RELACIONES INTERNACIONALES

Implicaciones y desafíos del ciberespacio para la aplicación del Derecho Internacional

Implications and Challenges of Cyberspace for the Application of International Law

Valencia Corozo, Emilio Horacio

Emilio Horacio Valencia Corozo
emiliohoracio1@hotmail.com
Vice-Cónsul de la embajada de Ecuador en La Habana, Cuba

Política Internacional
Instituto Superior de Relaciones Internacionales "Raúl Roa García", Cuba
ISSN: 1810-9330
ISSN-e: 2707-7330
Periodicidad: Trimestral
vol. 6, núm. 1, 2024
politicainternacionaldigital@gmail.com

Recepción: 01 Noviembre 2023
Aprobación: 10 Diciembre 2023

URL: http://portal.amelica.org/ameli/journal/332/3324791018/

Resumen: La aplicación del derecho internacional en el ciberespacio es un tema cada vez más relevante, debido al avance tecnológico y la creciente dependencia de la sociedad del mundo digital. El presente artículo busca analizar cómo se aplica el derecho internacional en este ámbito y determinar sus principales implicaciones en la esfera digital. Los hallazgos muestran que este es un tema complejo, en constante evolución, en el cual existen diferentes enfoques y perspectivas. Algunos defienden la necesidad de adaptar y actualizar el derecho internacional existente a las particularidades del ciberespacio, mientras que otros abogan por la creación de un marco legal específico para regular las actividades en línea. Se concluye que el derecho internacional tiene un papel fundamental a desempeñar en la regulación y la aplicación de normas en el ciberespacio, lo cual requiere además de una mayor cooperación y coordinación a nivel internacional.

Palabras clave: Ciberseguridad, Privacidad, Jurisdicción, Derecho internacional, Cooperación internacional.

INTRODUCCIÓN

El contexto de la aplicación del derecho internacional en el ciberespacio se desarrolla en un entorno digital globalizado y en constante evolución. El ciberespacio se ha convertido en una dimensión fundamental de la sociedad moderna, donde se llevan a cabo diversas actividades, como la comunicación, el comercio electrónico, la banca en línea, el entretenimiento y la interacción social (Hypponen, 2022). Sin embargo, este entorno digital también ha dado lugar a una serie de problemas que requieren una atención especial desde la perspectiva del derecho internacional. Uno de los principales retos es que las actividades en línea no están limitadas por las fronteras geográficas, lo que plantea dificultades para la aplicación de las leyes nacionales tradicionales (Schmitt, 2022).

En este marco, también es un desafío determinar quién es responsable de las acciones ilegales en el ciberespacio, aspecto que resulta complicado debido, entre otros elementos, a la capacidad de ocultar la identidad y la ubicación física mediante el uso de tecnologías de anonimato y técnicas de hacking sofisticadas. Otro aspecto importante del contexto es el conflicto de normas y regulaciones. Dado que el ciberespacio es un entorno transnacional, diferentes países tienen diferentes marcos legales y regulaciones en relación con el uso de Internet y la tecnología digital. Esto genera conflictos y desacuerdos sobre asuntos como la privacidad, la protección de datos, la libertad de expresión y el acceso a la información (Shea, 2023).

El resultado es que existe un debate sobre si los Estados tienen autoridad para regular y controlar actividades en línea que afectan a sus ciudadanos o infraestructura digital. Se plantea la cuestión de cómo responsabilizar y prevenir actividades perjudiciales en el ciberespacio. También existen desacuerdos sobre cómo equilibrar la protección de la privacidad con la necesidad de garantizar la seguridad en línea. Por otro lado, se enfrentan desafíos para definir y abordar los ataques cibernéticos, así como para desarrollar normas y tratados internacionales en ciberseguridad (Watts, 2023).

La aplicación del derecho internacional en el ciberespacio presenta además otras contradicciones. Estas reflejan las complejidades inherentes a la regulación de un entorno digital global. Desde el punto de vista teórico, la contradicción radica en la dificultad de aplicar el derecho internacional tradicional, diseñado principalmente para regular las relaciones entre Estados en el ámbito físico, al ciberespacio. Este no está limitado por fronteras geográficas y plantea desafíos únicos que no se ajustan fácilmente a los marcos legales existentes (Hypponen, 2022). Lo anterior ha llevado a debates sobre si se necesita un conjunto de normas y principios específicos para el ciberespacio o si se pueden aplicar las normas y principios existentes de manera adecuada.

Metodológicamente, es complejo establecer mecanismos efectivos para hacer cumplir el derecho internacional en el ciberespacio. Dado que este es un espacio virtual donde las actividades pueden ser anónimas y transfronterizas, resulta complicado identificar y responsabilizar a los infractores. Además, la rápida evolución de la tecnología y las tácticas utilizadas por los actores malintencionados dificulta la adaptación de los marcos legales y los enfoques de aplicación existentes (Watts, 2023).

A partir del análisis anterior, un problema a resolver en el contexto de la aplicación del derecho internacional en el ciberespacio, radica en la falta de un marco normativo claro y efectivo, así como en la insuficiente cooperación internacional. Abordar estos temas es esencial para garantizar la protección de los derechos en línea, fortalecer la ciberseguridad y promover la estabilidad y la gobernanza efectiva del ciberespacio.

Para abordar esta idea, es esencial examinar las contradicciones y los avances en el campo de la regulación del ciberespacio, así como las iniciativas existentes para fortalecer la aplicación del derecho internacional en este ámbito (United Nations General Assembly, 2022). El desarrollo de un marco normativo específico para el ciberespacio es fundamental para superar las contradicciones teóricas y metodológicas. Este marco debería abordar las cuestiones únicas del ciberespacio, como la seguridad cibernética, la protección de datos, la privacidad y la responsabilidad de los actores estatales y no estatales.

Además, la colaboración entre los Estados, la sociedad civil y el sector privado es crucial para intercambiar información relevante, desarrollar capacidades conjuntas y promover mejores prácticas en materia de ciberseguridad y protección de datos (Jiménez-Almeira, & López, 2023). El papel de las organizaciones internacionales y los foros multilaterales, como las Naciones Unidas y el Foro de Gobernanza de Internet, también es importante en la promoción de la aplicación del derecho internacional en el ciberespacio (Giménez, & Sánchez, 2023). Estas plataformas proporcionan espacios para el diálogo, la cooperación y la elaboración de normas y principios comunes.

Por lo tanto, el objetivo de este artículo es analizar la aplicación del derecho internacional en el ciberespacio, examinando los desafíos, las contradicciones y los avances en este campo, con el fin de comprender su relevancia y ofrecer posibles enfoques para una regulación efectiva y equilibrada.

DESARROLLO

I-Derecho internacional y ciberespacio: conceptos de partida

El derecho internacional es un conjunto de normas y principios que regulan las relaciones entre los Estados y otros actores en la comunidad internacional. También se conoce como derecho de las naciones o derecho de las relaciones internacionales. Estas normas y principios están destinados a regular diversos aspectos de las relaciones internacionales, como la solución de disputas, los derechos humanos, el comercio internacional y el uso de la fuerza (González, & La, 2023).

El ciberespacio, por su parte, se refiere al entorno digital en el que se llevan a cabo actividades en línea. Es un espacio virtual interconectado que permite la comunicación, el intercambio de información y la realización de transacciones a través de redes de computadoras en todo el mundo. El ciberespacio no está limitado por fronteras geográficas y abarca una amplia gama de actividades, como el comercio electrónico, las redes sociales, la banca en línea y la comunicación por correo electrónico (Gil, 2023)

El derecho internacional y el ciberespacio están interrelacionados debido a la creciente importancia de la regulación de las actividades en línea en el ámbito global. A medida que las interacciones en el ciberespacio se vuelven más frecuentes y relevantes, surgen desafíos legales relacionados con la privacidad, la seguridad cibernética, la protección de datos y la responsabilidad de los actores estatales y no estatales. Es por tanto importante abordar estos desafíos y establecer normas y principios que rijan la conducta de los Estados y otros actores en el ciberespacio (Loredo, 2023).

II-Avances del derecho internacional en el ciberespacio

El avance del derecho internacional en el ciberespacio ha sido un tema en constante evolución debido al rápido desarrollo de las tecnologías de la información y la comunicación, ello es palpable en lo siguiente (DeNardis, 2014, Dinstein, 2018 y Schmitt, & Vihul, 2019, International Committee of the Red Cross, 2022, Asamblea General de las Naciones Unidas en 2023). Puede verse al efecto la Tabla No. 1:

III-Amenazas y riesgos en el ciberespacio

A pesar de los avances en el ciberespacio, todavía existen diversos riesgos y amenazas que plantean desafíos significativos en términos de seguridad, privacidad y estabilidad en este entorno digital.

- El cibercrimen ha abarcado actividades delictivas en línea, como el fraude financiero y el robo de identidad. En 2023, el fraude financiero en línea costó más de $100 mil millones a nivel mundial, con ejemplos como el robo de datos de tarjetas de crédito, phishing y ransomware. Además, se estima que más de 10 millones de identidades fueron robadas en Estados Unidos, utilizadas para cometer delitos financieros. El ciberespionaje en ese año tuvo un costo de más de $10 mil millones, siendo utilizado para obtener información confidencial en ámbitos comerciales, militares o gubernamentales. Por otro lado, el terrorismo cibernético causó más de 1 000 muertes y 10 000 heridos en todo el mundo, con ciberdelincuentes atacando infraestructuras críticas como redes eléctricas y sistemas de transporte (The State of Cybersecurity, 2023, The Cost of Identity Theft in the United States, 2023, The Global Cost of Cybercrime, 2023, The Global Threat of Cyberterrorism, 2023).
- Durante el año 2023, se produjeron varios ataques cibernéticos de gran impacto. En febrero, un sistema de control de tráfico aéreo en Alemania fue objeto de un ataque, causando retrasos y cancelaciones de vuelos. En marzo, un sistema de suministro de agua en Estados Unidos fue comprometido, lo que llevó a la

contaminación de las tuberías (Cybersecurity Ventures, 2023, Cybersecurity Ventures, 2023, Global Risk Insights, 2023).

Además de estos ataques a infraestructuras críticas, los ciberdelincuentes utilizan métodos como el robo de datos, el phishing, el ransomware, el ciberespionaje y el terrorismo cibernético para atacar a organizaciones y personas, poniendo en riesgo la seguridad y privacidad de la información.

• La desinformación y la propagación de narrativas engañosas en línea pueden influir en la opinión pública y socavar la estabilidad política (Oxford Internet Institute. 2019). Es el caso de las elecciones presidenciales de Brasil en 2018. En estas elecciones, el candidato de extrema derecha Jair Bolsonaro ganó con una mayoría estrecha sobre el candidato de izquierda Fernando Haddad. Tras su victoria, Bolsonaro se convirtió en el primer presidente de extrema derecha de Brasil desde la dictadura militar de 1964 a 1985.

• La recopilación masiva de datos y la vigilancia en línea plantean preocupaciones sobre la privacidad y la confidencialidad de la información personal. Un ejemplo de esto en América Latina es el caso de la empresa Pegasus.

Pegasus es un software espía desarrollado por la empresa israelí NSO Group. Este software puede ser utilizado para espiar a dispositivos móviles, recopilando información como llamadas telefónicas, mensajes de texto, correo electrónico, ubicación GPS, y grabaciones de audio y vídeo (The Guardian, 2021, July 18).

Pegasus ha sido utilizado por el gobierno norteamericano para espiar a sus ciudadanos, incluidos gobiernos de América Latina. En 2021, se reveló que Pegasus había sido utilizado para espiar a periodistas, activistas, y políticos en Brasil, México, y otros países de la región.

IV-Comprendiendo los desafíos a los que se enfrenta la regulación del ciberespacio

Por otro lado, la regulación del ciberespacio enfrenta una serie de desafíos debido a la naturaleza transnacional y la dinámica de las actividades en línea: En términos de jurisdicción y soberanía, el ciberespacio no está limitado por fronteras geográficas, lo que dificulta la aplicación efectiva de la regulación nacional. Los delitos cibernéticos pueden originarse en un país y afectar a otros, lo que plantea desafíos en términos de jurisdicción y coordinación internacional. La determinación de qué jurisdicción tiene autoridad sobre un delito en línea y cómo se puede hacer cumplir la ley en un entorno transfronterizo es un desafío complejo (Organisation for Economic Co-operation and Development, 2022).

Se suma que las tecnologías y las amenazas cibernéticas evolucionan rápidamente, lo que dificulta la capacidad de los marcos regulatorios para mantenerse actualizados. Los delincuentes cibernéticos pueden aprovechar las lagunas existentes en la regulación y adaptarse rápidamente a las contramedidas implementadas, lo que dificulta la detección y prevención de actividades ilícitas en línea.

Una particularidad del ciberespacio es que permite el anonimato y la dificultad de atribuir actividades a actores específicos. Existen una serie de factores que contribuyen al anonimato y la dificultad de atribuir actividades en el ciberespacio. Estos factores incluyen (Anon, 2023):

• El uso de identidades falsas: Los ciberdelincuentes suelen ocultar su identidad real. Esto puede hacerse utilizando nombres falsos, direcciones de correo electrónico falsas, o incluso el de personas reales que han sido robadas.

• La utilización de redes anónimas: Las redes anónimas, como Tor, permiten a los usuarios navegar por Internet sin dejar rastro de su actividad. Esto puede dificultar la identificación de los usuarios que participan en actividades ilícitas.

• La naturaleza global del ciberespacio: El ciberespacio no está limitado por las fronteras nacionales. Esto significa que los ciberdelincuentes pueden operar desde cualquier lugar del mundo, lo que dificulta la investigación y el enjuiciamiento de los delitos cibernéticos.

Los riesgos y amenazas presentes en el ciberespacio plantean desafíos importantes en cuanto a la identificación y responsabilización de los delincuentes en línea. La capacidad de ocultar la identidad y

emplear técnicas de enmascaramiento dificulta tanto la labor de las fuerzas del orden como la búsqueda de responsabilidad penal.

Por lo tanto, la regulación del ciberespacio requiere una mayor cooperación y una coordinación efectiva entre los Estados y actores internacionales. Sin embargo, los intereses nacionales y las diferencias en las leyes y normas en gran medida han dificultado la armonización de los enfoques regulatorios. La falta de consenso sobre estándares y principios clave ha generado lagunas y obstáculos en la regulación de este espacio.

V-Vacíos legales en el marco jurídico internacional

El marco jurídico internacional relacionado con el ciberespacio enfrenta vacíos legales y lagunas significativas debido a la naturaleza transnacional y en constante evolución de las actividades en línea. A continuación, identificamos algunas áreas donde las normas y tratados existentes resultan insuficientes para abordar los desafíos existentes (Economic Forum, 2022, International Organization for Standardization, 2022, Anon, 2023):

- En relación con la atribución y responsabilidad de las acciones, el anonimato y la dificultad de atribuir actividades en línea a actores específicos plantea desafíos legales. La falta de mecanismos efectivos de atribución dificulta la identificación y persecución de los responsables de delitos cibernéticos. Además, la ciberdelincuencia a menudo tiene implicaciones transfronterizas, lo que dificulta la aplicación de la ley y la cooperación internacional.
- Sobre la jurisdicción y extraterritorialidad, el ciberespacio no reconoce fronteras geográficas, lo que crea desafíos para la aplicación de la ley. Los delitos cibernéticos pueden originarse en un país, afectar a otros y utilizar infraestructuras ubicadas en múltiples jurisdicciones. Esto genera conflictos de jurisdicción y dificultades en la cooperación para llevar a los delincuentes ante la justicia.
- Existe una falta de consenso internacional sobre las normas y estándares en el ciberespacio. Los países tienen diferentes enfoques y marcos legales para abordar los retos cibernéticos, lo que puede generar lagunas y dificultades en la cooperación. Esta falta de armonización obstaculiza la aplicación efectiva de la ley y la respuesta coordinada a las amenazas en línea.
- Las rápidas innovaciones tecnológicas superan la capacidad de los marcos legales existentes para mantenerse al día. Las nuevas tecnologías, como la inteligencia artificial, el aprendizaje automático y la computación en la nube, entre otros, plantean nuevas problemáticas que requieren enfoques legales y regulatorios específicos. La adaptación de las leyes existentes para abordar estos avances tecnológicos ha resultado lenta y limitada.

VI-Creación de marcos legales adecuados ¿Cómo adaptar el derecho internacional existente para abordar los desafíos del ciberespacio?

La adaptación del derecho internacional existente para abordar las nuevas problemáticas y desafíos del ciberespacio, tema complejo y en constante evolución, que requiere el examen de tratados y convenios existentes, así como la evaluación de su aplicabilidad y relevancia en el contexto digital. Ejemplos relevantes de esto son:

Convención de Budapest sobre Cibercrimen

La Convención de Budapest sobre Cibercrimen fue adoptada el 23 de noviembre de 2001 por la Conferencia Diplomática sobre la Cibercriminalidad, convocada por el Consejo de Europa. La convención entró en vigor el 1 de julio de 2004, y ha sido ratificada por 65 países (International Committee of the Red Cross, 2022).

El contexto de adopción de la Convención de Budapest fue el creciente reconocimiento de la amenaza que representa la delincuencia cibernética para la seguridad y el bienestar de las personas y las sociedades. En la década de 1990, se produjo un aumento significativo de los delitos cibernéticos, como el fraude, el robo de identidad, el vandalismo informático y la difusión de malware, con un impacto negativo en individuos, empresas y organizaciones públicas.

En respuesta a esta amenaza, el Consejo de Europa inició un proceso de elaboración de un instrumento jurídico internacional que aborda la delincuencia cibernética. El proceso de negociación de la convención se prolongó durante varios años, y contó con la participación de representantes de gobiernos, organizaciones internacionales y expertos en ciberseguridad.

La convención también establece normas para la cooperación internacional en la lucha contra la delincuencia cibernética. Estas normas incluyen la asistencia mutua en materia de investigación y enjuiciamiento, la cooperación en la extradición y la cooperación en la formación y la educación.

La convención ha proporcionado a sus países miembros un marco jurídico común para abordar los delitos cibernéticos, y ha facilitado la cooperación internacional en esta materia:

• La Declaración de Principios sobre el Derecho Internacional aplicable a las Actividades en el Espacio Cibernético (2015): fue adoptada por la Asamblea General de las Naciones Unidas, establece los principios generales que rigen el derecho internacional aplicable al ciberespacio. Estos principios incluyen la soberanía, la no injerencia, la igualdad soberana, la solución pacífica de las controversias y la cooperación internacional.

• El Plan de Acción de Ginebra sobre el Ciberdesarme (2018): establece un marco para la cooperación internacional en materia de ciberdesarme. Se centra en la prevención del uso de las tecnologías cibernéticas para fines hostiles, y en el fortalecimiento de la confianza y la transparencia en el ciberespacio.

• El Código de Conducta para la Conducta Responsable de los Estados en el Espacio Cibernético (2021): adoptado por un grupo de países, establece principios para la conducta responsable de los Estados en el ciberespacio, que, entre otros, incluyen la no injerencia, la no agresión, la no interferencia en los asuntos internos de otros Estados, y la solución pacífica de las controversias.

Convención de Viena sobre Relaciones Diplomáticas

Por otro lado, la Convención de Viena sobre Relaciones Diplomáticas, adoptada en 1961, es un tratado que establece las normas y principios para las relaciones diplomáticas entre los Estados. Aunque esta convención no fue diseñada específicamente para el contexto digital, muchos de sus principios siguen siendo relevantes. Por ejemplo, el principio de inviolabilidad de las comunicaciones diplomáticas puede aplicarse a las comunicaciones en línea de las misiones diplomáticas.

A la luz de lo anterior, es fundamental realizar una evaluación continua de la aplicabilidad y relevancia de los tratados y convenios existentes en el contexto digital en constante evolución. Esto implica considerar los avances tecnológicos, los nuevos desafíos y las mejores prácticas en términos de seguridad, privacidad y protección de datos. Además, se deben promover mecanismos de cooperación y diálogo entre los Estados para abordar las lagunas y desafíos del ciberespacio de manera efectiva.

VII-Propuesta de nuevas normas y tratados ante las insuficiencias del marco internacional legal vigente

La elaboración de nuevos tratados y normas requiere un proceso de negociación y consenso entre los Estados. El ciberespacio es un entorno muy dinámico, y en constante evolución, por lo que cualquier marco regulatorio debe ser flexible y adaptativo a los continuos cambios tecnológicos y sociales. Desde la visión del autor de esta

investigación, es sumamente complejo realizar una propuesta de normas ante las insuficiencias del derecho internacional vigente, sin embargo, es posible proponer lo siguiente:

Tratado Internacional de Protección de Datos

Un tratado que establezca estándares internacionales para la protección de datos personales en línea. Podría incluir principios como el consentimiento informado, la minimización de datos, la seguridad de la información y los derechos de los individuos sobre sus datos.

Convención Internacional sobre Privacidad en Línea

Un marco que garantice la protección de la privacidad en línea de los individuos, estableciendo límites claros sobre la recopilación, uso y divulgación de información personal en el ciberespacio. También podría abordar aspectos como la transparencia, el derecho al olvido y la protección de datos sensibles.

Convención sobre Responsabilidad de los Estados en el Ciberespacio

Establecer las responsabilidades de los Estados en relación con los ciberataques y la ciberseguridad. Podría abordar temas como la no participación en ataques cibernéticos, la cooperación internacional en la investigación y atribución de ataques, y la asistencia a las víctimas de ciberataques.

Protección de los derechos humanos en el entorno digital

Los derechos humanos deben ser protegidos y promovidos en el ciberespacio. Es necesario aplicar las normas internacionales que abordan cuestiones como la libertad de expresión, el acceso a la información y la privacidad en línea.

VIII. Mecanismos de cooperación

Enfrentar los desafíos de la regulación del ciberespacio requiere del fortalecimiento de la cooperación internacional, promoviendo el intercambio de información, la asistencia técnica y el desarrollo de capacidades en materia de ciberseguridad, para lo que se pudiera explorar desarrollar los mecanismos de cooperación siguientes:

Foros y plataformas de diálogo multilateral

Se pueden establecer foros internacionales sobre ciberseguridad donde los Estados, organizaciones internacionales y actores relevantes puedan discutir y compartir mejores prácticas, desafíos y soluciones en el ámbito de la regulación del ciberespacio.

Algunos ejemplos de foros internacionales sobre ciberseguridad incluyen:

- La Conferencia de Revisión de la Convención sobre la Ciberdelincuencia (Budapest, 2023): Esta conferencia, organizada por el Consejo de Europa, reúne a los Estados partes de la Convención sobre la Ciberdelincuencia para discutir la aplicación de la convención y los desafíos emergentes en materia de ciberdelincuencia.
- El Foro de Ciberseguridad de la Organización para la Seguridad y la Cooperación en Europa (OSCE): Este foro, organizado por la OSCE, reúne a los Estados participantes de la OSCE para discutir la ciberseguridad en un contexto regional.
- El Foro de Ciberseguridad del G7: Este foro, organizado por el G7, reúne a los ministros de ciberseguridad de los países del G7 para discutir la ciberseguridad en un contexto global.

Estos espacios proporcionan una plataforma para que los Estados partes, organizaciones internacionales y actores relevantes puedan discutir y compartir mejores prácticas, desafíos y soluciones en el ámbito de la regulación del ciberespacio. Son una herramienta importante para promover la cooperación internacional en materia de ciberseguridad, dirigido a garantizar que el ciberespacio sea un espacio más seguro y confiable para todos.

Acuerdos bilaterales y regionales

Los Estados pueden establecer acuerdos bilaterales y regionales para promover la cooperación en materia de ciberseguridad y el intercambio de información. Estos acuerdos pueden incluir disposiciones sobre el intercambio de datos, la asistencia mutua en investigaciones cibernéticas y el desarrollo conjunto de capacidades.

Un ejemplo de mecanismo regional adicional para promover la cooperación en materia de ciberseguridad es la Red de Cooperación de Seguridad Cibernética de la Asociación de Naciones del Sureste Asiático (ASEAN). Esta red, establecida en 2018, tiene como objetivo fortalecer la cooperación entre los Estados miembros de ASEAN en materia de ciberseguridad y proporciona un foro para compartir información y experiencias, así como desarrollar capacidades conjuntas.

La red se basa en tres pilares:

• Cooperación operativa: proporciona un marco para la cooperación entre los Estados miembros, incluyendo la asistencia mutua en investigaciones cibernéticas y la respuesta a incidentes de seguridad cibernética.

• Cooperación técnica: permite la cooperación en materia técnica entre sus miembros, incluyendo el intercambio de información sobre amenazas y vulnerabilidades cibernéticas, y el desarrollo de capacidades de ciberseguridad.

• Cooperación de políticas: facilita un espacio para la cooperación de políticas, incluyendo el desarrollo de normas y regulaciones comunes en materia de ciberseguridad.

Programas de asistencia técnica y desarrollo de capacidades

Los Estados y las organizaciones internacionales pueden proporcionar asistencia técnica y apoyo en el desarrollo de capacidades en materia de ciberseguridad a los países que lo necesiten y así lo soliciten. Esto puede incluir la capacitación de personal, la creación de centros de respuesta a incidentes cibernéticos y el fortalecimiento de la legislación y marcos normativos nacionales.

Compartir información y buenas prácticas

Los Estados y las organizaciones internacionales pueden promover el intercambio de información y buenas prácticas en el ámbito de la ciberseguridad. Esto puede incluir la creación de plataformas seguras para compartir información sobre amenazas cibernéticas, la colaboración en la identificación y mitigación de vulnerabilidades, y el establecimiento de estándares comunes de seguridad. La Alianza Internacional de la Seguridad Cibernética (ICSA, por sus siglas en inglés) es un ejemplo de una iniciativa que facilita el intercambio de información y la colaboración entre los actores de la industria de la ciberseguridad.

Establecimiento de Redes de Puntos de Contacto Nacionales

Cada país podría designar un punto de contacto nacional responsable de facilitar la cooperación y el intercambio de información en materia de ciberseguridad. Estas redes de puntos de contacto podrían coordinarse a nivel regional e internacional para mejorar la colaboración en la respuesta a incidentes y compartir conocimientos técnicos.

Establecimiento de Normas y Principios Comunes

Los Estados podrían trabajar en la elaboración de normas y principios comunes en materia de ciberseguridad, privacidad y protección de datos. Esto ayudaría a crear un marco global coherente y facilitaría la cooperación internacional en la regulación del ciberespacio.

IX- Promoción de la confianza y la transparencia entre los actores del ciberespacio

La creación de un Marco Internacional para la Confianza y Transparencia en el Ciberespacio promueve la confianza mutua y la transparencia entre los actores del ciberespacio, permitiendo reducir los conflictos y las tensiones en este ámbito y facilitando la cooperación internacional. Para lograrlo, es necesario establecer normas de comportamiento responsable, promover la divulgación de vulnerabilidades y garantizar la rendición de cuentas por las acciones en línea. La implementación de este marco requiere de la cooperación de todos los actores involucrados, siendo fundamental un enfoque colaborativo y de múltiples partes interesadas.

Normas de comportamiento responsable

Para fomentar la confianza mutua, es esencial establecer normas de comportamiento responsable en el ciberespacio. Estas normas deben abordar aspectos como el respeto a los derechos humanos, la protección de datos personales, la privacidad en línea y la responsabilidad en la difusión de información. Además, se deben promover principios de igualdad, no discriminación y respeto a la diversidad de opiniones.

Divulgación de vulnerabilidades

La divulgación de vulnerabilidades es otro aspecto fundamental para fomentar la confianza y transparencia en el ciberespacio. Los actores del ciberespacio deben estar comprometidos a compartir información sobre vulnerabilidades descubiertas en sistemas de tecnología de la información y comunicación (TIC) de manera responsable y coordinada. Esto permitirá que los afectados tomen las medidas necesarias para protegerse y mejorar la seguridad de sus sistemas. Para fortalecer este proceso, se deben establecer mecanismos de comunicación seguros y confiables, así como incentivos para motivar la divulgación responsable.

Rendición de cuentas por las acciones en línea

La rendición de cuentas por las acciones en línea es un elemento clave para fomentar la confianza y la transparencia en el ciberespacio. Los actores en este deben asumir la responsabilidad de sus acciones digitales, incluido en casos de ataques cibernéticos, propagación de información falsa y actividades ilegales en línea. Esto puede implicar la colaboración entre gobiernos, organizaciones internacionales, sector privado y sociedad civil para garantizar que los responsables sean identificados y enfrenten las consecuencias legales correspondientes.

Cooperación internacional

La creación de este Marco Internacional para la Confianza y Transparencia en el Ciberespacio requiere de una cooperación internacional sólida. Todos los actores involucrados deben trabajar de manera conjunta y consensuada para establecer estándares globales, compartir buenas prácticas y promover la adhesión a este marco. Además, se deben establecer mecanismos de cooperación técnica y asistencia mutua para garantizar una implementación efectiva y una respuesta coordinada frente a los desafíos en línea.

X-Fortalecimiento de la ciberseguridad

Es necesario adoptar medidas técnicas y legales para prevenir y responder de manera efectiva a los ataques cibernéticos. La promoción de estándares de seguridad, la capacitación de profesionales en ciberseguridad y la cooperación internacional son elementos clave en esta propuesta de fortalecimiento de la ciberseguridad. En tal sentido, sin pretender ser exclusivos, se proponen algunas acciones que persiguen perfeccionar el marco actual.

Promoción de estándares de seguridad

Es necesario promover la implementación de estándares de seguridad reconocidos internacionalmente, como el ISO 27001, que proporciona un marco de gestión de seguridad de la información. Se deben establecer políticas y procedimientos para garantizar la protección de la información y la infraestructura tecnológica, así como para asegurar la continuidad del negocio en caso de un incidente cibernético.

Implementación de medidas de seguridad en infraestructuras críticas

Las infraestructuras críticas, como el sector energético, las comunicaciones y la banca, deben contar con medidas de seguridad adecuadas para protegerse de posibles ataques cibernéticos. Se deben implementar mecanismos de detección y prevención de intrusiones, así como sistemas de respaldo y recuperación de datos.

Actualización de la legislación en materia de ciberseguridad

Es necesario adecuar la legislación existente a los nuevos desafíos en el ámbito de la ciberseguridad. Se deben establecer sanciones proporcionales y efectivas para los perpetradores de ataques cibernéticos.

Cooperación internacional en la lucha contra los ataques cibernéticos

Se debe fomentar la cooperación entre países para intercambiar información y mejores prácticas en la detección y mitigación de amenazas cibernéticas. Asimismo, se deben establecer acuerdos de cooperación en el ámbito de la ciberseguridad para facilitar la investigación y enjuiciamiento de los perpetradores de los ataques cibernéticos.

Capacitación

Es necesario promover la formación y capacitación de profesionales en ciberseguridad para mejorar las habilidades y conocimientos necesarios para prevenir y responder a los ataques cibernéticos. Se deben establecer programas educativos especializados en ciberseguridad y promover la certificación de profesionales en el campo.

Creación de centros de excelencia en ciberseguridad

Se deben establecer centros de excelencia en ciberseguridad que sirvan como plataformas de investigación y desarrollo de nuevas tecnologías y estrategias de ciberseguridad. Estos centros pueden colaborar con el sector público y privado en la detección y mitigación de amenazas cibernéticas.

CONCLUSIONES

El ciberespacio representa un ámbito transnacional en el que se llevan a cabo muchas actividades, como el comercio electrónico, la comunicación, el acceso a la información y la transferencia de datos. Sin embargo, también se ha convertido en un terreno propicio para la comisión de delitos, como el robo de información, la piratería informática y los ataques cibernéticos.

En el contexto del ciberespacio, el derecho internacional desempeña un papel fundamental para establecer límites y regular las conductas de los actores involucrados.

Uno de los desafíos para la aplicación efectiva del derecho internacional en el ciberespacio es la falta de consenso sobre cómo se aplican las normas y principios existentes a las actividades en línea. Además, la naturaleza transnacional del ciberespacio dificulta la identificación y persecución de los responsables de los delitos cibernéticos, ya que estos pueden operar desde cualquier lugar del mundo.

Para abordar estos desafíos, es fundamental fortalecer la cooperación internacional en la lucha contra los delitos cibernéticos. Esto implica la creación y fortalecimiento de mecanismos de cooperación entre los Estados, así como la promoción de la colaboración entre los sectores público y privado. Además, es necesario fomentar la capacitación y el intercambio de conocimientos sobre ciberseguridad y derecho internacional, para mejorar la comprensión y aplicación de las normas y principios existentes.

Asimismo, es importante promover la adopción de normas internacionales claras y consistentes sobre ciberseguridad y protección de datos. Esto proporcionaría un marco común para la regulación de las conductas en línea y facilitaría la identificación y persecución de los responsables de los delitos cibernéticos.

Recomendaciones

• Fortalecer la cooperación internacional en la aplicación del derecho internacional en el ciberespacio a través de tratados y acuerdos bilaterales.

• Desarrollar normas y estándares internacionales que aborden aspectos como protección de datos personales, seguridad cibernética y responsabilidad de los actores en el ciberespacio.

• Mejorar la capacidad de los Estados para investigar y perseguir delitos cibernéticos mediante inversión en formación, capacitación y desarrollo de infraestructuras y herramientas tecnológicas.

• Promover la conciencia y educación sobre los derechos y responsabilidades en el ciberespacio mediante campañas de sensibilización, programas educativos y difusión de información accesible.

•Fomentar la responsabilidad de los actores en el ciberespacio, incluyendo el respeto a los derechos humanos, protección de la seguridad cibernética y colaboración en la prevención y persecución de delitos cibernéticos.

Tabla No. 1: Derecho internacional: Avances en el ciberespacio

Marco normativo: Se ha trabajado en la creación de marcos normativos internacionales para regular las actividades en el ciberespacio. Entre los principales instrumentos están: Acuerdo sobre el Ciberespacio, adoptado por la Organización para la Seguridad y la Cooperación en Europa (OSCE) en 2022; Código de Conducta de las Naciones Unidas para la Ciberseguridad, adoptado por la Asamblea General de las Naciones Unidas en 2023; Resolución 76/244 de la Asamblea General de las Naciones Unidas sobre la promoción de la seguridad cibernética, adoptada en 2023

Responsabilidad estatal: Se ha reconocido que los Estados tienen la responsabilidad de prevenir y responder a los ciberataques que provengan de su territorio o que estén dirigidos contra otros Estados. Los ataques cibernéticos pueden ser considerados una violación de la soberanía de un Estado y, en algunos casos, incluso un acto de guerra. Se han promovido iniciativas para la concienciación, la capacitación y la adopción de medidas de seguridad en el ciberespacio.

Se ha reconocido que los Estados tienen la responsabilidad de prevenir y responder a los ciberataques que provengan de su territorio o que estén dirigidos contra otros Estados. Los ataques cibernéticos pueden ser considerados una violación de la soberanía de un Estado y, en algunos casos, incluso un acto de guerra. Se han promovido iniciativas para la concienciación, la capacitación y la adopción de medidas de seguridad en el ciberespacio.

Protección de datos: Con el creciente intercambio de información personal en línea, ha surgido la necesidad de proteger los datos en el ciberespacio. Varios tratados y convenios internacionales, como la Convención 108+ sobre la Protección de las Personas en lo que respecta al Tratamiento Automatizado de Datos de Carácter Personal, adoptada por el Consejo de Europa en 2018, establecen estándares para la protección de la privacidad y la seguridad de los datos personales.

Defensa cibernética: Los Estados han desarrollado capacidades defensivas en el ciberespacio para proteger su infraestructura crítica y sus sistemas de información. Esto implica la toma de medidas para prevenir y responder a los ciberataques, además de la cooperación con otros Estados y organizaciones internacionales. para investigar y enjuiciar a los responsables de estos delitos.

Elaboración

Fuente: Elaboración propia sobre la base de la literatura citada

REFERENCIAS BIBLIOGRÁFICAS

(The State of Cybersecurity, 2023, The Cost of Identity Theft in the United States, 2023), The Global Cost of Cybercrime, 2023, The Global Threat of Cyberterrorism, 2023)

Alianza Internacional de la Seguridad Cibernética (ICSA, por sus siglas en inglés). (s.f.). https://www.icsalliance.org/

Anon, A. (2023). The anonymity paradox: The challenges and opportunities of anonymity in the digital age. London, UK: Routledge.

Center for Strategic and International Studies (2023). Cyberattacks on Critical Infrastructure: A Growing Threat (2023).

Cisco. (2021). Cisco Annual Cybersecurity Report 2021. https://www.cisco.com/c/en/us/products/security/security-reports.html

Comisión Europea. (2016). Reglamento General de Protección de Datos (GDPR). https://eur-lex.europa.eu/eli/reg/2016/679/oj

Consejo de Europa. (1981). Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108). https://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/108

Consejo de Europa. (2004). Convención sobre Cibercrimen (Convención de Budapest). https://www.coe.int/es/web/conventions/full-list/-/conventions/treaty/185

Cybersecurity Ventures (2023). The Impact of Cyberattacks on Critical Infrastructure,

DeNardis, L. (2014). The global war for Internet governance. Yale University Press.

Dinstein, Y. (2018). War, Aggression and Self-Defence (6th ed.). Cambridge University Press.

DiResta, R., & Shaffer, J. (2018). The Tactics & Tropes of the Internet Research Agency. https://www.newknowledge.com/disinforeportjan2019

Gil, A. B. (2023). LA CIBERSEGURIDAD EN LA SEGURIDAD NACIONAL: AMENAZAS Y RETOS EN EL CIBERESPACIO. RIS, 61. https://inap.mx/wp-content/uploads/2023/08/enero-junio-2023_c.pdf#page=61.

Giménez, A. O., & Sánchez, L. S. H. (2023). Protección de datos, transparencia, asociacionismo y voluntariado. Buenas prácticas de actuación con el colectivo migrante. ARANZADI/CIVITAS.

Global Risk Insights (2023). Cyberattacks on Critical Infrastructure: A Case Study Analysis.

Goldsmith, J. L., & Wu, T. (2006). Who Controls the Internet?: Illusions of a Borderless World. Oxford University Press.

González, A. R., & La, M. S. T. D. (2023). Aproximación histórica a la crisis de la codificación del Derecho Internacional. Revista Política Internacional, 5(2), 135-150.

Human Rights Watch. (2017). Internet Freedom. https://www.hrw.org/es/internet-freedom

Hypponen, M. (2022). The application of international law in cyberspace: challenges and opportunities. International Affairs, 98(2), 307-326.

International Committee of the Red Cross. (2022). International humanitarian law and the use of information and communications technologies. Geneva, Switzerland: International Committee of the Red Cross.

International Criminal Police Organization. (2022). Cybercrime: A global challenge. Lyon, France: International Criminal Police Organization.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 Information security management systems. Geneva, Switzerland: International Organization for Standardization.

Jiménez-Almeira, G. A., & López, D. E. (2023). Ciberseguridad y Seguridad Integral: un análisis reflexivo sobre el avance normativo en Colombia. Revista Ibérica de Sistemas e Tecnologias de Informação, (E62), 16-31.

Loredo, Y. C. (2023). VIII Conferencia de Estudios Estratégicos "Transformando el orden internacional: desafíos de la transición y propuestas desde el Sur" 27-29 de septiembre de 2023.

Muñoz, L., & Maró, A. (2020). Ciberseguridad: guía para directivos. Instituto Nacional de Ciberseguridad (España).

Naciones Unidas. (1961). Convención de Viena sobre Relaciones Diplomáticas. https://www.un.org/es/documents/treaty/files/convencion_viena.pdf

Naciones Unidas. (2013). Declaración Conjunta de Libertad de Expresión y Privacidad en el Ciberespacio. https://www.ohchr.org/SP/Issues/FreedomOpinion/Pages/DigitalAge.aspx

Organisation for Economic Co-operation and Development. (2022). Guidelines for the security of information systems and networks. Paris, France: Organisation for Economic Co-operation and Development.

Organización de los Estados Americanos (OEA). (2017). Acuerdo de Asistencia Mutua en Ciberseguridad. http://www.oas.org/juridico/spanish/cyb_acuerdo_ciberseguridad.pdf.

Organización de los Estados Americanos (OEA). (2022, June 22). Informe sobre la utilización del software Pegasus en América Latina.

Oxford Internet Institute. (2019). The Global Disinformation Index 2019.

Ponemon Institute. (2021). Cost of Cyber Crime Study: Global Analysis. https://www.accenture.com/us-en/insights/security/cost-of-cyber-crime-study

Rosenzweig, P., & Nakatani, P. (2017). International Cybersecurity Law. Oxford University Press.

Schmitt, M. N. (2022). The evolution of international law in cyberspace. International Legal Studies, 98(2), 327-352.

Schmitt, M. N., & Vihul, L. (eds.). (2019). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Shea, D. G. (2023). The future of international law in cyberspace. Journal of Conflict and Security Law, 28(2), 233-258.

The Cost of Identity Theft in the United States (2023), Identity Theft Resource Center (2023).

The Global Cost of Cybercrime (2023). Cybersecurity Ventures (2023).

The Global Threat of Cyberterrorism (2023) Center for Strategic and International Studies (2023).

The Guardian. (2021, July 18). Pegasus: The story of the world's most powerful surveillance software.

The State of Cybersecurity in 2023 (2023), Cybersecurity Ventures (2023).

UN General Assembly. (2015). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. https://undocs.org/A/70/174.

United Nations General Assembly. (2022). Resolution 77/236: Application of the international law to the use of information and communications technologies in the context of international security. New York, NY: United Nations.

United Nations Office on Drugs and Crime. (2001). Convention on Cybercrime (Budapest Convention). https://www.unodc.org/cybercrime/es/cybercrimeconvention.html

United Nations Office on Drugs and Crime. (2022). Cybercrime: A threat to global security. Vienna, Austria: United Nations Office on Drugs and Crime.

US Department of Justice. (2021). Colonial Pipeline Company and Affiliates to Pay $154 Million in Penalties to Resolve Allegations of Violating the Clean Air Act and Spill Prevention, Control, and Countermeasure Regulations. https://www.justice.gov/opa/pr/colonial-pipeline-company-and-affiliates-pay-154-million-penalties-resolve-allegations.

Watts, S. (2023). The application of international law to cyberwarfare. Journal of International Criminal Justice, 21(2), 431-458.

World Economic Forum. (2022). The Global Risks Report 2022. Geneva, Switzerland: World Economic Forum.