Política Internacional

ISSN 2707-7330
RNPS: No. 2092
https://rpi.isri.cu/rpi
Vol. VI No. 1 | 2024

rpi@isri.minrex.gob.cu

La necesidad de un marco normativo internacional jurídicamente vinculante para el ciberespacio. Apuntes sobre el debate en las Naciones Unidas

The need for an international legally binding normative framework for cyberspace. Notes on the debate at the United Nations

Lic. Yailin Castro Loredo
Licenciada en Relaciones Internacionales. Especialista del Ministerio de Relaciones Exteriores, La Habana, Cuba.
ycastroloredo@gmail.com 0009-0007-1068-3262

Cómo citar (APA, séptima edición): Castro Loredo, Y. (2024). La necesidad de un marco normativo internacional jurídicamente vinculante para el ciberespacio. Apuntes sobre el debate en las Naciones Unidas. Política Internacional, VI (Nro. 1), 234-242. https://doi.org/10.5281/zenodo.10396402

DOI: https://doi.org/10.5281/zenodo.10396402

RECIBIDO: 19 DE NOVIEMBRE DE 2023 APROBADO: 20 DE DICIEMBRE DE 2023

RESUMEN El desarrollo de las tecnologías de la información y las comunicaciones tiene un impacto cada vez mayor en todas las esferas de la sociedad y, por tanto, en el comportamiento y la seguridad de las naciones. Su cada vez más creciente uso para incitar la violencia, la subversión y desestabilización, la difusión de noticias falsas, y realizar ataques cibernéticos, ha favorecido la militarización del ciberespacio. Mientras los conflictos tradicionales en el medio terrestre cuentan con un marco legal aplicable desde el Derecho Internacional, el ciberespacio, aún no cuenta con un marco normativo internacional vinculante, lo que refuerza la necesidad de su elaboración. Ello ha hecho que el tema se convierta en una prioridad de política exterior de las principales potencias y un tema de debate y relevancia para la política internacional, en particular en el marco de las Naciones Unidas.

Palabras claves: tecnologías de la información y las comunicaciones, ciberseguridad, ciberataque, seguridad internacional, relaciones internacionales, multilateralismo

ABSTRACT The development of information and communication technologies has a growing impact on all areas of society and therefore on the behavior and security of nations. It is increasingly used to incite violence, subversion and destabilization, spread false news, and carry out cyberattacks, which has favored the militarization of cyberspace. While traditional conflicts on the earth have a legal framework applicable under international law, cyberspace does not yet have a binding international framework, which reinforces the need for its elaboration. This has made the issue a foreign policy priority of the major powers and a topic of debate and relevance to international politics, particularly within the framework of the United Nations.

Keywords: information and communication technologies, cybersecurity, cyberattack, international security, international relations, multilateralism

INTRODUCCIÓN

El creciente desarrollo y uso de las tecnologías de la información y las comunicaciones (TIC) tiene un impacto cada vez mayor en todas las esferas de la sociedad. Las TIC representan un catalizador del progreso de las sociedades, ofreciendo ventajas para el desarrollo socioeconómico de nuestros países y creando nuevos espacios de cooperación.

Sin embargo, no se puede desconocer que a medida que estas se han desarrollado, se ha ampliado su doble uso. El uso del ciberespacio se ha extendido de manera exponencial en el ámbito militar y civil, con un impacto significativo en las infraestructuras críticas nacionales y la seguridad de las naciones.

Las amenazas derivadas del uso malicioso de las TIC son también crecientes y de naturaleza cambiante, lo que se ha convertido en una preocupación para los Estados y uno de los retos a enfrentar debido a las amenazas derivadas para la paz y la seguridad internacionales.

Actualmente, el uso malicioso de las TIC y de las plataformas de los medios de comunicación, incluidas las redes sociales, se ha convertido en un problema global. Mientras los conflictos tradicionales en el medio terrestre cuentan con marco jurídico aplicable desde el Derecho Internacional, el ciberespacio aún no cuenta con un marco normativo que permita hacer frente a los nuevos desafíos que genera el uso malicioso de las TIC.

La ciberseguridad es una de las prioridades de las principales potencias en el escenario multilateral en materia de seguridad internacional y se ha convertido en un tema complejo de debate permanente en la agenda de la Organización de Naciones Unidas.

En ese contexto, el presente trabajo tiene por objetivo analizar la relevancia del tema en la agenda de las Naciones Unidas y la necesidad de un marco normativo internacional jurídicamente vinculante que regule las actividades en el ciberespacio.

DESARROLLO

Consenso vs confrontación

Si bien las Naciones Unidas consideró la función de la ciencia y la tecnología en el contexto de la seguridad internacional desde los años 70 y 80, reconociendo que los avances científicos y tecnológicos podían tener aplicaciones civiles y militares, no fue hasta el año 1998 que los avances en la esfera de la información y las comunicaciones en el contexto de la seguridad internacional se consideró en la Primera Comisión de la Asamblea General de las Naciones Unidas (AGNU), dedicada a los temas de desarme y seguridad internacionales.

La primera resolución sobre el tema fue promovida por la Federación de Rusia en 1998. El texto expresó preocupación ante la posibilidad de que estos

medios y tecnologías se utilicen con fines incompatibles con el objetivo de garantizar la estabilidad y la seguridad internacionales y afecten negativamente a la seguridad de los Estados y solicitó el examen multilateral de los peligros actuales y posibles en el ámbito de la seguridad de la información (ONU, 1999).

En sus inicios, esta problemática emergió como un tema de consenso, y la resolución presentada fue adoptada sin votación, como reflejo de la voluntad de los principales actores del sistema internacional y una demanda de los países en desarrollo de atender este tema emergente. Sin embargo, no fue hasta el año 2004 que se aprueba la creación de un grupo de expertos gubernamentales (GGE, por sus siglas en inglés) que asistiría al Secretario General de las Naciones Unidas en el examen de las amenazas reales y potenciales en el ámbito de la seguridad de la información, y las posibles medidas de cooperación para enfrentarlas.

Teniendo en cuenta la ausencia de normas internacionales multilateralmente acordadas para regular el uso del ciberespacio, desde inicios de los años 2000 se dio un impulso a los debates sobre el tema en el marco de Naciones Unidas.

El primer GGE sesionó en 2004, sin alcanzar un acuerdo en relación con el mandato otorgado y la adopción de un informe final, dadas las contradicciones que ya emergían en el tema entre Rusia-Estados Unidos-China. Esto conllevó a que luego de ocho años de haberse considerado por primera vez el tema en la Asamblea General de las Naciones Unidas, Estados Unidos (EE.UU.) votó en solitario en contra del proyecto de resolución ruso, rompiendo el tradicional consenso en la Asamblea General de las Naciones Unidas.

A pesar del fracaso del primer GGE, tras la presión de EE.UU. y los países occidentales, se convocó un segundo grupo, que sesionó en 2009 y pudo presentar su primer informe sobre el tema a la AGNU en el 2010. Este reconoció que las amenazas reales y potenciales en la esfera de la seguridad de la información constituían algunos de los problemas más graves del siglo XXI, y que se derivaban de una amplia gama de fuentes y se manifiestan como actividades desestabilizadoras dirigidas por igual contra particulares, empresas, elementos de la infraestructura nacional y gobiernos, cuyos efectos entrañan considerables riesgos para la seguridad pública, la seguridad de las naciones y la estabilidad de la comunidad internacional en su conjunto. (ONU, 2010)

Sin embargo, este informe no fue ambicioso ni abarcador, solo se limitó a elaborar un conjunto de recomendaciones encaminadas a examinar las normas relativas al uso de las tecnologías de la información y las comunicaciones por los Estados; adoptar medidas de fomento de la confianza; determinar qué medidas de apoyo a la creación de capacidad en los países menos adelantados podrían adoptarse; y examinar las posibilidades de elaborar términos y definiciones comunes.

En el año 2013 sesionó otro grupo de expertos gubernamentales, cuyo informe final reflejó la conclusión del Grupo de que el derecho internacional, y en particular la Carta de las Naciones Unidas, son aplicables y esenciales para mantener la paz y la estabilidad y para promover un entorno abierto, seguro, pacífico y accesible para las tecnologías de la información y las comunicaciones. La soberanía del Estado y las normas y los principios internacionales que emanan de ella son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por parte de los Estados y a su jurisdicción sobre la infraestructura de tecnologías de la información y las comunicaciones dentro de su territorio. (ONU, 2013). Dichos temas pasarían a centrar el debate en la materia y serían desde ese momento, el punto de mayor confrontación.

Desde el GGE que sesionó en 2013, se comenzó a apreciar una tendencia por parte de EE.UU. y países europeos miembros del grupo, de introducir cuestiones asociadas a los derechos humanos y el derecho internacional humanitario, así como legitimar el uso de la fuerza en el ciberespacio mediante el

reconocimiento de la aplicación automática del artículo 51 de la Carta de las Naciones Unidas.

Nuevamente, en 2015, sesionó un GGE, que en su informe final estableció una serie de normas, reglas y principios de comportamiento responsable de los Estados, que serían la base para futuras discusiones en las Naciones Unidas.

Hasta la fecha, han sesionado seis GGE (2004, 2010, 2013, 2015, 2017, 2021). Excepto el de 2017, que tampoco alcanzó consenso, los otros GGE acordaron un conjunto de reglas, normas y principios de comportamiento de los Estados, que fueron los pasos iniciales de un complejo debate en la actualidad.

Debe señalarse que los GGE han sido mecanismos poco efectivos teniendo en cuenta su composición limitada y la casi nula posibilidad del resto de los Estados Miembros de incidir en las recomendaciones de dichos expertos. En la práctica, se ha convertido en un mecanismo que intenta legitimar los intereses de un grupo reducido de países sobre la mayoría de los Estados Miembros de las Naciones Unidas.

Teniendo en cuenta lo anterior, los países en desarrollo, fundamentalmente miembros del Movimiento de Países No Alineados, comenzaron a exigir a los promotores del tema la creación de un grupo de composición abierta donde todos los Estados pudieran debatir en igualdad de condiciones.

No fue hasta el año 2018 que se materializó esta aspiración, cuando hubo un punto de inflexión en la consideración del tema. Tras años de trabajo conjunto entre Rusia y EE.UU., se evidenció una ruptura entre estos, reflejo de la nueva política exterior del gobierno de Donald Trump. En consecuencia, EE.UU. dejó de apoyar el proyecto de resolución que presentaba Rusia y promoviendo en su lugar uno propio para convocar a un nuevo Grupo de Expertos Gubernamentales, tras el fracaso del que sesionó en 2017.

Se abrió así en las Naciones Unidas una nueva etapa de confrontación en la consideración del tema de la cual emergieron dos procesos paralelos: un grupo de expertos gubernamentales liderado por EE.UU. y un grupo de trabajo de composición abierta promovido por Rusia.

En este contexto, la Asamblea General de las Naciones Unidas adoptó dos resoluciones con objetivos y modalidades contrapuestas para hacer frente a las ciber amenazas. Rusia se vio obligada a convocar un Grupo de trabajo de composición abierta de la Asamblea General (GTCA), teniendo en cuenta que la propuesta de EE.UU. incluía la creación de un GGE, que hasta el momento había sido promovido por Rusia. Esta nueva propuesta rusa de un GTCA, sería el primero de su tipo en la Organización, para estudiar, entre otras cosas, normas, reglas y principios de comportamiento responsable de los Estados en el ciberespacio. Por otro lado, la resolución de Estados Unidos llamaba a la creación de un nuevo grupo de expertos gubernamentales que se ocupara de la aplicabilidad del Derecho Internacional para enunciar acciones en el ciberespacio e identificar mecanismos para garantizar el cumplimiento de las normas adoptadas por los GGE anteriores. Esta iniciativa de EE.UU. enfocaba las prioridades en la materia hacia la aplicación del Derecho Internacional en el ciberespacio.

Ante la falta de acuerdo, Naciones Unidas asumió dos procesos paralelos, cuya conclusión en 2021, demostró que no era posible establecer complementariedad entre ambos mientras existieran las pugnas entre las principales potencias.

Convergencias y divergencias en el reto que supone la ciberseguridad

En el contexto del aniversario por los 75 años de creada la Organización de Naciones Unidas, los Estados miembros se dieron a la tarea de identificar los principales retos y desafíos para los próximos años en el sistema internacional y el contexto multilateral, siendo uno de ellos: el uso de las TIC y la ciberseguridad.

En la Declaración aprobada en este aniversario, los Estados Miembros acordaron que hay que aprovechar al

máximo el instrumental diplomático de la Carta, para prevenir el estallido, la escalada y la reanudación de hostilidades por tierra y mar, y en el espacio ultraterrestre y el ciberespacio. (...) Las tecnologías digitales han transformado profundamente la sociedad y generan oportunidades sin precedentes y nuevos desafíos. Cuando se utilizan de manera impropia o maliciosa, pueden fomentar las divisiones dentro de los países y entre ellos, aumentar la inseguridad, socavar los derechos humanos y exacerbar la desigualdad. Forjar una concepción común de la cooperación digital y un futuro digital que muestre todas las posibilidades que ofrece el uso beneficioso de la tecnología, y abordar las cuestiones de confianza y seguridad digitales, debe seguir siendo una prioridad, pues nuestro mundo depende hoy más que nunca de las herramientas digitales para mantener la conectividad y la prosperidad socioeconómica. Las tecnologías digitales tienen el potencial de acelerar la realización de la Agenda 2030 y debemos garantizar un acceso digital seguro y asequible para todos. Las Naciones Unidas pueden brindar una plataforma para que todos los interesados participen en esas deliberaciones. (ONU, 2020)

En ese contexto, las Naciones Unidas otorgaron gran prioridad al debate gubernamental sobre la ciberseguridad. Incluso durante los dos años de mayor impacto de la pandemia de la COVID-19 (2020-2021), donde se pausaron procesos vinculados al desarme y la seguridad internacional, tanto el GGE como el GTCA continuaron sus labores.

Mientras el grupo de expertos gubernamentales convocado por Estados Unidos continúo debatiendo los temas abordados por los GGE anteriores, el Grupo de Trabajo de Composición Abierta marcó un hito histórico en la consideración de los temas asociados a la ciberseguridad en Naciones Unidas. Por primera vez, los Estados Miembros contaron con un mecanismo inclusivo, transparente, donde todos podían exponer sus posiciones y preocupaciones en igualdad de condiciones. De este GTCA emergió el primer documento de Naciones Unidas sobre el tema adoptado por consenso, que, si bien no incluyó todos los temas en debate, representó un delicado balance entre las diferentes posiciones existentes, incluyendo la necesidad de continuar debatiendo sobre futuras normas vinculantes.

Sin embargo, fue un período importante de debate y reflexión, donde se apreciaron las divergencias y convergencias en el tema, ante el reto y desafío que representan la ciberseguridad. Los principales temas de debate han sido las amenazas reales y potenciales, las reglas, normas y principios de comportamiento responsable de los Estados, la aplicación del Derecho Internacional, la creación de capacidades, las medidas de fomento de la confianza y el diálogo regular institucional para definir los pasos futuros.

Si bien los Estados han alcanzado consenso sobre las principales amenazas que se derivan del uso malicioso de las TIC, su uso con fines militares; el debate ha sido complejo en cuanto a las afectaciones a las infraestructuras nacionales. Si bien la mayoría de los países coinciden en que estas infraestructuras son definidas por cada gobierno, Estados Unidos y un grupo de países occidentales, con el apoyo del Comité Internacional de la Cruz Roja, insisten en asociar las afectaciones a las infraestructuras críticas, incluidas las infraestructuras informáticas, a la aplicación automática del Derecho Internacional Humanitario, sin que se haya alcanzado aún un consenso al respecto.

Por otra parte, persisten diferencias sobre la atribución y la responsabilidad internacional ante un incidente cibernético. Mientras un grupo de países desarrollados insisten en aplicar una atribución política, Rusia, China y un grupo de países en desarrollo, incluyendo Cuba, no respaldan este término, teniendo en cuenta que no existe un mecanismo multilateral que permita identificar los responsables, basado en las evidencias técnicas; al tiempo que todos los Estados no cuentan con las mismas capacidades para hacer frente a este tipo de amenazas.

En cuanto al debate sobre las reglas, normas y principios de comportamiento responsable de los Estados, prevalece un acuerdo sobre el reconocimiento a las ya acordadas por los grupos de expertos, pero los

países que no han participado en estos grupos de composición limitada reclaman que se revisen y propongan nuevas normas.

Sin dudas, el tema más complejo, y donde menos se ha podido avanzar en los debates, radica en la aplicación automática del Derecho Internacional. Las discusiones en la materia han demostrado el peligro que representa la ausencia de un instrumento internacional para el uso del ciberespacio. Los países occidentales quieren hacer predominar su visión sobre la aplicación del Derecho Internacional y la Carta de las Naciones Unidas (ONU) a las actividades en este medio. La imposición de interpretaciones sobre la legítima defensa y los intentos por equiparar el concepto de ataque armado tradicional, refrendado en la Carta de la ONU y que aplica a los conflictos tradicionales a un ciberataque, complejiza los debates en los foros multilaterales e imposibilita alcanzar un consenso.

El punto más importante de controversia ha sido el desacuerdo sobre la aplicabilidad del DIH al ciberespacio, lo que, hasta el momento, no ha podido incluirse explícitamente en los documentos de Naciones Unidas sobre el tema. Los países occidentales intentan legitimar en el ciberespacio el uso del artículo 51 de la Carta de la ONU sobre el derecho a la legítima defensa, mediante la aplicación del derecho de la guerra a un medio donde la mayoría de los Estados abogan por su no militarización y su uso estrictamente pacífico.

En ese sentido, las posiciones sobre la necesidad de un instrumento internacional jurídicamente vinculante han estado divididas. Si bien un grupo de países considera que las actividades en este medio deben estar reguladas de forma vinculante, otro grupo considera que las normas no vinculantes de comportamiento responsable de los Estados son suficientes para abarcar los vacíos legales en la materia.

La ciberseguridad: una prioridad de las principales potencias

Debido a las diferencias entre Rusia y EE.UU., y este último con China, la ciberseguridad ha ocupado un papel importante entre sus prioridades nacionales, lo que se evidencia en sus proyecciones en Naciones Unidas y en el escenario internacional.

La Estrategia Nacional de Ciberseguridad de EE.UU., publicada en septiembre de 2018 durante la administración de Donald Trump, tras 15 años respecto de la anterior, estableció su compromiso con una competencia estratégica a largo plazo con China y Rusia, destacando que dichos países habían ampliado sus competencias para incluir campañas persistentes en y a través del ciberespacio, lo que representa un riesgo estratégico a largo plazo para EE.UU., sus aliados y socios. En el documento se define la dependencia del dominio cibernético para el país y el riesgo que esto representa. Asimismo, el reconocimiento por parte de EE.UU. de sus capacidades militares en el ciberespacio para prepararse para un conflicto armado abrió un nuevo capítulo por la lucha de poder y el liderazgo en el tema en Naciones Unidas. (White House, 2018)

Antes de que finalizara en 2021 el GTCA, Rusia, para garantizar su liderazgo en el tema y darle continuidad al proceso, presentó un nuevo proyecto de resolución, que tenía como objetivo crear otro Grupo de Trabajo que sesionaría de 2021 a 2025. Dicha propuesta fue aprobada, pero encontró el rechazo de EE.UU. y los países europeos, quienes votaron en contra de la resolución.

China, por su parte, ha promovido también la creación del GTCA, así como la iniciativa de los Estados Miembros de la Organización de Cooperación de Shanghái sobre un "Código Internacional de Conducta para la Seguridad de la Información". De igual forma, en 2020 China presentó a la Asamblea General la "Iniciativa Global sobre Seguridad de Datos".

Los dos años de trabajo en un período de pandemia, y la posterior llegada del gobierno de Joe Biden en los Estados Unidos, permitió el acomodo de los intereses de las principales potencias en Naciones Unidas, para que ambos procesos culminaran con un resultado final. En el 2021, tras un acuerdo bilateral entre Rusia y

EE.UU., se regresó a un texto conjunto para reconocer el resultado de las labores tanto del GGE como del GTCA que había culminado, retomándose el consenso en sobre el tema en las Naciones Unidas.

De igual forma, la Estrategia Nacional de Ciberseguridad publicada en 2023 por la Administración Biden, incluye una visión completamente politizada de la cuestión, al establecer que los gobiernos de China, Rusia, Irán, Corea del Norte y otros "estados autocráticos" están utilizando agresivamente capacidades cibernéticas avanzadas para perseguir objetivos que van en contra de sus intereses y normas internacionales ampliamente aceptadas. Concluía además que el temerario desprecio de estos por el Estado de Derecho y los derechos humanos en el ciberespacio amenazan la seguridad nacional y la prosperidad económica de Estados Unidos. (White House, 2023). En esta Estrategia, China es representada ahora la más amplia, activa y persistente amenaza para la seguridad de los Estados Unidos en materia de ciberseguridad.

Asimismo, el componente bélico de las actividades en el ciberespacio promovido por Estados Unidos también ha ido cobrando mayor fuerza en las políticas de la Organización del Tratado del Atlántico Norte (OTAN, por sus siglas en inglés), donde la ciberdefensa representa un desafío de suma importancia en la renovación de la Alianza y en su adaptación a las nuevas amenazas. La OTAN ha incluido la ciberdefensa como una primera línea potencial en caso de un conflicto. De este modo, se unirá a la tierra, mar y aire como dominio operacional esencial ante cualquier incidente o guerra internacional. El nuevo plan estratégico de la OTAN para librar las futuras batallas en el campo digital, se incluye distintos parámetros y factores en los que los distintos países miembros deben ir avanzando para garantizar un alto nivel defensivo.

Al margen de estos procesos, las potencias han continuado promoviendo sus intereses en otros espacios. Los países europeos, con el apoyo de Estados Unidos, lograron la adopción en la Primera Comisión de la Asamblea General en 2022, de una resolución que mandata el establecimiento de un Programa de Acción sobre Ciberseguridad bajo los auspicios de Naciones Unidas, como una alternativa paralela al Grupo promovido por Rusia.

De igual forma, el Convenio de Budapest, iniciativa europea adoptada fuera de Naciones Unidas sobre la ciberdelincuencia, se intenta elegir como paradigma en el tema, mientras que Rusia con el apoyo de China y otros países en desarrollo, trabajan en la adopción de una Convención Internacional para la Cooperación en materia delitos cibernéticos, que es rechazada por los países occidentales.

La existencia de todas estas iniciativas de forma paralela y la imposibilidad de avanzar en alguna de ellas de forma conjunta, evidencia las grandes divergencias existentes entre las principales potencias en la materia y cómo estas se han trasladado a los espacios multilaterales.

CONCLUSIONES

El desarrollo de las tecnologías de la información y las comunicaciones tiene un impacto cada vez mayor en todas las esferas de la sociedad y, por tanto, en el comportamiento de las naciones. Su uso malicioso, con fines delictivos y desestabilizadores, lo ha convertido en uno de los temas prioritarios de los debates internacionales, y un punto permanente en la agenda de las Naciones Unidas.

Actualmente la ciberseguridad es uno de los temas más complejos que se debaten en la Organización, donde las divisiones y polarizaciones son evidentes, delineándose un grupo de países que promueven compromisos vinculantes que regulen la conducta de los Estados en el ciberespacio, mientras que otro grupo, en su mayoría países occidentales, intentan avanzar con normas y reglas no vinculantes.

Los debates internacionales sobre el tema han demostrado el peligro que representa la ausencia de un instrumento internacional jurídicamente vinculante

para el uso del ciberespacio y los intentos de polos de poder occidentales de imponer sus entendidos sobre la legítima defensa, así como sus intentos por equiparar el concepto de ataque armado tradicional refrendado en la Carta de la ONU a un ciberataque, legitimando así el uso de la fuerza. En ese sentido, Estados Unidos se destaca como uno de los grandes líderes a nivel internacional, con una visión belicista y con el claro objetivo de imponer su visión hegemónica.

El estado actual de los debates sobre el tema refuerza la necesidad de un instrumento internacional jurídicamente vinculante que regule el comportamiento de los diferentes actores en este medio. La ausencia de una terminología común a emplear sobre el ciberespacio, y de un mecanismo para determinar la atribución o responsabilidad internacional por un ciberataque, temas que pueden ser fácilmente manipulados según los intereses políticos, hace que, los países en desarrollo presentan las mayores desventajas al no contar con un marco legal que los proteja, o las capacidades técnicas necesarias para hacer frente a un ataque cibernético.

La consideración del tema en las Naciones Unidas, los mecanismos de seguimiento y los contenidos asociados, responden a los intereses de los principales actores del sistema internacional: China, Rusia y EE.UU., por lo que se vislumbra que siga siendo un tema de constante debate en la agenda de la Organización y una prioridad en el sistema multilateral.

No obstante, la posibilidad de alcanzar un instrumento internacional jurídicamente vinculante no parecería ser la alternativa más probable al corto o mediano plazo.

REFERENCIAS BIBLIOGRÁFRICAS

ONU. (1999). Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. Resolución de Naciones Unidas A/RES/53/70, 1999, pp.2.

ONU. (2010). Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. Informe A/65/21 de Naciones Unidas, 2010, pp.2.

ONU. (2013). Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. Informe A/68/98 de Naciones Unidas, 2013, pp.3.

ONU. (2020). Declaración sobre la conmemoración del 75º aniversario de las Naciones Unidas. Resolución A/RES/75/1 de Naciones Unidas.

White House. (2018). National Cyber Strategy of the United States of America.

White House. (2023). National Cyber Strategy of the United States of America.

BIBLIOGRAFÍA

Aguilar, J. (2002). La gestión del Conocimiento en la Comunicación: Un enfoque Tecnológico y de Gestión de Contenidos. Madrid: Universidad Complutense de Madrid.

Aguilar, J. (2003). Historia de la Sociedad de la Información. Hacia la sociedad del Conocimiento" en Revolución tecnológica. Alicante: Universidad de Alicante.

Bejerano, S. E. (2021). La ciberseguridad, el ciberespacio, Internet y las tecnologías de la información y las comunicaciones. La Habana.

Cuba. (2019). Documento de Trabajo al Grupo de Trabajo sobre Ciberseguridad. La Habana, Cuba. MINREX: Archivo pasivo del GTCA.

Cuba. (2021). Decreto Ley No.35 "De las Telecomunicaciones, las Tecnologías de la Información y la Comunicación y el uso del Espectro. La Habana .

Hernández, L. E. (2017). Un siglo de teoría de las relaciones internacionales. Selección de temas y lecturas

diversas. La Habana: Instituto Superior de Relaciones Internacionales.

Merced, R. G. (2006). El uso del ciberespacio: consideraciones éticas y legales. Cuaderno de Investigación en la Educación, Número 21, pp. 103-116.

Niazi, Z. (2021). Cyber Space Regulation and the International Humanitarian Law . Pakistan Review of Social Sciences.

ONU. (1999). Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional. Resolución de Naciones Unidas A/RES/53/70, 1999, pp.2.

ONU. (2010). Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. Informe A/65/21 de Naciones Unidas, 2010, pp.2.

ONU. (2013). Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. Informe A/68/98 de Naciones Unidas, 2013, pp.3.

ONU. (2020). Declaración sobre la conmemoración del 75º aniversario de las Naciones Unidas. Resolución A/RES/75/1 de Naciones Unidas.

Reaching Critical Will. (2019). Cyber Peace & Security Monitor, Vol. 1, No. 1.

Reaching Critical Will. (2019). Cyber Peace & Security Monitor, Vol. 1, No. 2.

Reguera, J. (2015). Aspectos legales en el Ciberespacio. La ciberguerra y el Derecho Internacional Humanitario. Revista Análisis GESI, 7/2015.

UNODA. (s.f). Documents and Statements of the Open-ended Working Group on security of and in the use of information and communications technologies. Loclizado en https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021

White House. (2018). National Cyber Strategy of the United States of America.

White House. (2023). National Cyber Strategy of the United States of America.

CONFLICTO DE INTERESES

La autora declara que no existen conflictos de intereses relacionado con el artículo.