículo 32 del Convenio de Budapest sobre la Ciberdelincuencia, en relación con el acceso transfronterizo a datos informáticos almacenados con consentimiento o cuando estén disponibles de forma pública, establece lo siguiente:

"Una Parte podrá, sin la autorización de otra Parte:

a. acceder a datos informáticos almacenados disponibles públicamente (fuente abierta), con independencia del lugar geográfico en que se encuentren los datos; o

acceder o recibir, a través de un sistema informático en su territorio, datos informáticos almacenados ubicados en otra Parte, si la Parte obtuviere el consentimiento legal y voluntario de la persona que tiene la autoridad legal para revelar los datos a la Parte mediante ese sistema informático".[92]

Chile: "No obstante, además de pruebas, son necesarias pruebas que sean concluyentes para cualquier delito y eso incluye Internet, o todo otro procedimiento conectado a la red, o que pueda utilizarse para probar o no el delito".[93]

1 de septiembre de 2022

Ecuador: "Ecuador, en este sentido, ha identificado varias necesidades. Serían demasiadas para citarlas todas en este momento, pero, a modo de ejemplo, puedo mencionar los problemas actuales con los ISP, los proveedores de servicios de Internet, dado que no quieren tener direcciones IPv4 y han tenido que utilizar protocolos como el CGNET que hace posible que miles de usuarios utilicen la misma dirección IP pública. Esto dificulta la identificación del autor del ciberdelito. Y en este sentido, solicitamos que el futuro Convenio incluya una disposición que obligue a los Estados parte a organizar sus normas internas para solicitar a los ISP que, en un plazo razonable, migren totalmente de IPv4 a IPv6. Esto permitiría tener

[90] UN Web TV, (1.ª reunión) Tercera sesión. Comité Ad Hoc para Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, 29 de agosto de 2022, (comienza en 02:13:22), https://media.un.org/en/asset/k1x/k1xh926qrt
[91] UN Web TV, (2.ª reunión) Tercera sesión. Comité Ad Hoc para Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, 29 de agosto de 2022, (comienza en 1:43:42), https://media.un.org/en/asset/k1j/k1jbh2v1z7
[92] Consejo de Europa, Serie de Tratados Europeos - N.º 185, Convenio sobre Ciberdelincuencia, Budapest, 23 de noviembre de 2001, pág. 17, https://rm.coe.int/1680081561
[93] UN Web TV, (2.ª reunión) Tercera sesión. Comité Ad Hoc para Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, 29 de agosto de 2022, (comienza en 2:37:05), https://media.un.org/en/asset/k1j/k1jbh2v1z7

resultados favorables en la investigación de los ciberdelitos y, por lo tanto, sería posible cumplir con los requisitos de asistencia técnica en este campo".[94]

El Presidente comentó esta cuestión: “Vemos con ustedes que existen varias discrepancias con las direcciones IP y esto... nos da mucho margen para avanzar, y nos permite ver que hay grandes diferencias a nivel de entendimiento técnico".[95]

Omán: "Me sumo a la declaración del representante de Ecuador sobre la importancia de intercambiar mecanismos de trabajo y pasar del 4.º protocolo al 6.º protocolo. Esto tendría un impacto positivo [...] en la lucha contra el ciberdelito. Cuando las empresas o los proveedores de servicios cambien el protocolo con el que trabajan, me refiero al 6.º protocolo, esto tendría un impacto mucho mayor en términos de lucha contra el ciberdelito".[96]

7 de septiembre de 2022

Pakistán: "Pakistán siempre ha apoyado la idea de las CBM y propone además la siguiente acción recomendada que insta a aumentar la cooperación entre los respectivos Equipos de Respuesta ante Emergencias Informáticas (CERT) de los Estados miembros para abordar las solicitudes de investigación / rastreo de Protocolos de Internet y resolver los impedimentos técnicos en el camino de la ciberatribución".[97]

Rusia: "La Federación Rusa sugirió la adición de los siguientes párrafos al documento (informe): [...] Los Estados señalan la importancia de adoptar medidas para proteger la disponibilidad general y el funcionamiento seguro y estable de Internet teniendo en cuenta la soberanía de los Estados en su espacio de información, así como para garantizar la participación equitativa de los Estados en la gobernanza de esta red".[98]

Contexto: Al igual que en las intervenciones ante el OEWG, Rusia no aporta pruebas de que exista una participación desigual de los Estados en la gobernanza de Internet. Como ya se ha explicado, la Federación Rusa es miembro del GAC en la ICANN y, como tal, participa en pie de igualdad con todos los demás miembros del GAC en los trabajos de la ICANN.

---

[94] UN Web TV, (8.ª reunión) Tercera sesión. Comité Ad Hoc para Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, 1 de septiembre de 2022, (comienza en 1:54:12), https://media.un.org/en/asset/k1o/k1o39wyquf

[95] UN Web TV, (8.ª reunión) Tercera sesión. Comité Ad Hoc para Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, 1 de septiembre de 2022, (comienza en 1:58:09), https://media.un.org/en/asset/k1o/k1o39wyquf

[96] UN Web TV, (8.ª reunión) Tercera sesión. Comité Ad Hoc para Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, 1 de septiembre de 2022, (comienza en 2:06:20), https://media.un.org/en/asset/k1o/k1o39wyquf

[97] Compendio de declaraciones en explicación de posición sobre la adopción del Informe sobre el Progreso Logrado del Grupo de Trabajo de Composición Abierta contenido en A/77/275, anexo, 7 de septiembre de 2022, pág. 26, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/compendium_2022.pdf

[98] Compendio de declaraciones en explicación de posición sobre la adopción del Informe sobre el Progreso Logrado del Grupo de Trabajo de Composición Abierta contenido en A/77/275, anexo, 7 de septiembre de 2022, pág. 37, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/compendium_2022.pdf

Sesiones cuarta[99] y quinta[100] del AHC

Documento de negociación consolidado del AHC:

El documento de negociación consolidado con el estado “al 21 de abril de 2023” se publicó tras la quinta sesión del AHC. El documento de negociación contenía el texto preliminar del Convenio sobre Ciberdelito de las Naciones Unidas elaborado por el Presidente del Comité Ad Hoc. No todas las sugerencias fueron aceptadas por las delegaciones y se hicieron más adiciones al texto del convenio preliminar. No obstante, citamos aquí el texto por su relevancia.

21 de abril de 2023

Documento de negociación consolidado:

India, Pakistán, EE. UU., China, Nueva Zelanda, Egipto, Kenia, Sudán, Australia, Rusia, Colombia, Noruega, Canadá, Tanzania, República Árabe Siria, Argelia, Burkina Faso, Singapur, Sudáfrica, Nicaragua, Macao, Tonga, la Unión Europea y los Estados miembros, y Fiyi declararon que quieren suprimir la versión preliminar del artículo 72 sobre "acceso transfronterizo a [datos informáticos] [información electrónica/digital] almacenados con consentimiento o cuando estén a disposición del público" del documento de negociación consolidado sobre el preámbulo, las disposiciones relativas a la cooperación internacional, las medidas preventivas, la asistencia técnica y el mecanismo de aplicación, y las disposiciones finales de un convenio internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Dos países, Ecuador y Venezuela, se mostraron a favor de mantener el texto de este artículo tras las modificaciones.[101] El texto completo del artículo es el siguiente:

“Un Estado parte podrá, sin la autorización de otro Estado parte:
(a) Acceder a [datos informáticos] [información electrónica/digital] almacenados de acceso público (fuente abierta), independientemente del lugar geográfico en que se encuentren [los datos] [la información]; o
(b) Acceder o recibir, a través de [un sistema informático] [un sistema/dispositivo de tecnología de la información y las comunicaciones] en su territorio, [datos informáticos] [información electrónica/digital] almacenados ubicados en otro Estado parte, si el Estado parte que accede o recibe los [datos] [la información] obtiene el consentimiento legal y voluntario de la persona que tiene la autoridad legal para divulgar los [datos] [la información] a ese Estado parte a través de ese sistema informático".[102]

---

[99] Este capítulo no contiene ninguna cita de la cuarta sesión del Comité Ad Hoc. Consultar, a modo de referencia, la cuarta sesión del Comité Ad Hoc, del 9 al 20 de enero de 2023, Viena, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html

[100] Quinta sesión del Comité Ad Hoc, del 11 al 21 de abril de 2023, Viena, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main

[101] Comité Ad Hoc encargado de elaborar un Convenio Internacional Integral Contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, quinta sesión del 11 al 21 de abril de 2023. Documento de negociación consolidado sobre el preámbulo, las disposiciones relativas a la cooperación internacional, las medidas preventivas, la asistencia técnica y el mecanismo de aplicación y las disposiciones finales de un convenio internacional integral contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, pág. 38, 21 de abril de 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf

[102] Ibidem

Malasia, Angola y Namibia optaron por excluir solo la parte "b)" del artículo preliminar.

Comentario: La copia preliminar de seguimiento del proyecto de texto del convenio preparada para la sexta sesión del AHC, no contenía el artículo preliminar "Artículo 72 sobre el acceso transfronterizo a [datos informáticos] [información electrónica/digital] almacenados con consentimiento o cuando estén a disposición del público" análogo al artículo 32 del Convenio de Budapest sobre la Ciberdelincuencia.[103]

Sexta sesión del AHC[104]

Los trabajos durante la sexta sesión del AHC concluyeron el 1 de septiembre de 2023.

Texto preliminar del convenio (versión al 2 de septiembre de 2023)

Durante la sexta sesión del AHC se elaboró el texto de 80 páginas del borrador del convenio sobre ciberdelito. Quisiéramos llamar su atención sobre las siguientes disposiciones de este texto y comentar algunas de ellas.

"Artículo 2: Uso de términos.

[...]

(c) Por "datos de tráfico" se entenderá cualquier [dato informático] [información digital] que recopile un proveedor de servicios, excluidos los datos de contenido, relacionados con: (i) El tipo de servicio prestado y su duración cuando se refieran a datos técnicos y datos identificativos de las medidas técnicas o interfaces conexas utilizadas por el suscriptor o cliente o facilitadas al mismo, y a datos relacionados con la validación del uso del servicio, excluidas las contraseñas u otros medios de autenticación utilizados en lugar de una contraseña, que sean proporcionados por un usuario o creados a solicitud de un usuario; (ii) El inicio y la finalización de una sesión de acceso de un usuario a un servicio, como la fecha y la hora de uso, o de inicio y fin de sesión en el servicio; y (iii) los metadatos de comunicaciones procesados en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar datos de contenido, incluidos los datos utilizados para rastrear e identificar el origen y el destino de una comunicación, los datos sobre la ubicación del equipo terminal utilizado en el contexto de la prestación de servicios de comunicaciones, y la fecha, hora, duración y tipo de la comunicación";[105]

---

[103] Comité Ad Hoc encargado de elaborar un Convenio Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, sexta sesión, 21 de agosto - 1 de septiembre de 2023, Convenio Preliminar (copia anticipada), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf

[104] Sexta sesión del Comité Ad Hoc, 21 de agosto - 1 de septiembre 2023, Nueva York, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main

[105] Comité Ad Hoc encargado de elaborar un Convenio Internacional Integral Contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos. Sexta sesión, 21 de agosto - 1 de septiembre de 2023. Texto preliminar del convenio (Situación al 2 de septiembre de 2023 con actualizaciones de los Estados miembros), pág. 3, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

Comentario: Esto difiere de la definición proporcionada en el Convenio de Budapest sobre la Ciberdelincuencia. Según el Convenio de Budapest: "datos de tráfico" significa cualquier dato informático relativo a una comunicación por medio de un sistema informático, generado por un sistema informático que forme parte de la cadena de comunicación, que indique el origen, el destino, la ruta, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente de la comunicación".[106]

El Convenio de Budapest sobre la Ciberdelincuencia proporciona las mismas definiciones de "proveedor de servicios" e "información del suscriptor",[107] *pero no proporciona la definición de "datos de contenido". La versión preliminar del Convenio de las Naciones Unidas sí la proporciona.*[108]

[...]

República Dominicana agregó la disposición preliminar al "Artículo 2. Uso de términos". Quiere definir quiénes son las "partes interesadas pertinentes"[109].

La Federación Rusa, Irán, Bielorrusia, Burkina Faso, Venezuela y Egipto introdujeron: "Artículo 10 bis. Interferencia ilícita en la infraestructura crítica de información.
1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la creación, distribución y/o utilización intencionales de programas informáticos u otro tipo de información digital concebidos deliberadamente para interferir ilícitamente en la infraestructura crítica de información, incluidos los programas informáticos u otro tipo de información digital para la destrucción, el bloqueo, la modificación, la copia de información contenida en ellos, o para la neutralización de funciones de seguridad. 2. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno la violación de las normas de funcionamiento de los medios diseñados para el almacenamiento, procesamiento y transferencia de información digital protegida contenida en la infraestructura crítica de información o en sistemas de información o redes de información y comunicación que pertenezcan a la infraestructura crítica de información, o la violación de las normas de acceso a los mismos, si dicha violación daña la infraestructura crítica de información".[110]

---

[106] Consejo de Europa, Convenio sobre Ciberdelincuencia, Budapest, 23 de noviembre, pág. 3, https://rm.coe.int/1680081561

[107] Consejo de Europa, Serie de Tratados Europeos - N.º 185, Convenio sobre Ciberdelincuencia, Budapest, 23 de noviembre de 2001, págs. 3 y 9, https://rm.coe.int/1680081561

[108] "(d) Por 'datos de contenido' se entenderá cualquier [dato informático] [información digital] relativo a una comunicación efectuada por medio de un [sistema informático] [dispositivo de tecnología de la información y las comunicaciones] que se refiera al fondo o al propósito de dicha comunicación, como texto, mensajes de voz, grabaciones sonoras, grabaciones de vídeo y otros tipos de información". El Convenio Europeo para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal ofrece la definición de "datos personales", término que tiene una formulación similar en el texto preliminar del convenio de las Naciones Unidas: "Datos personales" se refiere a los datos relacionados con cualquier persona física identificada o identificable." Comité Ad Hoc encargado de elaborar un Convenio Internacional Integral Contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, sexta sesión, 21 de agosto - 1 de septiembre de 2023. Texto preliminar del convenio (Situación al 2 de septiembre de 2023 con actualizaciones de los Estados miembros), págs. 3 y 4, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

[109] Ibidem, pág. 4

[110] Ibidem, pág. 9

Comentario: Australia, Estados Unidos, la UE y sus Estados miembros, Nueva Zelanda, Georgia, Noruega, Reino Unido, Liechtenstein, Canadá, Chile, Japón y México se oponen a la inclusión de este artículo en el convenio y solicitan que se elimine.

China, Irán, la Federación Rusa, Venezuela y Egipto presentaron lo siguiente:
"Artículo 10 ter. Prestación ilícita de servicios.
Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno, cuando se cometan intencionalmente y sin derecho
(a) La prestación de servicios o asistencia técnica, incluidos el acceso a Internet, el alojamiento en servidores, el almacenamiento en línea, la transmisión de comunicaciones o servicios similares; o
(b) La creación de sitios web, redes de comunicación

con la intención de que el servicio o asistencia técnica se utilice para la comisión de cualquiera de los delitos tipificados conforme al presente Convenio".[111]

Comentario: Australia, Estados Unidos, la UE y sus Estados miembros, Nueva Zelanda, Georgia, Noruega, Reino Unido, Liechtenstein, Canadá, Japón y México se oponen a la inclusión de este artículo en el convenio y solicitan que se elimine.

La Federación Rusa, Mali, Bielorrusia, Nicaragua, Burkina Faso, Eritrea, Venezuela, Sudán, Cuba, Nigeria, Burundi, RPDC, Egipto, Turquía y Sierra Leona presentaron lo siguiente:
"Artículo 15 septies. Delitos relacionados con el terrorismo.
Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan por medio de las tecnologías de la información y la comunicación, la comisión de actos de terrorismo, la incitación, el reclutamiento u otra forma de participación en actividades terroristas, la apología y la justificación del terrorismo o la recaudación o el suministro de fondos para su financiación, el adiestramiento para la comisión de actos terroristas, la facilitación de la comunicación entre organizaciones terroristas y sus miembros, incluida la creación, publicación o utilización de un sitio web o la prestación de apoyo logístico a los autores de actos terroristas, la difusión de métodos para la fabricación de explosivos empleados en particular en actos terroristas, y la propagación de la discordia, la sedición, el odio o el racismo".[112]

Comentario: Canadá, Estados Unidos, Nueva Zelanda, República Dominicana, Guatemala, Noruega, Georgia, Australia, la UE y sus Estados miembros, Israel, Reino Unido, Líbano, Liechtenstein, Chile, Japón y México se oponen a la inclusión de este artículo en el convenio y solicitan que se elimine.

Argelia, Canadá y la Federación Rusa propusieron mantener el texto original de:
Artículo 21: Enjuiciamiento, sentencia y sanciones
[...]
"Cada Estado parte podrá adoptar, de conformidad con su derecho interno, las medidas legislativas y de otra índole que sean necesarias para establecer circunstancias agravantes en relación con los delitos tipificados conforme a los artículos 6 a 9 de este Convenio, incluidas las circunstancias que afecten la infraestructura crítica de información".[113]

[111] Ibidem, pág. 9
[112] Ibidem, pág. 19
[113] Ibidem, pág. 25

Comentario: Liechtenstein, Nueva Zelanda, Noruega, Tanzania, Estados Unidos, la UE y sus Estados miembros, Suiza, Nigeria, Israel, Filipinas, Australia, Georgia, Noruega, CARICOM, se oponen a la inclusión de este artículo en el convenio y solicitan que se elimine.

"Artículo 26: Conservación inmediata y divulgación parcial de datos de tráfico
Cada Estado parte adoptará, con respecto a los datos de tráfico que deban conservarse en virtud de lo dispuesto en el artículo sobre la conservación inmediata de [datos informáticos] [información digital] almacenados, las medidas legislativas y de otro tipo que sean necesarias para: [...] (b) Garantizar la divulgación expeditiva a la autoridad competente del Estado parte, o a una persona designada por dicha autoridad, de una cantidad suficiente de datos de tráfico que permita al Estado parte identificar a los proveedores de servicios y la ruta a través de la cual se transmitió la comunicación o la información indicada".[114]

"Artículo 27: Orden de producción de prueba
Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para ordenar: [...] (b) A un proveedor de servicios que ofrezca sus servicios en el territorio del Estado parte que presente la información sobre los suscriptores en relación con dichos servicios que esté en posesión o bajo el control de ese proveedor de servicios".[115]

La Federación Rusa, Argentina, Venezuela, Egipto y Sudáfrica se mostraron a favor de mantener el texto del siguiente artículo:
"Artículo 29: Recopilación de datos de tráfico en tiempo real[116] 1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes para: (a) Recopilar o registrar, mediante la aplicación de medios técnicos en el territorio de ese Estado parte; y (b) Obligar a un proveedor de servicios, dentro de su capacidad técnica existente: (i) Recopilar o registrar, mediante la aplicación de medios técnicos en el territorio de ese Estado parte; o ii) Cooperar y prestar asistencia a las autoridades competentes en la recopilación o registro de datos de tráfico, en tiempo real, asociados a comunicaciones especificadas en su territorio transmitidas por medio de [un sistema informático] [un dispositivo de tecnologías de la información y la comunicación]. 2. Cuando un Estado parte, debido a los principios de su ordenamiento jurídico interno, no pueda adoptar las medidas a que se refiere el literal (a) del apartado 1, podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para garantizar la recopilación o el registro en tiempo real de datos de tráfico asociados a comunicaciones especificadas transmitidas en su territorio, mediante la aplicación de medios técnicos en dicho territorio. 3. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para obligar a un proveedor de servicios a

[114]Comité Ad Hoc encargado de elaborar un Convenio Internacional Integral Contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, sexta sesión, 21 de agosto - 1 de septiembre de 2023, Convenio preliminar (copia anticipada), página 13, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf

[115] Ibidem

[116] El 1 de septiembre de 2023, el Presidente del Grupo del AHC, debatió los artículos 29 y 30 (Recopilación en tiempo real de datos de tráfico e interceptación de datos de contenido, respectivamente) y expresó lo siguiente: "Sin embargo, en relación con los artículos 29 y 30, varias delegaciones solicitaron reserva a los facilitadores para proponer enmiendas y esperan poder continuar con los debates en la 7.ª sesión del Comité." UN Web TV, (23.ª reunión). Sexta sesión del Comité Ad Hoc encargado de elaborar un Convenio Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, 1 de septiembre de 2023, (comienza en 2:01:23), https://media.un.org/en/asset/k17/k17lzfhyyp

mantener la confidencialidad del hecho de la ejecución de cualquier facultad prevista en el presente artículo y de cualquier información relacionada con ella".[117]

Comentario: Singapur, Suiza, Malasia y Vietnam se oponen a la inclusión de este artículo en el convenio y solicitan que se elimine.

"Artículo 36: Protección de datos personales.
1. Un Estado parte que transfiera datos personales en virtud del presente Convenio lo hará con sujeción a las condiciones del derecho interno de dicho Estado parte y del derecho internacional aplicable. Los Estados parte no estarán obligados a transferir datos personales de conformidad con el presente Convenio si no pueden hacerlo en cumplimiento de su legislación aplicable en materia de protección de datos personales. También podrán procurar imponer condiciones, de conformidad con dichas leyes aplicables, para lograr el cumplimiento a fin de responder a una solicitud de datos personales. Se recomienda a los Estados parte que establezcan acuerdos bilaterales o multilaterales para facilitar la transferencia de datos personales".[118]

CARICOM, la UE y sus Estados miembros, Vanuatu, Nueva Zelanda, Albania, Georgia, Estados Unidos, Reino Unido, China, Noruega, Cabo Verde, Tanzania, Líbano, Colombia, Ecuador, Pakistán, Suiza, Tonga y Australia respaldaron la inclusión de esta disposición en el Artículo 36: "1 bis. Cuando la transferencia de datos personales no pueda llevarse a cabo de conformidad con el apartado 1, los Estados parte podrán procurar imponer condiciones apropiadas (de conformidad con su legislación aplicable en materia de protección de datos personales [...] para lograr el cumplimiento a fin de responder positivamente a una solicitud de datos personales".[119]

Comentario: India propuso eliminar la disposición adicional mencionada.

La Federación Rusa propuso esta adición en:
"Artículo 40: Principios y procedimientos generales relativos a la asistencia judicial recíproca.
[...] 3. La asistencia judicial recíproca que debe prestarse de conformidad con el este artículo podrá solicitarse para cualquiera de los fines siguientes: [...] [(l bis) Retirada del nombre de dominio utilizado para actividades delictivas".[120]

"Artículo 43: Divulgación expeditiva de datos de tráfico conservados
1. Cuando, en el curso de la ejecución de una solicitud formulada conforme al artículo 42 para preservar los datos de tráfico relativos a una comunicación específica, el Estado parte requerido descubra que un proveedor de servicios de otro Estado parte participó en la transmisión de la comunicación, el Estado parte requerido revelará sin demora al Estado parte requirente una cantidad suficiente de datos de tráfico para identificar a ese proveedor de servicios y la vía por la cual se transmitió la comunicación".[121]

---

[117] Comité Ad Hoc encargado de elaborar un Convenio Internacional Integral Contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, sexta sesión, 21 de agosto - 1 de septiembre de 2023. Texto preliminar del convenio (Situación al 2 de septiembre de 2023 con actualizaciones de los Estados miembros), pág. 33
https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf
[118] Ibidem, pág. 38
[119] Ibidem
[120] Ibidem, pág. 47
[121] Los Estados parte acordaron "ad referéndum" esta disposición, Ibidem, pág. 26

Artículo 45: Asistencia jurídica mutua en la recopilación de datos de tráfico en tiempo real
1. Los Estados parte se prestarán asistencia judicial recíproca en la recopilación en tiempo real de datos de tráfico asociados a comunicaciones especificadas en su territorio transmitidas por medio de [un sistema informático] [un dispositivo de tecnología de la información y la comunicación]. Con sujeción a lo dispuesto en el párrafo 2, dicha asistencia se regirá por las condiciones y procedimientos previstos en el derecho interno".

[...]

"3. Una solicitud formulada de conformidad con el párrafo 1 del este artículo deberá especificar: (c) Los [datos informáticos] [información digital] en relación con los cuales se requiere la obtención de los datos de tráfico y su relación con el delito u otro acto ilícito; (d) Cualquier dato disponible que identifique al propietario o usuario de los datos o la ubicación del [sistema informático] [dispositivo de tecnología de la información y la comunicación];"[122]

Contexto: El AHC estaba celebrando consultas informales en el período entre sesiones entre la sexta y la última sesión en enero-febrero de 2024. Las múltiples partes interesadas no fueron invitadas a participar de estas consultas y son únicamente para los gobiernos. El objetivo de la Presidencia era elaborar un proyecto de texto abreviado y "depurado" del Convenio para fines de noviembre de 2023.

[122] Ibidem

Pacto Digital Mundial y Cumbre del Futuro

Introducción/Antecedentes

En 2020, en el informe del Secretario General Guterres, Nuestra Agenda Común, se propuso una Cumbre del Futuro, con una vía tecnológica que condujera a un Pacto Digital Mundial (GDC): "Además, sobre la base de las recomendaciones de la hoja de ruta para la cooperación digital (Consultar A/74/821), las Naciones Unidas, los gobiernos, el sector privado y la sociedad civil podrían reunirse en un grupo de múltiples partes interesadas en tecnología digital como preparación para una Cumbre del Futuro con el fin de acordar un Pacto Digital Mundial. Esto esbozaría principios compartidos para un futuro digital abierto, libre y seguro para todos".[123]

El Pacto Digital Mundial

El 25 de abril de 2023, el Secretario General de las Naciones Unidas publicó el Informe sobre Políticas n.º 5, que contenía específicamente el texto del Secretario General de las Naciones Unidas sobre los parámetros del marco para el futuro Pacto Digital Mundial (GDC). Consultar el blog de la ICANN donde se contextualizan algunas citas sobre el GDC.[124]

Extractos de presentaciones escritas para el GDC por parte de Estados miembros, coaliciones y organizaciones supranacionales

Contexto: La oficina del Enviado de las Naciones Unidas para la Tecnología organizó una serie de sesiones de profundización sobre temas relacionados con el Pacto Digital Mundial (GDC) en primavera y verano de 2023. El personal de Participación Gubernamental (GE) de la ICANN estuvo presente durante estas presentaciones; sin embargo, las deliberaciones no se registraron oficialmente y GE no puede proporcionar citas de estos debates. No obstante, algunas de las contribuciones por escrito reflejan las intervenciones orales de las delegaciones de los países durante estas deliberaciones.

Abril de 2023

El 13 de abril de 2023, la Unión Europea declaró: "La UE cree que, [...] Internet debe seguir siendo abierta, global, libre, interoperable y descentralizada. Respaldamos enérgicamente el enfoque multisectorial de la gobernanza de Internet, que garantiza que todos los actores, incluidos los gobiernos, el sector privado, la sociedad civil y las comunidades técnicas, participen en la configuración del futuro de Internet".

[…]
"Un ejemplo positivo de la promoción del enfoque de múltiples partes interesadas fue la exitosa transición de la custodia de la IANA a la ICANN en 2016. Todas las partes interesadas,

[123] Declaración sobre la Conmemoración del Septuagésimo Quinto Aniversario de las Naciones Unidas. Resolución adoptada por la Asamblea General el 21 de septiembre de 2020, A/RES/75/1, 28 de septiembre de 2020, https://documents.un.org/prod/ods.nsf/xpSearchResultsE.xsp
[124] Blogs de la ICANN, 13 de junio de 2023, https://www.icann.org/en/blogs/details/un-secretary-general-policy-report-considerations-for-the-icann-community-13-06-2023-es

incluidos los gobiernos, son bienvenidos a participar en la ICANN y pueden contribuir a incrementar la seguridad y la estabilidad del sistema mundial de nombres de dominio, DNS".[125]

La República Islámica de Irán declaró: "Preparar un marco de cooperación eficaz entre los custodios del ecosistema de gobernanza de Internet, y los guardianes de la propiedad intelectual y el sistema de gestión con los organismos encargados del cumplimiento de la ley y las autoridades judiciales de los países para la prevención y lucha contra los ciberdelitos".[126]

Los Países Bajos declararon: "El Pacto Digital Mundial debe comprometerse a evitar la fragmentación de la infraestructura técnica de Internet, lo que impedirá la capacidad de los sistemas para interoperar y amenazará la integridad general y la disponibilidad de la infraestructura básica de Internet. Esto incluye el enrutamiento y reenvío de paquetes, los sistemas de nombres y números, las [tecnologías] de cifrado y las infraestructuras físicas subyacentes".[127]

El G77 y China declararon: “El Pacto Digital Mundial debe basarse en documentos y foros clave para avanzar en la cooperación digital, entre otros, la Cumbre Mundial sobre la Sociedad de la Información (CMSI), en particular la Agenda de Túnez y el Plan de Acción de Ginebra, el Foro de Gobernanza de Internet, y tener en cuenta la Hoja de Ruta del Secretario General para la Cooperación Digital".
[…]
"El Grupo subraya que los resultados de la CMSI deben preservarse como guía para la cooperación digital internacional y para la gobernanza de Internet, dado que se basan en principios que favorecen el desarrollo".
"La Agenda de Túnez y la Declaración de Principios y el Plan de Acción de Ginebra establecerán los principios rectores para el desarrollo de cualquier nuevo mecanismo sobre cooperación digital, incluido el Pacto Digital Mundial".

[...]
"Reconocemos que no se debe permitir que un solo país o parte interesada, o un pequeño grupo de ellos, monopolice o controle la infraestructura básica de Internet".
"Los Estados que tienen el monopolio y el dominio en el entorno de las TIC, incluido Internet, no deben utilizar los avances de las TIC como herramientas de contención y supresión del legítimo desarrollo económico y tecnológico de otros Estados".
"El Pacto Digital Mundial debe reiterar que Internet debe ser abierta, segura, inclusiva, accesible e interoperable".
[...]
"La gobernanza de Internet debe abordarse en una configuración global, respaldada por el sistema de las Naciones Unidas, a través de una amplia participación de todos los Estados con

[125] Delegación de la Unión Europea ante las Naciones Unidas en Nueva York, Declaración de la UE -- Pacto Digital Mundial: Análisis en Profundidad sobre la Gobernanza de Internet, 13 de abril de 2023, https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-global-digital-compact-deep-dive-internet-governance_en?s=63
[126] Contribución de la República Islámica de Irán al Pacto Digital Mundial, abril de 2023, modificada por última vez el 2 de mayo de 2023, pág. 20, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_Islamic-Republic-Iran.pdf
[127] Documento del Pacto Digital Mundial presentado por el Reino de los Países Bajos, 28 de abril de 2023, pág. 7, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission-Kingdom-of-the-Netherlands.pdf

un enfoque de múltiples partes interesadas, tal como se establece en los resultados de la CMSI".
[…]
"Se debe mantener la seguridad, la protección y la estabilidad de Internet, sin poner en peligro los esfuerzos por lograr un desarrollo sostenible. La cooperación internacional a través del fortalecimiento del multilateralismo en este ámbito es muy importante".[128]

El Salvador reafirmó "… la importancia de continuar con el enfoque de múltiples partes interesadas esbozado en la Cumbre de Ginebra de 2003 y la Agenda de Túnez de 2005".[129]

Francia redactó lo siguiente: "Acciones propuestas: […] También habrá que trabajar en los protocolos para mantener la unidad, neutralidad y resiliencia de Internet".[130]

La República Popular China declaró: "Los Estados tienen derecho a participar en la gestión y distribución de los recursos internacionales básicos de Internet en igualdad de condiciones, y deben abstenerse de aprovechar los recursos y las tecnologías de Internet para socavar los derechos legítimos de otros Estados a acceder a Internet, poniendo así en peligro la seguridad, la estabilidad y la conectividad de la Internet global".[131]
[...]

"Los Estados deben fomentar un ciberespacio que ofrezca paz, seguridad, apertura, cooperación y orden, y deben oponerse a la división y fragmentación de Internet. Los Estados deben formular reglas y normas comunes interoperables a nivel mundial en el ciberespacio a través de una amplia participación de los Estados miembros bajo los auspicios de las Naciones Unidas, y deben seguir comprometidos con la construcción de un sistema internacional de gobernanza de Internet que se caracterice por el multilateralismo, la democracia y la transparencia".[132]

Reunión informal de lanzamiento del Informe sobre Políticas n.º 5 de Nuestra Agenda Común
Un Pacto Digital Mundial: Un Futuro Digital Abierto, Libre y Seguro para Todos[133]

En una reunión informal celebrada en la sede de las Naciones Unidas el 5 de junio de 2023, el Secretario General António Guterres presentó el Informe sobre Políticas n.º 5. En sus

[128] Aportes del G77 y China a los debates del Pacto Digital Mundial, 28 de abril de 2023, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_G77-and-China.pdf
[129] Presentación Nacional de El Salvador sobre las áreas temáticas propuestas por el Pacto Digital Mundial, última modificación 1 de mayo de 2023, pág. 3, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_El-Salvador.pdf
[130] Contribución de Francia al Pacto Digital Mundial - Traducción de cortesía, modificada por última vez el 8 de mayo de 2023, pág. 5, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_France.pdf
[131] Posiciones de China sobre la Gobernanza Digital Mundial (Contribución al Pacto Digital Mundial), modificada por última vez el 24 de mayo de 2023, pág. 5, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_China.pdf
[132] Ibidem, pág. 13
[133] Consultar la página de blogs de la ICANN para obtener información detallada sobre el Informe sobre Políticas: https://www.icann.org/en/blogs/details/un-secretary-general-policy-report-considerations-for-the-icann-community-13-06-2023-es

observaciones introductorias, el Sr. Guterres expresó: "El informe propone un Foro de Cooperación Digital que evaluaría los progresos en la gobernanza digital y pondría de manifiesto las brechas. Se trataría del primer marco mundial que reuniría a todas las partes interesadas para impulsar una actuación coordinada en materia de tecnología digital. Trabajaría con organismos regionales y redes de múltiples partes interesadas y apoyaría los intercambios entre organismos existentes, como el Foro de Gobernanza de Internet. Contaría con una amplia participación, involucraría a quienes desarrollan las tecnologías digitales para comprender su potencial y promovería su aplicación responsable".[134]

Respuestas de los delegados de algunos Estados miembros de las Naciones Unidas:

La Unión Europea (en nombre de sus 27 Estados): "Apoyar y reforzar estructuras establecidas como el Foro de Gobernanza de Internet, la UIT y la UNESCO, entre otras, podría ayudar a evitar la duplicación y fragmentación de esfuerzos". [...] "Un enfoque multilateral sería clave para apoyar el Pacto Digital Mundial"[135]

Canadá (también en nombre de Australia y Nueva Zelanda, o CANZ): "Nuestros países están plenamente comprometidos a trabajar con otros para garantizar la continuidad de una Internet libre, abierta, interoperable, fiable y segura a nivel mundial". [...] También somos firmes partidarios del modelo multisectorial de gobernanza de Internet, que es la base de la apertura, resiliencia y estabilidad de Internet. Un enfoque multilateral reconoce que todos tienen algo que decir sobre cómo se gestiona Internet. Debemos reconocer la función que las organizaciones multisectoriales existentes están desempeñando con éxito en el desarrollo y funcionamiento de Internet. Aunque admiramos la ambición de las propuestas contenidas en el informe sobre políticas, instamos encarecidamente a que cualquier nueva iniciativa potencial tenga como primer objetivo reforzar y complementar los esfuerzos ya realizados con éxito en la cooperación digital global en las Naciones Unidas".[136]

Lituania: "Quisiera subrayar especialmente la importancia de implicar la participación de las agencias especializadas, como la UIT, otorgándoles una función más claramente determinada para contribuir a los objetivos del Pacto".[137]

Pakistán: "Nos gustaría profundizar en la necesidad de tener un proceso intergubernamental que orientase el pacto hacia una línea más de desarrollo en lugar de una dirección reguladora y esto debería estar en consonancia con la agenda de Túnez donde las políticas públicas relacionadas con Internet son competencia, es decir, derecho soberano de los Estados. Por supuesto, también estamos considerando este Foro de Cooperación Digital que nos gustaría ver, y cómo se complementaría con el Foro de Gobernanza de Internet y con el Foro de la CMSI, así como con el Grupo de Trabajo de Composición Abierta sobre Seguridad en el Uso de las TIC".[138]

[134] Sesión informativa del Secretario General sobre los Informes de Políticas de Nuestra Agenda Común para la Cumbre del Futuro (organizada por la Oficina Ejecutiva del Secretario General (OESG), UN Web TV, 7 de mayo de 2023, (comienza en 19:35), https://media.un.org/en/asset/k1n/k1nugz7a7n,
[135] Ibidem, (comienza en: 20:30)
[136] Ibidem, (comienza en: 30:33)
[137] Ibidem, (comienza en: 34:00)
[138] Ibidem, (comienza en: 39:38)

Estados Unidos de América: "En cuanto al Pacto Digital Mundial para garantizar la transparencia, la inclusión y la participación activa y significativa de todas las partes interesadas en el proceso del GDC, recomendamos a las Naciones Unidas ofrecer oportunidades para que la comunidad de partes interesadas también efectúe comentarios con respecto al informe sobre políticas del GDC".[139] "Los esfuerzos por dirigir la cooperación digital desde Nueva York no reflejan el hecho de que los enfoques de múltiples partes interesadas, multisectoriales y descentralizados ofrecen un medio más efectivo para el aprovechamiento de las tecnologías digitales para el logro de los ODS".[140]

Suiza: ""La propuesta de crear un nuevo Foro de Cooperación Digital entraña el riesgo de entorpecer innecesariamente la aplicación del Pacto. En lugar de aportar un valor añadido auténtico, constituye una amenaza de duplicar los esfuerzos ya iniciados en las estructuras digitales para la cooperación existente. En particular, el Foro de Gobernanza de Internet ha demostrado su efectividad para hacer un seguimiento con carácter multisectorial de los temas contemplados en el Pacto".[141]

Estonia: "Para lograr una conectividad universal y significativa es necesaria una cooperación multilateral con base en nuestros valores y principios comunes, como ya acordamos en la Agenda de Túnez".[142]

China: "Sobre el GDC. China respalda a las Naciones Unidas para que desempeñen un papel fundamental en la coordinación de los esfuerzos conjuntos de las distintas partes interesadas con vistas a reforzar la cooperación digital, reducir la brecha digital y mejorar la gobernanza digital, de modo que la tecnología digital pueda ser provechosa para toda la humanidad. El proceso de redacción debe estar pensado en función de los problemas...".[143]

Indonesia: "En cuanto al GDC, tomamos nota de que comparte ideas similares con el tema del Foro de Gobernanza de Internet de 2023. Y, en este sentido, nos gustaría seguir escuchando opiniones sobre cómo garantizar que el Pacto Digital Mundial (GDC), en particular la iniciativa del Foro de Cooperación Digital Mundial, complemente el proceso existente, evite la duplicación y fortalezca el IGF".[144]

Reino Unido: "Toda nueva iniciativa debería complementar los esfuerzos de cooperación digital existentes que ya se están llevando a cabo en las Naciones Unidas. El Reino Unido reconoce que las organizaciones multisectoriales existentes son los cimientos de una Internet abierta, resiliente y estable".[145]

India: "Nuestro enfoque debe basarse en evitar la duplicación de esfuerzos o el establecimiento de procesos paralelos".[146]

[139] Ibidem, (comienza en: 1:06:50)
[140] Ibidem, (comienza en: 1:08:15)
[141] Ibidem, (comienza en: 1:10:17)
[142] Ibidem, (comienza en: 1:12:46)
[143] Ibidem, (comienza en: 1:18:24)
[144] Ibidem, (comienza en: 1:19:40)
[145] Ibidem, (comienza en: 1:24:30)
[146] Ibidem, (comienza en: 1:34:32)

Durante su discurso de clausura, el Secretario General de las Naciones Unidas expresó lo siguiente: "No obstante, es preciso distinguir cuál es el alcance del proceso intergubernamental, en lo que se refiere a la soberanía de los Estados miembros, y el alcance, las áreas en las que es conveniente el compromiso de todos para lograr que las cosas avancen en la dirección correcta. [...] Esperaba la pregunta sobre el Foro[147] porque también debatimos en nuestros equipos. Una vez más, no es una cuestión de fe. Es algo que proponemos; si los Estados miembros están de acuerdo, bien; si no lo están: no se muere nadie. Pero dicho esto, creo que la cuestión no es un tema de duplicación. Es una cuestión de dónde convergen las cosas. Hay varias opciones alrededor. Tenemos el Foro de Gobernanza de Internet, existen los mecanismos de la UIT, tenemos los mecanismos de la UNESCO, pero están todos separados. Y lo que creo que hace falta aquí, en Nueva York, en el entorno de la Asamblea General, es algo que permita conjugar estas opciones. [...] Duplicar no es lógico; resulta lógico garantizar que exista un espacio donde todas estas cosas se perciban de manera conjunta. Y es el único motivo por el que se puso esta propuesta sobre la mesa".[148]

Reunión ministerial preparatoria de la Cumbre del Futuro - Asamblea General, 78.ª sesión

El 21 de septiembre de 2023 se realizaron varias declaraciones ministeriales y de alto nivel sobre el Pacto Digital Mundial y la Gobernanza de Internet, entre ellas:

Ruanda: "La cooperación digital mundial será clave en virtud del GDC, proporciona dicho marco de cooperación digital".[149]

Noruega: "También debemos trabajar juntos en pos de una transformación digital mundial justa y el Pacto Digital Mundial".[150]

Rusia: "Avalamos la inclusión de las cuestiones de tecnología e innovaciones en la agenda de la Cumbre a fin de superar la desigualdad digital y lograr la democratización de la Gobernanza de Internet y la regulación de la AI con una estricta observancia de la soberanía nacional de todos los Estados".[151]

Bulgaria: "La preservación del enfoque multisectorial y la integridad de Internet es donde debemos obtener mejores resultados".[152]

México: "Estamos plenamente comprometidos con el Pacto Digital Mundial".[153]

[147] en el presente documento: Foro de Cooperación Digital
[148] Sesión informativa del Secretario General sobre los Informes de Políticas de Nuestra Agenda Común para la Cumbre del Futuro (organizada por la Oficina Ejecutiva del Secretario General (OESG), UN Web TV, 7 de mayo de 2023, (comienza en 1:55:11) https://media.un.org/en/asset/k1n/k1nugz7a7n
[149] UN Web TV, (Apertura, Plenario, Clausura) Reunión ministerial preparatoria de la Cumbre del Futuro - Asamblea General, 78.ª sesión, 21 de septiembre de 2023, (comienza en: 42:52), https://media.un.org/en/asset/k1z/k1zzbbnqaq
[150] Ibidem, (comienza en: 1:39:10)
[151] Ibidem, (comienza en: 02:55:05)
[152] Ibidem, Consultar el original en francés (comienza en: 03:24:40)
[153] Ibidem, (comienza en: 04:05:19)

UIT: "Estos desafíos requieren que todas las partes interesadas trabajen en forma conjunta. La Cumbre Mundial sobre la Sociedad de la Información y su proceso de seguimiento, como el IGF y el Foro de la CMSI, tienen una importante función que desempeñar y así lo han reconocido los cofacilitadores del Pacto Digital Mundial".[154]

India: "Acogemos con beneplácito el objetivo del SoTF de hacer realidad el Pacto Digital Mundial a fin de minimizar cualquier brecha digital".[155]

Zimbabue: "Es necesario un enfoque multilateral más holístico de la gobernanza tecnológica dados los rápidos avances de la tecnología y las amenazas y riesgos asociados. Necesitamos imperiosamente un Pacto Digital Mundial".[156]

Finlandia: "Una de las áreas clave de la futura Cumbre sería acordar el Pacto Digital Mundial. El Pacto debe aportar un valor añadido auténtico y tangible sobre el modo de cooperar en las prioridades digitales comunes, impulsar soluciones en pos de los ODS y salvaguardar los derechos humanos en el espacio digital, entre ellos la privacidad y la libertad de expresión".[157]

Otras iniciativas de las Naciones Unidas

Documentos oficiales de la 77.ª sesión de la Asamblea General de las Naciones Unidas

El 15 de mayo de 2023, Rusia, Bielorrusia, Corea del Norte, Nicaragua y Siria (como copatrocinadores) presentaron el Concepto del Convenio de las Naciones Unidas para Garantizar la Seguridad de la Información Internacional como documento oficial de la 77.ª sesión de la Asamblea General de las Naciones Unidas.[158]
Los copatrocinadores nombraron, entre otros, el siguiente principio y propuesta que "podría servir de base para las disposiciones del Convenio que rigen las actividades de los Estados y definen los derechos y obligaciones de los Estados con respecto a la promoción de la creación de capacidades publica en el ámbito de la seguridad en el uso de las tecnologías de la información y la comunicación: [...] la promoción del desarrollo y la utilización de tecnologías de la información y la comunicación seguras de conformidad con el principio de neutralidad de la red mundial de comunicaciones, incluida la reforma evolutiva de los protocolos y los métodos de transferencia de información para eliminar la posibilidad de utilizar esta red con fines delictivos;"[159]

Contexto: Rusia y los copatrocinadores del proyecto de convenio insistieron en que se mencionara el concepto de proyecto de convenio en el Informe Anual del Progreso Logrado

[154] Ibidem, (comienza en: 05:15:40)
[155] Ibidem, (comienza en: 06:36:55)
[156] Ibidem, (comienza en: 07:10:40)
[157] Ibidem, (comienza en: 07:48:55)
[158] Ministerio de Asuntos Exteriores de la Federación Rusa, comunicado de prensa sobre el Concepto del Convenio de las Naciones Unidas sobre Seguridad de la Información Internacional, 16 de mayo de 2023, https://mid.ru/ru/foreign_policy/news/1870609/?lang=en
[159] Concepto actualizado del Convenio de las Naciones Unidas para Garantizar la Seguridad de la Información Internacional, 15 de mayo de 2023, pág. 8, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf

2023 del OEWG. Rusia afirmó que China e Irán también apoyan la inclusión de dicha mención en el Informe Anual sobre el Progreso Logrado del OEWG.[160]

Declaraciones del Enviado del Secretario General para la Tecnología (Enviado de las Naciones Unidas para la Tecnología)

El 13 de octubre de 2022, el Enviado de las Naciones Unidas para la Tecnología, el embajador Amandeep Singh Gill, declaró lo siguiente: "La Cumbre del Futuro de 2024 es una oportunidad para que la comunidad internacional reinicie el multilateralismo y nos preparemos mejor para los desafíos del mañana.

La Asamblea General de la Naciones Unidas ha decidido la celebración de la cumbre en función de un informe que se solicitó al Secretario General. Este informe se titula Nuestra Agenda Común, y el Pacto Digital Mundial (GDC) es una de las propuestas allí contenidas. Se adoptará en la Cumbre del Futuro".[161]
El 24 de octubre de 2022, el embajador Gill declaró lo siguiente: "No dudo en afirmar que ese compromiso con los enfoques multisectoriales es sumamente sólido. De hecho, cuando el Secretario General se dirigió a la Asamblea General, dejó claro que o llegábamos al GDC a través de un proceso multisectorial o no lo haríamos en absoluto. Fue una declaración muy clara y contundente que realizó en Nueva York. Y honramos ese cometido a través de estas y otras muchas consultas, y mediante un firme compromiso no sólo con el IGF, sino también con otros foros como la ICANN".[162] Y continuó: ""Ahora, su planteamiento sobre cómo podemos ir más allá de la esencia ritual de los enfoques multisectoriales y cómo abordar esta dualidad, es o bien el multilateralismo intergubernamental o los enfoques multisectoriales, que acaban convirtiéndose en interesantes debates consultivos; sin embargo ¿cuál es el sendero hacia la implementación? Tenemos dificultades y, francamente, nadie lo ha resuelto".[163]
"He oído decir en Nueva York que la fórmula de la CMSI de Túnez es acertada para la participación de múltiples partes interesadas. Ya saben que esa formulación forma parte de nuestros respectivos mandatos y autoridades. No tengo delante el texto exacto, pero para algunos esa fórmula no es lo suficientemente ambiciosa y para otros es demasiado ambiciosa. Así que vamos a ver dónde desembocamos con que es uno de esos buenos ejemplos también a tener en cuenta. Tal vez podamos llegar a una fórmula sui generis que satisfaga a David, Adam[164] y todos los demás en este aspecto".[165]

El 23 de junio de 2023, el Enviado de las Naciones Unidas para la Tecnología expresó lo siguiente: ""Los invito a que lean la última sección de este informe [del Secretario General de las Naciones Unidas] sobre la idea de una evaluación periódica de la implementación del pacto para seguir el ritmo de los avances tecnológicos. Y lo que quiero recalcar de nuevo, especialmente en referencia a los comentarios anteriores de este panel, es que se trata de un foro de múltiples partes interesadas.

[160] UN Web TV, (8.ª reunión) Grupo de Trabajo de Composición Abierta sobre Tecnologías de la Información y la Comunicación (TIC). Quinta sesión sustantiva, 27 de julio de 2023, (comienza en 13:50), https://media.un.org/en/asset/k1n/k1ngmoogyi
[161] Noticias de la UIT. Establecimiento del Pacto Digital Mundial: Sesión de preguntas y respuestas con Amandeep Singh Gill, 13 de octubre de 2023, https://www.itu.int/hub/2022/10/establishing-the-global-digital-compact-qa-with-amandeep-singh-gill/
[162] IGF, Reunión con el Enviado del Secretario General de las Naciones Unidas para la Tecnología, 24 de octubre de 2022, (comienza en 49:53), https://youtu.be/NEmXNzQzsCk?t=2991
[163] Ibidem, (comienza en 51:31), https://youtu.be/NEmXNzQzsCk?t=3091
[164] En este punto, el Enviado de la ONU para la Tecnología se refiere a las preguntas que le plantearon el representante de Canadá y el miembro del MAG sobre la función del proceso de la CMSI y la comunidad técnica.
[165] Ibidem, (comienza en 1:06:13), https://youtu.be/NEmXNzQzsCk?t=397

Por lo dicho, la preparación es tripartita, por lo que esas palabras se utilizan claramente en la sociedad civil, lo que incluye a todos los actores de la comunidad técnica, el sector académico y el valor de la experiencia científica independiente, en particular en torno a la AI, ya se sabe que hoy se entiende perfectamente que hay sector privado y hay gobiernos".[166]

Evento Paralelo a la Semana contra el Terrorismo de 2023

El 22 de junio de 2023, Tech Against Terrorism (Tecnología contra el Terrorismo), una iniciativa apoyada por la Dirección Ejecutiva del Comité contra el Terrorismo de las Naciones Unidas (DECT) solicitó a los Estados que "consideren formas de mejorar los mecanismos para eliminar los sitios web operados por terroristas, lo que incluye ayudarnos a intervenir ante los registradores de nombres de dominio, las redes de distribución de contenidos y los proveedores de alojamiento".[167]

Conclusión

Los debates en curso en las Naciones Unidas en el marco del OEWG concluirán en 2025; el informe constituirá el resultado de estas deliberaciones si se adopta como fruto del consenso. Está previsto que las deliberaciones del AHC concluyan en febrero de 2024 con la adopción del convenio sobre ciberdelito por consenso o, si no fuera posible lograr el consenso, con la mayoría de dos tercios de las delegaciones de los países presentes y con derecho a voto. La función Participación Gubernamental (GE) seguirá ambos procesos e informará sobre ellos, aunque en su opinión, es probable que sus resultados tengan mínima o ninguna repercusión en la misión de la ICANN.

Las negociaciones sobre el GDC comenzarán en enero de 2024, y está previsto que la fase final tenga lugar del 20 al 23 de septiembre de 2024 durante la Cumbre del Futuro, en la que se espera que el Pacto se adopte por consenso. En la actualidad, este proceso presenta demasiadas incógnitas para la organización. GE seguirá todas las deliberaciones sobre el GDC para informar a la comunidad de la ICANN sobre los avances y novedades a medida que se desarrolle la dinámica de las negociaciones.

[166] Video de YouTube, EuroDIG 2023 - Pre 05 | Promovamos la visión europea de la gobernanza y la cooperación digitales, 23 de junio de 2023, (comienza en 1:36:42), https://youtu.be/RctcgFscohU?t=5802
[167] UN Web TV, Prevención y lucha contra el uso de tecnologías nuevas y emergentes con fines terroristas: el camino hacia una respuesta multilateral holística (evento paralelo a la Semana contra el Terrorismo 2023), 22 de junio de 2023, (comienza en 1:08:27), https://media.un.org/en/asset/k1i/k1iy7ltzvt

Un mundo, una Internet

Visiten **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin.com/company/icann

soundcloud.com/icann

instagram.com/icannorg