Actualización de las Naciones Unidas: Debates relacionados con la cibernética

Participación Gubernamental y de las Organizaciones Intergubernamentales (OIG) de la ICANN

Veni Markovski
GE-005
15 de julio de 2020

ÍNDICE

Prólogo

El presente documento proporciona una actualización de las actuaciones de los grupos de trabajo de la Asamblea General de las Naciones Unidas (AGNU), en los que se debaten cuestiones relacionadas con Internet y ciberseguridad.

Durante estos debates, en ocasiones, se plantean cuestiones que afectan a la misión de la ICANN y que podrían seguir mencionándose en el futuro. El monitoreo de los debates forma parte de la manera en que la función de Participación Gubernamental (GE) de la organización de la ICANN apoya la misión de la ICANN, y también demuestra el compromiso y la responsabilidad de GE de mantener informada a la comunidad de la ICANN en su conjunto sobre cuestiones de importancia para una Internet global, única e interoperable y su sistema de identificadores únicos.[1]

En nuestro documento anterior, "Breve reseña de las deliberaciones de las Naciones Unidas sobre ciberseguridad y ciberdelito", proporcionamos información sobre el establecimiento de los diferentes grupos de trabajo y procesos en las Naciones Unidas (ONU).[2] En el presente documento nos centramos en las actualizaciones del Grupo de Trabajo de composición abierta (OEWG) y del Comité intergubernamental especial de expertos de composición abierta (OECE).

[1] Como se explica en nuestro plan operativo y financiero quinquenal, p. 47: "Supervisar la legislación, la regulación, las normas, los principios y las iniciativas que puedan afectar a la misión de la ICANN"

[2] El presente documento forma parte de una serie publicada por Participación Gubernamental a partir del 28 de febrero de 2020. Para consultar todos los documentos de Participación Gubernamental, visite nuestra página web aquí.

Actualizaciones sobre el OECE, el OEWG y el GEG

OECE

El OECE[3] comenzó su trabajo sobre la "lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos" con la publicación de un documento en el que se proponía un esquema y modalidades para los próximos cuatro años.[4] El documento, cuyo debate está previsto para la primera reunión del grupo en agosto de 2020, proporciona un marco para el trabajo del OECE hasta su conclusión en junio de 2024.

El 10 de julio se celebró una reunión virtual informal relacionada con la sesión de organización del Comité Especial sobre Delito Cibernético. Durante la reunión, la ONUDD proporcionó información actualizada sobre las cuestiones de procedimiento relacionadas con el período de sesiones de organización del comité especial celebrado en agosto y luego los Estados miembros examinaron la agenda provisional del período de sesiones de organización del comité especial.[5] En el sitio web del OECE, se puede encontrar más información sobre esta reunión informal virtual de julio, en particular, en el documento titulado "Resumen de la información proporcionada por el Director de la División para Asuntos de Tratados, ONUDD, en la reunión informal del 10 de julio de 2020".[6]

A partir del 13 de julio de 2020, el OECE ha publicado en su página web comentarios de los siguientes Estados miembros: Australia, Canadá, Estados Unidos de América, Federación de Rusia, Japón, Reino Unido de Gran Bretaña e Irlanda del Norte, República Dominicana, Unión Europea y República Islámica de Irán.

OEWG

Desde marzo de 2020, el Presidente del OEWG[7] publicó un informe preliminar inicial el 11 de marzo de 2020.[8] Dicho documento estuvo abierto para recepción de comentarios de todas las partes interesadas con la intención de que se examinara en una reunión presencial a finales de

[3] OECE son las siglas en inglés de *Open-ended ad hoc intergovernmental committee of experts* (Comité intergubernamental especial de expertos de composición abierta); está formado por todos los Estados miembros de las Naciones Unidas y se encarga de redactar una nueva convención de las Naciones Unidas sobre el ciberdelito. En el presente documento utilizamos el término "convención sobre el ciberdelito", sin embargo la ONU utiliza el término "convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos".
[4] El documento se encuentra disponible aquí.
[5] Oficina de las Naciones Unidas contra la Droga y el Delito, https://www.unodc.org/
[6] Descargue el PDF aquí.
[7] OEWG son las siglas en inglés de *Open-ended Working Group* (Grupo de trabajo de composición abierta) sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional; en nuestro documento utilizamos el término ciberseguridad.
[8] Descargue el PDF aquí.

marzo de 2020. Sin embargo, debido a la COVID-19, esa reunión no se celebró.[9] En su lugar, se invitó a los Estados miembros a que envíen comentarios por escrito. Docenas de Estados miembros, organizaciones intergubernamentales y organizaciones no gubernamentales enviaron sus comentarios, que se publicaron en el sitio web del grupo.[10]

En el presente documento, citamos algunos de los comentarios presentados en respuesta a la solicitud de comentarios del Presidente.[11] Nos centramos únicamente en los comentarios que podrían interpretarse como relacionados con la misión o el cometido de la ICANN.

***

El punto 38 del informe preliminar comienza con:

"*Los Estados, durante los debates y mediante comunicaciones por escrito, también propusieron sugerencias para la 'mejora', así como una mayor elaboración de las normas. Las propuestas incluían, entre otras, que los Estados afirmaran su compromiso con la paz y la seguridad internacional en la utilización de las TIC; que se reafirmara que los Estados son los principales responsables de mantener un entorno de TIC seguro y confiable; que se protegiera la disponibilidad general o la integridad del núcleo público de Internet; [...]".*

Comentarios de algunos Estados miembros sobre el informe preliminar

> Brasil: "*Desde el punto de vista de Brasil, las infraestructuras de TI que sustentan los procesos electorales también merecen la misma protección que se otorga al núcleo público de Internet (párrafo 38)*".
>
> China: "*En virtud de la cantidad limitada de tiempo de la cual disponemos, también se debería prestar atención para evitar introducir en el informe conceptos que aún no han obtenido un consenso a nivel mundial (por ejemplo, el 'núcleo público')*".
> y: *"Durante los dos períodos de sesiones anteriores, las partes, incluida China, han presentado docenas de propuestas constructivas sobre cuestiones como la soberanía cibernética, la seguridad de la cadena de suministro, la protección de la infraestructura crítica, la abstención de sanciones unilaterales y la lucha contra el ciberterrorismo. Se espera que estas propuestas puedan incorporarse en el informe".*
>
> Egipto: "*Se debería alentar a los Estados miembros a que lleguen a una definición común acordada de lo que constituye 'infraestructura crítica', con miras a acordar, según corresponda, la prohibición de todo acto que utilice de forma deliberada o intencional capacidades ofensivas de TIC para dañar o perjudicar de otro modo el uso y el funcionamiento de la infraestructura crítica*".
>
> Alemania: "*Los agentes estatales y no estatales no deberían realizar ni permitir deliberadamente actividades que perjudiquen de forma intencional y sustancial la disponibilidad general o la integridad del núcleo público de Internet y, por consiguiente, la estabilidad del ciberespacio" [sería] una orientación para la implementación de la*

[9] Nota: la COVID-19 ha afectado el funcionamiento habitual de las Naciones Unidas y de los grupos de trabajo mencionados anteriormente. Por ejemplo, el OEWG tuvo la primera ronda de reuniones informales virtuales en junio y julio de 2020.
[10] https://www.un.org/disarmament/open-ended-working-group/
[11] Puede ver la invitación aquí.

recomendación 13(f) del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015 y, por lo tanto, incluirla también en el ámbito de aplicación de la recomendación 13 (g) del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015
y: *"En lo que respecta al párrafo 31, Alemania desea subrayar que la atención del OEWG debería centrarse en el fortalecimiento de las normas existentes y en la mejora de su comprensión e implementación. A este respecto, consideramos que las propuestas para proteger el núcleo público de Internet, para no perturbar la infraestructura esencial para los procesos políticos, para no perjudicar las instalaciones médicas y para destacar la infraestructura transnacional como adiciones útiles a las normas ya existentes sobre la protección de infraestructura crítica que figuran en el informe del Grupo de Expertos Gubernamentales de 2015".*

Irán: "*Sin embargo, en la versión preliminar no se han reconocido algunas importantes amenazas correspondientes, como las medidas coercitivas unilaterales, el monopolio de la gobernanza de Internet, el anonimato de personas y cosas, las estrategias y políticas cibernéticas ofensivas, etc., que afectan claramente el conocimiento, la resiliencia y las capacidades de los países*".

Países Bajos: *"Para hacer frente a estas amenazas, los Países Bajos desean sugerir que el OEWG considere la recomendación que señala que "los agentes estatales y no estatales no deberían realizar ni permitir deliberadamente actividades que perjudiquen de forma intencional y sustancial la disponibilidad general o la integridad del núcleo público de Internet y, por consiguiente, la estabilidad del ciberespacio" como orientación para la implementación de la recomendación 13(f) del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015 y, por lo tanto, incluirla también en el ámbito de aplicación de la recomendación 13 (g) del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015".*
y: *"Los Países Bajos desean sugerir que el informe del OEWG considere la amenaza que plantean las ciberoperaciones contra la disponibilidad general o la integridad del núcleo público de Internet. A lo largo de los años, las ciberoperaciones contra la integridad, el funcionamiento y la disponibilidad de Internet han demostrado ser una amenaza real y verosímil".*

Nicaragua: señala que la actual *"regulación insuficiente de las actividades del sector privado en el ámbito de las TIC"* es una *"gran amenaza para el desarrollo de un entorno pacífico de las TIC".*

Pakistán: "*Se debería alentar a los Estados miembros a que lleguen a una definición común acordada de lo que constituye 'infraestructura crítica', con miras a acordar la prohibición de cualquier actividad de las TIC que dañe de forma deliberada o intencional la infraestructura crítica o que de otro modo perjudique el uso y el funcionamiento de la infraestructura crítica*".

Rusia: *"Se exagera artificialmente la importancia de un 'enfoque de múltiples partes interesadas' con énfasis en la contribución de los sectores no gubernamental, empresarial y académico para garantizar un comportamiento responsable en el espacio de la información. Al mismo tiempo, se omite el problema de la reglamentación insuficiente de las actividades del sector privado en la esfera de las TIC y el problema cada vez más urgente de la monopolización de esa área como una de las principales amenazas al desarrollo de un entorno de TIC pacífico y competitivo".*

Suiza: *"Por ejemplo, las propuestas relativas a la protección del núcleo público de Internet, a no dañar las instalaciones médicas, a no perturbar la infraestructura esencial para los procesos políticos y relativas a la infraestructura crítica transnacional podrían, en nuestra opinión, proporcionar una valiosa orientación para las normas existentes".*

EE. UU.: *"...la elaboración selectiva de normas o la identificación de sectores específicos de infraestructura crítica conlleva cierto riesgo de dar prioridad a ciertas cuestiones sobre otras".*

Unión Europea: *"Por lo tanto, la protección de la infraestructura crítica es de tal importancia, que la UE y sus Estados miembros sugieren que en el informe del OEWG se consideren esas amenazas, incluida la que se plantea contra la disponibilidad general o la integridad del núcleo público de Internet".*

Comentarios de organizaciones no gubernamentales

Global Partners Digital: *"Recomendación: Respaldamos las recomendaciones de los Países Bajos en el 'documento no oficial', de explicar en detalle y proporcionar más orientación sobre las normas (f) y (g) del informe del Grupo de Expertos Gubernamentales de las Naciones Unidas de 2015 (Res 70/237), a saber: 'los agentes estatales y no estatales no deberían realizar ni permitir deliberadamente actividades que perjudiquen de forma intencional y sustancial la disponibilidad general o la integridad del núcleo público de Internet y, por consiguiente, la estabilidad del ciberespacio'".*

Sociedad de Internet: *"El núcleo público de Internet encapsula los sistemas de enrutamiento, asignación de nombres y números de Internet (el Sistema de Nombres de Dominio), los mecanismos de criptografía de identidad y seguridad y los cables de comunicaciones. Estas son las funciones principales que hacen que Internet funcione y deben ser protegidas para asegurar que Internet siga siendo una tecnología instrumental que tenga integridad y alcance global. Recomendamos al OEWG que tenga debidamente en cuenta los valores de la Norma de la GCSC para proteger el núcleo público, que hace hincapié en la necesidad de que los agentes estatales y no estatales se abstengan de permitir cualquier actividad que pueda perjudicar de forma intencional o sustancial la disponibilidad general o la integridad del núcleo público de Internet y, por consiguiente, la estabilidad del ciberespacio".*

Microsoft: en su primera presentación expresa: *"apoya firmemente varias de las nuevas normas que han sido propuestas por los Estados miembros que creemos que son adiciones fundamentales a la base existente de normas cibernéticas previamente acordadas en el contexto del Grupo de Expertos Gubernamentales: los agentes estatales y no estatales no deberían realizar ni permitir deliberadamente actividades que perjudiquen de forma intencional y sustancial la disponibilidad general o la integridad del núcleo público de Internet y, por consiguiente, la estabilidad del ciberespacio".* Microsoft también insta a sus miembros a que sigan el principio del Llamamiento de París de *"Impedir actividades que perjudiquen de forma intencional y sustancial la disponibilidad general o la integridad del núcleo público de Internet".*

Microsoft, en una segunda comunicación, declara lo siguiente: *"Los compromisos anteriores del Grupo de Expertos Gubernamentales reflejan esta importancia y diversas*

declaraciones realizadas desde entonces, entre ellas el Llamamiento de París y la GCSC, reflejan el creciente compromiso de proteger de los ciberataques a la tecnología que constituye la columna vertebral de la propia Internet. Algunos esfuerzos se refieren a esto como la protección de la disponibilidad general o la integridad del 'núcleo público' de Internet, mientras que otros prefieren referirse a los componentes técnicos de Internet. Es importante señalar que los Estados deberían ponerse de acuerdo sobre una nueva norma para proteger esos componentes centrales sin los cuales la Internet global dejaría de funcionar. La GCSC define estos componentes como: enrutamiento y reenvío de paquetes; sistemas de asignación de nombres y números; mecanismos criptográficos de seguridad e identidad; medios de transmisión, software y centros de datos".

Doce ONG[12] emitieron una declaración conjunta: *"Los ataques a la infraestructura crítica y, en este caso, también a la 'infraestructura crítica de información supranacional' (que debe entenderse que incluye el Sistema de Nombres de Dominio y otros elementos del núcleo público de Internet), plantean no solo 'una amenaza a la seguridad, sino también al desarrollo económico y a la subsistencia de las personas' (párrafo 19). Sugerimos que este costo humano de los ataques a infraestructuras críticas y su impacto en los derechos humanos se mencione de forma directa y clara en el informe*." y *"Apoyamos la recomendación del párrafo 38 que señala que se debe proteger la disponibilidad general o la integridad del núcleo público de Internet, lo cual debería entenderse como una especificación o elaboración más detallada de las normas ya acordadas del Grupo de Expertos Gubernamentales de 2015 para proteger la infraestructura crítica. El núcleo público refiere a los elementos críticos de la infraestructura de Internet, a saber, enrutamiento y reenvío de paquetes, sistemas de asignación de nombres y números, mecanismos criptográficos de seguridad e identidad, medios de transmisión, software y centros de datos".*

***

El 27 de mayo de 2020, el presidente del OEWG publicó[13] una versión revisada del informe preliminar y un documento no oficial actualizado[14] que refleja, según la carta del presidente, las "nuevas propuestas recibidas dentro del tema de la agenda 'Reglas, normas y principios'".[15] Este informe preliminar actualizado y el documento no oficial se analizaron en una reunión virtual que tuvo lugar los días 15, 17 y 19 de junio y 2 de julio de 2020. Según una carta publicada el 16 de julio de 2020 por el Presidente del OEWG y el Representante Permanente de Suiza ante las Naciones Unidas, Embajador Jürg Lauber, el programa para las próximas reuniones informales para debatir el informe preliminar es el siguiente: segunda ronda del 29 de septiembre al 1.º de octubre de 2020; tercera ronda del 17 a 19 de noviembre de 2020; y cuarta ronda del 1.º al 3 de diciembre de 2020.[16]

[12] Estas 12 ONG son las siguientes: Access Now, Asociación para el Progreso de las Comunicaciones, Centro para la Gobernabilidad de las Comunicaciones de la Universidad Nacional de Derecho en Delhi, Derechos Digitales, Fundación Karisma, Global Partners Digital, Red de Acción de Tecnologías de la Información y la Comunicación de Kenia (KICTANet), Centro Internacional de Derecho No Lucrativo (ICNL), R3D: Red en Defensa de los Derechos Digitales, Research ICT Africa, Media Foundation for West Africa, Centro de capacitación informática y estudio digital de la YMCA, Gambia.
[13] https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf
[14] https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-non-paper.pdf
[15] La carta está publicada aquí.
[16] La carta se puede descargar (PDF) aquí.

En la segunda ronda se analizarán cuestiones de derecho internacional; en la tercera se estudiarán las medidas de fomento de la confianza y creación de capacidades; y la cuarta, consistirá en un diálogo institucional periódico y comentarios generales. Después de esto, se prevé que el presidente publique un informe del Borrador Cero (a principios de 2021), que se analizará durante la tercera reunión sustantiva del 8 al 12 de marzo de 2021. A partir de la fecha de la carta del presidente, el plan es que las reuniones informales sean virtuales o híbridas y que la reunión sustantiva sea física.

Grupo de Expertos Gubernamentales (GEG)

No hay ninguna actualización nueva sobre el trabajo del GEG desde la información de nuestro documento del 28 de febrero de 2020.[17]

Participación de la ICANN y próximos pasos

El equipo de Participación Gubernamental (GE) de la organización de la ICANN organizó y copatrocinó una sesión informativa virtual para diplomáticos de las Misiones Permanentes ante las Naciones Unidas el 22 de abril de 2020. La reunión informativa fue copatrocinada por las Misiones Permanentes de Bulgaria y Estonia ante las Naciones Unidas en Nueva York y por la Oficina de las Naciones Unidas en Ginebra. El Director de Tecnologías de la ICANN, David Conrad, y Naela Sarras, Gerenta Sénior, Servicios de la IANA, hablaron e interactuaron con los 116 diplomáticos que participaron. Explicaron la función de la ICANN en el ecosistema de Internet y respondieron las preguntas que presentaron los diplomáticos.

El equipo de Participación Gubernamental de la ICANN continuará siguiendo las deliberaciones en la ONU y publicará las actualizaciones necesarias, según corresponda.

ANEXO 1

Información de referencia sobre la ONU y los Comités de la AGNU

La ONU fue fundada el 24 de octubre de 1945 y ha participado recientemente en debates que incluyen diferentes temas relacionados con Internet. La AGNU ha estado deliberando durante años sobre resoluciones, en el marco de la Primera Comisión y la Segunda Comisión, relativas a la ciberseguridad y la gobernanza de Internet.[18]

[17] https://www.un.org/disarmament/group-of-governmental-experts/

[18] Como se ha explicado anteriormente, las Naciones Unidas no utilizan el término "ciberseguridad", pero nosotros sí lo hacemos a título informativo en el presente documento.

La Primera Comisión de la AGNU[19] es la comisión que históricamente inició el debate de la primera resolución relacionada con el ciberespacio.[20] En 2018, estableció dos grupos de trabajo sobre ciberseguridad: el OEWG[21] y el GEG, que se han analizado en el documento publicado en febrero de 2020.[22]

La Segunda Comisión de la AGNU[23] aborda las cuestiones relacionadas con Internet en el marco de la resolución sobre las Tecnologías de la Información y la Comunicación (TIC) para el desarrollo.[24] Los debates relacionados con la Gobernanza de Internet comenzaron[25] con la resolución A/RES/56/183[26] de la AGNU de 2002 durante la Cumbre Mundial sobre la Sociedad de la Información (CMSI). Esa resolución se actualizó varias veces en 2003 y 2005, en preparación de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) en Ginebra (2003) y Túnez (2005). Entre las fases de la CMSI de Ginebra y Túnez, se estableció un Grupo de Trabajo sobre Gobernanza de Internet (WGIG), que publicó su propio informe.[27]

La CMSI aprobó un documento, la Agenda de Túnez de la CMSI, que ha servido desde 2005 como uno de los documentos clave para explicar (entre muchas otras cuestiones) el modelo de gobernanza de Internet de múltiples partes interesadas.[28]

La Segunda Comisión de la AGNU revisa anualmente la resolución sobre las TIC para el desarrollo. En 2015, también dedicó una cantidad considerable de tiempo a las deliberaciones de la *CMSI+10*, que culminaron con la publicación del Documento Final de la CMSI+10[29] y que culminaron con una reunión de alto nivel de la AGNU los días 15 y 16 de diciembre de 2015.[30] El Documento Final, entre otras cosas, reconfirmó el modelo de gobernanza de Internet de múltiples partes interesadas y prorrogó el Foro de Gobernanza de Internet (IGF) por otro período de diez años.[31]

La Tercera Comisión de la AGNU[32] comenzó investigando el ciberdelito, con una resolución[33] de 2019, que creó el Comité intergubernamental especial de expertos de composición abierta

---

[19] http://www.un.org/en/ga/first/index.shtml
[20] La resolución A/RES/53/70, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, fue propuesta en 1998.
[21] El OEWG es para “los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”.
[22] https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en
[23] https://www.un.org/en/ga/second/index.shtml
[24] Desde 2018, las TIC para el desarrollo sostenible, como se puede ver en el sitio web de la UNCTAD.
[25] La CMSI fue debatida por primera vez por la UIT en su Conferencia de Plenipotenciarios de 1998, y su decisión de celebrar la CMSI fue respaldada por la AGNU en 2001.
[26] https://unctad.org/en/PublicationsLibrary/ares56d183_en.pdf
[27] Puede consultarlo en el Departamento de Estado de EE. UU. o puede descargar el PDF del propio sitio web del WGIG.
[28] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html
[29] El sitio de la ONU no funciona, pero el documento se puede encontrar mediante una búsqueda de su nombre: UNPAN95735.pdf
[30] Sitio web oficial: https://publicadministration.un.org/wsis10/GA-High-Level-Meeting
[31] https://www.intgovforum.org/multilingual/
[32] https://www.un.org/en/ga/third/index.shtml
[33] Puede descargarlo en uno de los idiomas de la ONU aquí.

(OECE) para comenzar a redactar una nueva convención de las Naciones Unidas sobre el ciberdelito.[34]

[34] El nombre completo de este grupo es “comité intergubernamental especial de expertos de composición abierta, representativo de todas las regiones, para elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”.