VIII Conferencia de Estudios Estratégicos

"Transformando el orden internacional: desafíos de la transición y propuestas desde el Sur"

27- 29 de septiembre de 2023

PONENCIA

Tema: La ciberseguridad en el contexto de las Naciones Unidas

Autor: Lic. Yailin Castro Loredo

Institución: Ministerio de Relaciones Exteriores

País: Cuba

Resumen: El desarrollo de las tecnologías de la información y las comunicaciones (TIC) tiene un impacto cada vez mayor en todas las esferas de la sociedad y, por tanto, en el comportamiento de las naciones. Si bien han aportado avances, su uso malicioso de las ha favorecido al promover el discurso de odio, la violencia, la subversión y desestabilización, la difusión de noticias falsas, así como a la proliferación de ataques cibernéticos y una creciente militarización del ciberespacio. Mientras los conflictos tradicionales en el medio terrestre cuentan con un marco desde el Derecho Internacional aplicable, el ciberespacio, aún no cuenta con un marco normativo internacional aplicable, lo que dificulta entre otros elementos, determinar la responsabilidad ante actos indebidos y por tanto la atribución. 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.

Introducción:

Las tecnologías de la información y las comunicaciones tienen un impacto cada vez mayor en el desarrollo de las naciones. Sin embargo,

sus usos maliciosos han traído preocupaciones a los países ya que podrían generar problemas para la paz y la seguridad internacionales.

El uso del ciberespacio se ha extendido de manera exponencial en el ámbito militar y civil, con un impacto significativo en las infraestructuras críticas y la seguridad nacionales. El uso malicioso de las TIC ha favorecido al promover el discurso de odio, la violencia, la subversión y desestabilización, la difusión de noticias falsas, así como a la proliferación de ataques cibernéticos y una creciente militarización del ciberespacio.

Al propio tiempo, del uso creciente del ciberespacio, se han derivado otras preocupaciones desde el punto de vista legal y ético. Mientras los conflictos tradicionales en el medio terrestre cuentan con un marco aplicable y sólido desde el Derecho Internacional, el ciberespacio, no cuenta con ningún marco normativo jurídicamente vinculante que regule el comportamiento en este medio.

En un contexto internacional marcado por pugnas y luchas de poder entre las grandes potencias, el ciberespacio constituye una de las prioridades en materia de seguridad en la política exterior de estas y un tema de debate y relevancia en el ámbito de Naciones Unidas.

Desarrollo:

El avance en la esfera de la información y las comunicaciones en el contexto de la seguridad internacionales fue introducido en la agenda de la Organización de Naciones Unidas en 1998, a solicitud de Rusia y con el apoyo de China y Estados Unidos. Por considerarse una cuestión de paz y seguridad internacionales, se consideró en la Primera Comisión de las Naciones Unidas que se centra en los temas de desarme y seguridad internacionales.

En un órgano donde se veían hasta el momento, los avances o temas de interés vinculados a los armamentos y medios tradicionales, el ciberespacio emergió como tema de consenso y su primera resolución se adoptó sin votación como reflejo de la voluntad política de los principales actores del sistema internacional en atender cuestiones emergentes con impacto en la seguridad nacional de los Estados.

Si bien se mantuvo en la agenda de la Asamblea General de las Naciones Unidas año tras año con pocas modificaciones en el texto a adoptar, no fue hasta el año 2004 que se institucionalizó el debate multilateral mediante la creación de un Grupo Expertos Gubernamentales (GGE, por sus siglas en inglés) para examinar las amenazas existentes y potenciales en el ámbito cibernético y las posibles medidas de cooperación para hacerle frente.

Hasta la fecha, han sesionado seis GGE (2004, 2010, 2013, 2015, 2017, 2021). El primer GGE no pudo alcanzar consenso en torno a un documento final dadas las contradicciones que ya emergían en el tema entre Rusia-Estados Unidos-China. Excepto el de 2017 que tampoco alcanzó consenso, los otros GGE cordaron un conjunto de reglas, normas y principios de comportamiento de los Estados, que fueron los pasos iniciales de un complejo debate en la actualidad.

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. Es 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, en particular 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 reflejo de la política exterior del nuevo gobierno de Donald Trump, donde EE.UU. dejó de apoyar el proyecto de resolución que presentaba Rusia y lazó su propio proyecto de resolución para convocar un nuevo Grupo de Expertos Gubernamentales tras el fracaso del de 2017.

En noviembre de 2018, la Asamblea General de las Naciones Unidas adoptó dos resoluciones 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), primero de su tipo en la Organización, que 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.

Ante la falta de acuerdo entre estos dos países, 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 potencias. Ambos procesos sesionaron en 2020 y 2021. Mientras el GGE convocado por Estados Unidos continúo debatiendo los temas de los Grupos de Expertos Gubernamentales 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 primero 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.

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

Los dos años de trabajo en un período de pandemia, y con la posterior llegada de un nuevo gobierno en los Estados Unidos con la Administración Biden, 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 el tema en las Naciones Unidas.

A pesar de las concesiones realizadas por Rusia para mantener el compromiso de los países occidentales con el nuevo GTCA que comenzó sus labores a finales de 2021, este grupo ha sido secuestrado por estos países, que con iniciativas sin consenso han intentado frenar las discusiones sustantivas para demostrar que es un proceso sin éxito.

Al margen de estos procesos, las potencias han continuado promoviendo sus intereses en otros espacios. Los países europeos con el apoyo de Estados Unidos han comenzado a promover un Programa de Acción sobre Ciberseguridad bajo los auspicios de Naciones Unidas como una alternativa paralela al Grupo promovido por Rusia. 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.

Los debates internacionales sobre el tema han demostrado el peligro que representa la ausencia de un instrumento internacional para el uso del ciberespacio. Los países occidentales quieren imponer su visión sobre la aplicación del Derecho Internacional y la Carta de la ONU a las actividades en este medio. La imposición de entendidos 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 que, hasta el momento, no ha podido incluirse explícitamente en los documentos de Naciones Unidas sobre el tema. Los países occidentales intentan legitimar el uso del artículo 51 de la Carta de la ONU sobre el derecho a la legítima defensa en el ciberespacio, para legitimar de esta forma el uso de la fuerza ante un ciberataque.

Las discusiones en curso sobre ciberseguridad en el marco de las Naciones Unidas son reflejo de las contradicciones entre las principales potencias. Tanto la Estrategia Nacional de Ciberseguridad lanzada por la Administración Trump en 2018 como la de la Administración Biden, de marzo de 2023 consideran el ciberespacio como medio de conflicto y lo definen como amenaza a la seguridad nacional en el ciberespacio a China y Rusia.

En ese sentido, Estados Unidos se destaca como uno de los grandes líderes en la materia a nivel internacional, con el claro objetivo de imponer su visión hegemónica y ejercer influencia sobre el resto del mundo, lo que se evidencia en el plano multilateral.

El componente bélico de las actividades en el ciberespacio promovido por Estados Unidos también ha ido cobrando mayor fuerza en las políticas de la OTAN, 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 incluyen distintos parámetros y factores en los que los distintos países miembros deben ir avanzando para garantizar un alto nivel defensivo.

Este contexto, 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.

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, convirtiéndolo en uno

de los temas prioritarios de los debates internacionales, y un punto permanente en la agenda de las Naciones Unidas.

Actualmente 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 mientras que otro grupo, en su mayoría países occidentales intentan avanzar con normas y reglas no vinculantes que regulen la conducta de los Estados en el ciberespacio.

Los debates internacionales sobre el tema han demostrado el peligro que representa la ausencia de un instrumento internacional para el uso del ciberespacio y los intentos de polos de poder occidentales de imponer sus entendidos sobre la legítima defensa y sus intentos por equiparar el concepto de ataque armado tradicional refrendado en la Carta de la ONU a un ciberataque.

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.

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.

Blanca, L. C. (2018). *Estrategia Nacional de Ciberseguridad de los Estados Unidos de América.*

Cuba. (2019). *Documento de Trabajo al Grupo de Trabajo sobre Ciberseguridad.* La Habana, Cuba.

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). *· Guzmán Merced, Rosa. (2006). El uso del ciberespacio: consideraciones éticas y legales.* Cuaderno de Investigación en la Educación.

Naciones Unidas. (s.f.). *Grupo de Trabajo de Composición Abierta de la Asamblea General sobre avances en la esfera de la información y las comunicaciones en el contexto de la seguridad internacional.*

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

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.*

Unidas, N. (2020). *Declaración sobre la conmemoración del 75º aniversario de las Naciones Unidas.* Nueva York.

Unidas, N. (2021). *Final Substantive Report of the OEWG.* Nueva York.