Cuadernos de Nuestra América/Nueva Época/No. 010 / enero-marzo 2024/
RNPS: 2529 /ISSN: 2959-9849/99 pp.

Ciberseguridad en las Relaciones Internacionales: ¿Cómo los ataques cibernéticos pueden crear tensiones internacionales?

Cybersecurity in International Relations: How can Cyberattacks create International Tensions?

Recibido: enero 2024
Aprobado: febrero 2024.

Ms.C. Dania Onora De León Nazareno

Ministerio de Relaciones Exteriores y Movilidad Humana.
Ciudad: Quito-Ecuador.
Email: dleon@cancilleria.gob.ec
ORCID: 0009-006-1098-472X.

Resumen

La ciberseguridad es un tema cada vez más importante en las relaciones internacionales debido a la creciente dependencia de la tecnología y la información en el mundo moderno. Los ataques cibernéticos pueden tener graves consecuencias para la seguridad nacional y la estabilidad de las relaciones internacionales, lo que hace que la ciberseguridad sea una prioridad para los gobiernos y las organizaciones internacionales. La pregunta a investigar en este tema es ¿cómo los ataques cibernéticos pueden crear tensiones internacionales?. La metodología de la investigación es cualitativa y se basa en la revisión documental de artículos, informes y estudios sobre la ciberseguridad y las tensiones internacionales causadas por los ataques cibernéticos. El objetivo de la investigación es analizar cómo los ataques cibernéticos pueden afectar las relaciones internacionales y las tensiones entre los países. Los hallazgos de la investigación muestran que los ataques cibernéticos pueden tener un impacto significativo en la seguridad nacional y la estabilidad de las relaciones internacionales. Los ataques cibernéticos pueden ser utilizados como herramientas de espionaje y sabotaje, lo que puede llevar a la pérdida de información confidencial y la interrupción de servicios críticos. Además, los ataques cibernéticos también pueden ser utilizados como una forma de guerra cibernética, lo que puede crear tensiones internacionales y desencadenar conflictos. Los países pueden acusarse mutuamente de llevar a cabo ataques cibernéticos, lo que puede aumentar la desconfianza y la hostilidad entre ellos. En conclusión, la ciberseguridad es un tema crucial en las relaciones internacionales y los ataques cibernéticos pueden crear tensiones internacionales significativas. Los gobiernos y las organizaciones internacionales deben tomar medidas para fortalecer la ciberseguridad y prevenir los ataques cibernéticos para garantizar la seguridad nacional y la estabilidad de las relaciones internacionales

Palabras clave: *Ciberseguridad, ciberguerra, ataques cibernéticos, relaciones internacionales, tensiones internacionales.*

Abstract

Cybersecurity is an increasingly important topic in international relations due to the growing dependence on technology and information in the modern world. Cyber attacks can have serious consequences for national security and the stability of international relations, making cybersecurity a priority for governments and international organizations. The research question in this topic is how cyber attacks can create international tensions. The research methodology is qualitative and based on a documentary review of articles, reports, and studies on cybersecurity and the international tensions caused by cyber attacks. The objective of the research is to analyze how cyber attacks can affect international relations and tensions

between countries. The research findings show that cyber attacks can have a significant impact on national security and the stability of international relations. Cyber attacks can be used as tools for espionage and sabotage, leading to the loss of confidential information and the disruption of critical services. Furthermore, cyber attacks can also be used as a form of cyber warfare, which can create international tensions and trigger conflicts. Countries can accuse each other of carrying out cyber attacks, increasing distrust and hostility between them. In conclusion, cybersecurity is a crucial topic in international relations, and cyber attacks can create significant international tensions. Governments and international organizations must take steps to strengthen cybersecurity and prevent cyber attacks to ensure national security and the stability of international relations.

Keywords: *Cybersecurity, cyber warfare, cyber attacks, international relations, tensions*

Introducción

En el contexto actual de avances tecnológicos y globalización, la ciberseguridad se ha convertido en un tema de suma importancia en el ámbito de las relaciones internacionales. Con el aumento de la interconexión digital a nivel global, los ataques cibernéticos también han experimentado un incremento considerable. Estos ataques pueden llevar consigo una serie de consecuencias que van más allá de lo tecnológico y que pueden generar tensiones en las relaciones entre Estados. Por lo tanto, es fundamental explorar cómo los ataques cibernéticos pueden crear tensiones internacionales y buscar soluciones eficientes para su prevención y mitigación.

A pesar de la creciente importancia de la ciberseguridad en las relaciones internacionales, existen aún vacíos por investigar en este campo (Rid, & Perez, 2018). Por ejemplo, se requiere una mayor comprensión de la dimensión política de los ataques cibernéticos y cómo estos pueden afectar las relaciones entre Estados. Por tanto, es necesario indagar en las motivaciones y estrategias utilizadas por los actores internacionales en la realización de ataques cibernéticos, así como en las vulnerabilidades y fallas en los sistemas de ciberseguridad (Escudero, 2016).

A nivel internacional, se argumenta, que los ataques cibernéticos pueden generar tensiones internacionales al ser vistos como una forma de guerra no convencional, lo que lleva a una mayor militarización y conflictos entre países. Por otro lado, otros señalan que los ataques cibernéticos son simplemente una forma de espionaje o sabotaje que existe desde hace años, sin necesariamente generar tensiones significativas en las relaciones entre Estados.

En la práctica, existe una contradicción en cómo los Estados actúan frente a los ataques cibernéticos. Aunque la mayoría de los países reconocen la importancia de la ciberseguridad y trabajan en medidas para proteger sus sistemas, también existe una tendencia a utilizar ataques cibernéticos como herramientas de política exterior. Algunos países han sido acusados de llevar a cabo ataques cibernéticos como forma de intimidación o para obtener ventajas en disputas políticas o comerciales, lo que genera tensiones significativas en las relaciones internacionales (Lewis, 2018 y Arquilla, & Ronfeldt, 1997). Sin embargo, la respuesta a estos ataques varía, y muchos países optan por no atribuir públicamente los ataques o responder con acciones militares o diplomáticas claras.

Según el análisis anterior la interrogante que se plantea la presente investigación es la siguiente: ¿Cómo los ataques cibernéticos pueden generar tensiones internacionales y qué estrategias se pueden implementar para prevenir y mitigar estas tensiones? Por lo que el objetivo de esta investigación es analizar la relación entre los ataques cibernéticos y las tensiones internacionales, así como proponer estrategias eficientes para prevenir y mitigar dichas tensiones.

Hipótesis: Los ataques cibernéticos pueden crear tensiones internacionales en las relaciones políticas y económicas debido a su capacidad para causar daño a infraestructuras vitales, obtener información confidencial y violar la privacidad de los Estados.

La ciberseguridad se ha convertido en un tema crucial en las relaciones internacionales debido al aumento de los ataques cibernéticos y su capacidad para afectar a múltiples sectores, como el militar, el económico y el político. En el ámbito militar, los ataques cibernéticos pueden dirigirse a las infraestructuras de defensa de

un Estado, comprometiendo su capacidad para responder a amenazas y generando inestabilidad en la región. Según Arquilla y Ronfeldt, (1997), la ciberguerra se ha convertido en una forma de conflicto emergente que puede desencadenar tensiones entre Estados y aumentar el riesgo de escalada.

En el ámbito económico, los ataques cibernéticos pueden tener consecuencias desastrosas. Según Lewis (2018), el cibercrimen y los ciberataques pueden causar pérdidas económicas significativas, erosionar la confianza en las transacciones digitales y obstaculizar el comercio internacional. Esto puede generar tensiones entre los Estados afectados y los presuntos perpetradores, así como provocar conflictos comerciales y sanciones.

Además, los ataques cibernéticos pueden violar la privacidad y la soberanía de los Estados al obtener información confidencial. Según Escudero (2016), la ciberespionaje y la injerencia en asuntos internos pueden causar fricciones diplomáticas y debilitar la confianza entre los Estados. Este tipo de ataques pueden desencadenar represalias y generar tensiones geopolíticas.

En este sentido la importancia de tratar el tema de la ciberseguridad en las relaciones internacionales radica en que los ataques cibernéticos representan una amenaza cada vez más real y recurrente en el escenario global. Estos ataques pueden tener consecuencias graves, tanto a nivel económico como político y social, y pueden generar tensiones y conflictos entre Estados. Por lo tanto, es esencial comprender y abordar adecuadamente esta problemática, promoviendo la cooperación internacional y la implementación de medidas de ciberseguridad efectivas. Solo a través de un enfoque integral y colaborativo, será posible hacer frente a los desafíos que plantea la ciberseguridad en el ámbito de las relaciones internacionales.

Ciberseguridad en las relaciones internacionales y ataques cibernéticos

La ciberseguridad en las relaciones internacionales se refiere a la protección de los sistemas de información y comunicación en el ámbito de las relaciones entre países (Johnson, 2010). A medida que las tecnologías de la información y la comunicación (TIC) se han vuelto más integradas en la sociedad y en las operaciones gubernamentales, también han surgido nuevas amenazas y vulnerabilidades relacionadas con la ciberseguridad (Australian Government Department of Home Affairs, 2020).

En el contexto de las relaciones internacionales, la ciberseguridad se centra en proteger la infraestructura crítica de un país, como sistemas de energía, transporte, comunicaciones y defensa de posibles ataques cibernéticos. También implica proteger la seguridad y la privacidad de la información sensible, como datos diplomáticos, militares o financieros, frente a ciberespionaje, ciberataques o cibercrimen (Heap, *et al*., 2016). La ciberseguridad en las relaciones internacionales es importante debido a que los países dependen cada vez más de las TIC y están cada vez más interconectados digitalmente (Rid, & Moore, 2014). Un ataque informático a un país puede tener consecuencias graves, desde el robo de información sensible hasta el sabotaje de infraestructuras críticas o el compromiso de la seguridad nacional.

Para abordar estos desafíos, los países colaboran a nivel internacional para establecer normas y acuerdos en materia de ciberseguridad, promover la cooperación en la lucha contra el ciberdelito y desarrollar capacidades para la defensa cibernética (Vacca, 2014). Estos esfuerzos incluyen la participación en organizaciones internacionales como la ONU, la OTAN y foros de cooperación como el Grupo de Expertos Gubernamentales sobre el Ciberespacio de las Naciones Unidas (Mitnick, & Simon, 2005).

Ataques cibernéticos: sus tipos

Los ataques cibernéticos son acciones maliciosas llevadas a cabo por individuos o grupos con el objetivo de comprometer la seguridad de sistemas informáticos, redes o dispositivos electrónicos. Estos ataques pueden tener diferentes propósitos, como robar información confidencial, interrumpir servicios en línea, dañar sistemas o llevar a cabo fraudes (Norton, 2022, Segerson, Huh, J., & Grubesic, 2016 y Cimpanu, 2020).

Los ataques cibernéticos son uno de los principales desafíos que enfrenta actualmente la sociedad digitalizada. Estos ataques se llevan a cabo por personas o grupos con el objetivo de acceder, alterar, robar o dañar información sensible o sistemas informáticos. Estos ataques no solo afectan a empresas, gobiernos u organizaciones, sino también a usuarios individuales. Desde la pérdida de datos personales y financieros, hasta el robo de identidad o el acceso no autorizado a cuentas en línea, los ataques cibernéticos representan una amenaza seria para la privacidad y seguridad de las personas (Symantec, 2017).

Para combatir los ataques cibernéticos, es fundamental mantenerse informado sobre las posibles técnicas utilizadas por los atacantes y tomar medidas preventivas, como utilizar contraseñas fuertes, mantener el software actualizado y tener instalado un buen antivirus. También es importante contar con una buena educación en ciberseguridad y fomentar una cultura de protección y cuidado de la información en todos los niveles de la sociedad.

Tipos de ataques cibernéticos

Existen diferentes tipos de ataques cibernéticos, algunos de los más comunes son **(**Clarke, 2017, Kyriakidis, et al., 2017, Rid, & Moore, 2014, Stuttard, & Pinto, 2011 y Cimpanu, 2020**)*:***

Malware: consiste en la introducción de software malicioso en un sistema, como virus, gusanos, troyanos o ransomware, con el objetivo de dañar o comprometer la seguridad del sistema.

Phishing: es una técnica de ingeniería social en la que los atacantes se hacen pasar por entidades confiables para engañar a los usuarios y obtener información personal o credenciales de acceso a cuentas.

Ataques de fuerza bruta: en este tipo de ataque, se intenta descifrar contraseñas probando diferentes combinaciones hasta encontrar la correcta.

Denegación de servicio (DoS): consiste en inundar un sistema o red con una gran cantidad de solicitudes, lo que provoca su saturación y la interrupción de los servicios. Una ampliación de este es el ataque de **denegación de servicio distribuido (DDoS)**

Ataques de inyección: se aprovechan de vulnerabilidades en las aplicaciones web para inyectar código malicioso y obtener acceso no autorizado al sistema.

Ingeniería social: Este ataque se basa en la manipulación psicológica de los usuarios para obtener información confidencial. Los ciberdelincuentes pueden utilizar llamadas telefónicas, mensajes de texto o correos electrónicos para hacerse pasar por una persona de confianza y obtener datos sensibles.

Ataques de ransomcloud: Se trata de un tipo de ataque de ransomware que se dirige específicamente a los servicios de almacenamiento en la nube. El objetivo es cifrar los archivos almacenados en la nube y exigir un rescate para desbloquearlos.

Casos de ataques cibernéticos: su impacto en las relaciones internacionales

Ataque cibernético a Sony: En 2014, un grupo de hackers respaldados por Corea del Norte atacó la empresa de entretenimiento Sony Pictures. Los hackers filtraron información confidencial, correos electrónicos y películas inéditas, lo que resultó en daños económicos significativos para Sony. Además, este ataque exacerbó las tensiones políticas entre Estados Unidos y Corea del Norte, lo que tuvo un impacto en las relaciones bilaterales y en la geopolítica de la región.

Ataque cibernético a Estonia en 2007: En 2007, Estonia sufrió un ataque cibernético masivo que afectó a su infraestructura digital, incluyendo sistemas gubernamentales, medios de comunicación y servicios bancarios. Se cree que el ataque fue llevado a cabo por Rusia en respuesta a una disputa política entre los dos países. El ataque tuvo un impacto económico significativo, ya que muchos ciudadanos y empresas estonias dependían de servicios digitales, lo que provocó interrupciones en las operaciones comerciales y financieras. También tuvo un impacto político, ya que aumentó las tensiones entre Estonia y Rusia, y llevó a la OTAN a establecer un Centro de Excelencia en Ciberdefensa en el país.

Ataque cibernético a Ucrania: En 2015 y 2016, Ucrania sufrió una serie de ataques cibernéticos que afectaron la infraestructura eléctrica del país. Estos ataques fueron atribuidos a Rusia y resultaron en apagones masivos en algunas áreas, lo que tuvo un impacto económico significativo en el país. Además, este ataque tuvo implicaciones políticas, ya que aumentó las tensiones entre Ucrania y Rusia, y culturales, ya que puso de relieve la creciente importancia de la ciberseguridad en el panorama internacional.

Actores involucrados: motivaciones y objetivos

En el ámbito de los ataques cibernéticos, existen diversos actores que pueden llevar a cabo este tipo de acciones. Ente los actores más destacados están (Valdés, 2021, Cimpanu, 2020, y Landler, 2018):

Los estados-nación son actores poderosos que pueden llevar a cabo ataques cibernéticos tanto para obtener información como para llevar a cabo acciones de sabotaje. Estos ataques suelen estar motivados

por razones políticas, como la obtención de información estratégica o la desestabilización de otros países. Ejemplos de estados-nación conocidos por llevar a cabo ataques cibernéticos son Rusia, China, Estados Unidos y Corea del Norte.

Los ciberdelincuentes, también conocidos como hackers, son individuos o grupos que realizan ataques cibernéticos con el objetivo de obtener beneficios económicos. Estos ataques pueden incluir el robo de información personal o financiera, extorsiones y fraudes. Los ciberdelincuentes suelen actuar de forma independiente, pero también pueden formar parte de organizaciones criminales más grandes. Algunos ejemplos de grupos de ciberdelincuentes conocidos son Anonymous y Lizard Squad.

Grupos terroristas han comenzado a utilizar el ciberespacio como una herramienta para llevar a cabo acciones de propaganda, reclutamiento y sabotaje. Estos grupos pueden utilizar técnicas de hacking para acceder a información sensible, interrumpir servicios en línea o difundir propaganda. Ejemplos de grupos terroristas que han llevado a cabo acciones cibernéticas son ISIS y Al-Qaeda.

Las ***motivaciones y objetivos*** de estos actores pueden variar dependiendo de sus características específicas. Los estados-nación, por ejemplo, pueden llevar a cabo ataques cibernéticos con el objetivo de obtener información estratégica, llevar a cabo acciones de sabotaje o influir en las decisiones políticas de otros países. Los ciberdelincuentes, por otro lado, buscan obtener beneficios económicos a través del robo de información personal o financiera. Los grupos terroristas, por su parte, pueden utilizar los ataques cibernéticos como una herramienta más para difundir propaganda, reclutar seguidores o desestabilizar sociedades (Symantec, 2017).

Consecuencias de los ataques cibernéticos en las relaciones internacionales

Los ataques cibernéticos son una forma de agresión que utiliza la tecnología para comprometer la seguridad y la confidencialidad de los sistemas informáticos de una entidad, ya sea un estado o una organización. Estos ataques pueden tener un impacto significativo en la confianza entre estados y generar tensiones que pueden desencadenar conflictos (Greenwald, 2013). En este sentido, es importante analizar cómo los ataques cibernéticos pueden socavar la confianza y generar tensiones entre estados.

Los ataques cibernéticos en las relaciones internacionales pueden tener varias consecuencias negativas, incluyendo (Marozzi, 2018, Ratti, 2017, Wright, 2019, Nishihata, 2009, Biersteker, 2014):

Provocan desconfianza entre los estados, ya que estos actos violan la seguridad y la privacidad de los sistemas y la información. Esta falta de confianza puede afectar las relaciones diplomáticas y hacer que sea más difícil para los países cooperar en temas de interés mutuo.

Generan tensiones y conflictos entre los estados. Si se descubre que un estado es responsable de un ataque cibernético, el estado afectado puede tomar represalias, lo que puede desencadenar una escalada de hostilidades y provocar conflictos políticos y militares.

Causan daños económicos significativos. Por ejemplo, los ataques dirigidos a infraestructuras clave, como los sistemas financieros o las redes eléctricas, pueden tener un impacto devastador en la economía de un país. Además, los ataques cibernéticos pueden resultar en robos de propiedad intelectual y secretos comerciales, lo que puede debilitar la competitividad económica de un país.

Tienen implicaciones significativas para la seguridad nacional. Por ejemplo, los ataques cibernéticos pueden ser utilizados para obtener información sensible sobre la defensa de un país, lo que puede comprometer la seguridad del país y su capacidad para proteger a sus ciudadanos.

Dificultan la cooperación internacional en temas de seguridad cibernética. Si se percibe que un estado no está tomando las medidas adecuadas para prevenir o responder a los ataques cibernéticos, otros estados pueden ser menos propensos a cooperar con ese estado en temas de ciberseguridad, lo que puede frenar los esfuerzos globales para abordar los desafíos cibernéticos.

Pueden afectar la infraestructura crítica de un Estado, como el sistema eléctrico, los servicios de agua o las redes de transporte. Estos ataques pueden causar interrupciones en los servicios básicos, afectando la economía y el bienestar de la población. Un ejemplo de esto es el ataque cibernético que sufrió Ucrania en 2015, donde se interrumpió el suministro de energía en varias regiones del país. Este incidente generó tensiones entre Ucrania y Rusia, ya que se sospechaba que el ataque provenía de actores estatales rusos

Comprometen la seguridad nacional de un estado, permitiendo a actores maliciosos acceder a información confidencial, como documentos gubernamentales o datos de inteligencia. Esta violación de la seguridad nacional puede generar sospechas y tensiones entre estados, especialmente si se sospecha que el ataque proviene de actores estatales. Un ejemplo notable de esto es el ataque cibernético sufrido por la Agencia Nacional de Seguridad (NSA) de Estados Unidos en 2013, donde se filtraron documentos clasificados que revelaban programas de vigilancia masiva. Este incidente generó tensiones diplomáticas entre Estados Unidos y varios países

Pueden tener repercusiones en la estabilidad política de un estado. Por ejemplo, un ataque cibernético puede ser utilizado para interferir en las elecciones de un país, afectando la confianza de la población en el sistema democrático y generando tensiones internas. Un ejemplo reciente de esto es el supuesto ataque cibernético ruso durante las elecciones presidenciales de Estados Unidos en 2016, donde se acusó a Rusia de interferir en el proceso electoral.

Implicaciones para la diplomacia, el comercio y la cooperación internacional

Los ataques cibernéticos pueden tener un gran impacto en diferentes áreas, como la diplomacia, el comercio, la seguridad nacional y la cooperación internacional. Aquí están algunas formas en las que estos ataques pueden afectar estas áreas (Schmitt, 2017, Rid, & Perez, 2018 y Clarke, 2017):

En el contexto de la diplomacia, los ataques cibernéticos pueden comprometer la comunicación y la confianza entre los estados y los actores internacionales. Pueden interrumpir las redes diplomáticas y filtrar información delicada, lo que puede socavar las relaciones entre países y dificultar la cooperación en temas diplomáticos y políticos.

Para el caso del comercio, pueden afectar el comercio internacional al comprometer los sistemas de información y las redes de empresas y organizaciones. Esto puede resultar en el robo de propiedad intelectual, datos comerciales confidenciales y la interrupción de las operaciones comerciales. Además, los ataques pueden dañar la reputación de las empresas y disminuir la confianza de los consumidores.

Son un medio de obstaculizar la cooperación entre países al socavar la confianza y afectar la capacidad de intercambio de información y datos (Wright, 2019). Esto puede dificultar la coordinación en asuntos de seguridad, la lucha contra el cibercrimen y la cooperación en áreas de interés común, como el cambio climático o la salud global.

Los ataques cibernéticos pueden poner en peligro la seguridad nacional de un país al comprometer las infraestructuras críticas, como los sistemas de energía, transporte y comunicaciones. Esto puede provocar interrupciones en los servicios públicos y poner en riesgo la seguridad de los ciudadanos. Además, los ataques cibernéticos también pueden ser utilizados para robar información clasificada o confidencial, lo que puede comprometer la seguridad y la defensa de un país.

Políticas y estrategias implementadas por los estados para prevenir y mitigar los ataques cibernéticos

Las políticas y estrategias implementadas por los estados para prevenir y mitigar los ataques cibernéticos varían en función de cada país y su nivel de desarrollo en materia de seguridad cibernética. Algunas de las principales políticas y estrategias implementadas incluyen (Herath, & Moitra, 2019, Lewis, J. A. (2012, Schmitt, 2017, Segerson, *et al*., 2016).

Marco legal y normativo

Los estados implementan leyes y regulaciones que establecen las responsabilidades y requisitos para las entidades públicas y privadas en materia de seguridad cibernética. Estas leyes pueden incluir la obligación de adoptar medidas de seguridad, reportar incidentes, y proteger los datos personales de los ciudadanos.

Creación de agencias y centros de ciberseguridad

Muchos estados han creado agencias o centros especializados en ciberseguridad para coordinar y ejecutar las políticas y estrategias de seguridad cibernética. Estas entidades son responsables de monitorear y proteger las infraestructuras críticas, responder a incidentes cibernéticos, y promover la concienciación y educación en seguridad cibernética.

Cooperación internacional

Los estados trabajan en colaboración con otros países y organizaciones internacionales para compartir información sobre amenazas cibernéticas, intercambiar mejores prácticas y coordinar respuestas a incidentes. Estas colaboraciones pueden incluir acuerdos de cooperación bilateral o multilateral, participación en ejercicios de ciberseguridad conjuntos, y la creación de mecanismos de alerta temprana.

Promoción de la concienciación y educación en seguridad cibernética

Los estados implementan campañas de concienciación pública y programas educativos para promover la seguridad cibernética. Estos programas informan a los ciudadanos sobre las amenazas cibernéticas, brindan consejos sobre cómo protegerse y promueven buenas prácticas en el uso de la tecnología.

Colaboración con el sector privado

Los estados trabajan en colaboración con el sector privado para desarrollar y promover mejores prácticas en materia de seguridad cibernética. Esto puede incluir la participación de expertos del sector privado en el diseño de políticas y estrategias, así como la promoción de estándares y certificaciones de seguridad cibernética en los sectores críticos.

Importancia de la cooperación internacional en la lucha contra los ataques cibernéticos

La cooperación internacional es de vital importancia en la lucha contra los ataques cibernéticos debido a varias razones (Council of the European Union, 2013, Council on Foreign Relations, 2019), Greenwald, 2013, Deibert, & Crete-Nishihata, 2009):

Los ataques cibernéticos suelen ser internacionales en su alcance y son perpetrados por grupos distribuidos en diferentes países. La cooperación internacional permite el intercambio de información sobre las amenazas y los métodos utilizados por los ciberdelincuentes, lo que permite a los países y organizaciones estar más preparados y responder de manera más efectiva a los ataques.

La cooperación internacional facilita la colaboración entre los diferentes países y organizaciones involucradas en la ciberseguridad. Esto permite la coordinación de esfuerzos en la identificación, prevención y respuesta a los ataques cibernéticos. Además, se pueden establecer mecanismos de colaboración para compartir las mejores prácticas en ciberseguridad y desarrollar estándares comunes.

En relación al fortalecimiento de capacidades, la cooperación internacional puede ayudar a los países en desarrollo a fortalecer sus capacidades en ciberseguridad. Esto puede incluir la capacitación de personal, el intercambio de conocimientos y la transferencia de tecnología. Al fortalecer las capacidades de los países más vulnerables, se contribuye a la seguridad cibernética a nivel global.

Contribuye a dale persecución de los ciberdelincuentes, muchos ciberdelincuentes operan desde países donde no hay una legislación adecuada o una cooperación insuficiente en la persecución de los delitos cibernéticos. La cooperación internacional puede facilitar la colaboración entre las autoridades nacionales y la extradición de los delincuentes para enfrentar la justicia.

Permite la protección de las infraestructuras críticas, como sistemas financieros, de energía y de transporte, son cada vez más interconectadas a nivel global. La cooperación internacional puede ayudar a proteger estas infraestructuras de los ataques cibernéticos, ya que requieren una respuesta coordinada y una colaboración continua entre diferentes países y organizaciones.

Análisis de casos

El ciberespionaje entre China y Estados Unidos ha sido un tema de preocupación durante años. Siendo uno de los casos más conocidos de tensiones internacionales generadas por ataques cibernéticos. Ambos países han sido acusados de llevar a cabo ataques cibernéticos sofisticados para robar información clasificada y propietaria, así como también para obtener ventajas económicas y militares, lo que ha generado un ambiente de desconfianza y tensión en sus relaciones bilaterales.

Un ejemplo destacado de este conflicto fue el caso de la empresa estadounidense Mandiant, que en 2013 reveló una unidad militar china responsable de ciberespionaje hacia objetivos estadounidenses. Según Mandiant, esta unidad, conocida como APT1, estaba ubicada en un edificio en Shanghái y había llevado a cabo numerosos ataques cibernéticos a empresas e instituciones estadounidenses.

En este ámbito las respuestas y medidas adoptadas por los actores involucrados para abordar estos problemas han sido las siguientes Lewis, J. (2018, Wright, 2019, Nishihata, 2009, Heap, Valleriani, A., & Ziemer, 2016 y Biersteker, 2014).:

China:

Negación y desafío: China ha negado repetidamente cualquier implicación en actividades de ciberespionaje. Han desafiado las acusaciones realizadas por Estados Unidos y otros países, argumentando que ellos también han sido víctimas de ataques similares.

Promulgación de leyes: China ha promulgado varias leyes y regulaciones para abordar los problemas de ciberseguridad. La ley de Seguridad Cibernética de 2017 impone restricciones a las compañías extranjeras y exige que cumplan con requisitos de seguridad establecidos por las autoridades chinas. Sin embargo, algunas de estas regulaciones se han visto como obstáculos para el acceso abierto a la información y la libre competencia en el mercado.

Tratados y acuerdos internacionales: China ha estado dispuesta a participar en tratados y acuerdos internacionales para abordar los problemas de ciberseguridad. Han participado en diálogos bilaterales y multilaterales con otros países, incluido Estados Unidos, para establecer normas y mecanismos de cooperación en el ámbito de la seguridad cibernética.

Estados Unidos:

Aumento de la conciencia pública: Estados Unidos ha buscado aumentar la conciencia pública sobre la amenaza del ciberespionaje chino. Han llevado a cabo investigaciones y han hecho públicos los casos de espionaje chino para educar al público y presionar a China a tomar medidas.

Respuesta militar: Estados Unidos ha adoptado medidas defensivas y ofensivas para abordar el ciberespionaje chino. Han fortalecido su capacidad de defensa cibernética y han realizado ataques cibernéticos preventivos para disuadir y contrarrestar los ataques (United States Department of Homeland Security, 2018).

Sanciones y medidas económicas: Estados Unidos ha impuesto sanciones y medidas económicas a empresas y personas relacionadas con el ciberespionaje chino. Han buscado cortar el acceso de China a tecnología y recursos clave, y han presionado a otros países para que limiten su cooperación con empresas chinas sospechosas de actividades cibernéticas ilegales.

En los años siguientes, se han llevado a cabo negociaciones diplomáticas entre ambos países para abordar estas tensiones. Se han realizado reuniones bilaterales y se han establecido mecanismos de diálogo, como el Diálogo Estratégico y Económico China-Estados Unidos, para discutir temas relacionados con la seguridad cibernética.

Sin embargo, a pesar de estos esfuerzos, las tensiones siguen existiendo y los ciberataques continúan siendo un problema entre China y Estados Unidos. Esto destaca los desafíos que implica abordar los conflictos cibernéticos a nivel internacional y la necesidad de establecer normas claras y acuerdos mutuos para prevenir y responder a estos ataques.

En general, el ciberespionaje entre China y Estados Unidos sigue siendo un desafío y una fuente de tensión entre los dos países. Aunque ambos han tomado medidas para abordar el problema, persisten desafíos en términos de confianza mutua, respeto de los derechos y la privacidad de los ciudadanos y la competencia justa en el ámbito económico. Lograr un equilibrio adecuado entre la seguridad cibernética y la apertura digital sigue siendo un objetivo difícil de alcanzar (Tsagourias, & Buchan, 2014).

Implicaciones legales y éticas en el contexto de las relaciones internacionales

Las implicaciones legales de los ataques cibernéticos en el contexto de las relaciones internacionales son significativas y complejas. A medida que el ciberespacio se convierte en un nuevo campo de batalla en el ámbito internacional, es crucial comprender cómo los ataques cibernéticos afectan las normas y leyes internacionales (Herath, Moitra, 2019 y Valdés, 2021).

En primer lugar, los ataques cibernéticos violan la soberanía nacional de un país. Según el derecho internacional, cada país tiene el derecho de controlar y proteger su territorio y sus sistemas de información. Los ataques cibernéticos que involucran la infiltración a sistemas y redes de otro país pueden

ser considerados como una violación de su soberanía. Esto puede desencadenar disputas diplomáticas y tensiones entre países.

Los ataques cibernéticos son considerados actos de guerra. Si un ataque cibernético causa daños significativos, como la destrucción de infraestructuras críticas o la pérdida de vidas humanas, podría ser tratado como un acto de guerra. La Carta de las Naciones Unidas prohíbe el uso de la fuerza en las relaciones internacionales, y los ataques cibernéticos pueden caer dentro de esta definición de uso de la fuerza (Johnson, 2010).

Sin embargo, uno de los desafíos principales en el ámbito legal internacional es atribuir con certeza un ataque cibernético a un Estado en particular. Los ataques cibernéticos a menudo pueden ser llevados a cabo por actores no estatales o por Estados actuando a través de intermediarios o de forma encubierta. Esto dificulta la responsabilidad y las represalias legales.

Los ataques cibernéticos en el contexto de las relaciones internacionales también plantean varias implicaciones éticas, entre las cuales se pueden destacar las siguientes (Kyriakidis, Zabbas, Papathanasiou, & Polemi, 2017 y Lee, 2015):

Los ataques cibernéticos violan la soberanía de un país al infiltrarse en sus sistemas de infraestructura crítica, como centrales eléctricas, comunicaciones o plantas nucleares. Esto plantea cuestiones éticas en cuanto al respeto y la no interferencia en los asuntos internos de otro Estado.

Son utilizados con fines de espionaje para obtener información confidencial de gobiernos o empresas extranjeras. Esto plantea preocupaciones éticas en términos de privacidad y confidencialidad de la información.

Contribuyen a difundir información falsa o desinformación con el objetivo de manipular la opinión pública o influir en procesos políticos. Esta práctica plantea cuestiones éticas en cuanto a la honestidad y la transparencia en las relaciones internacionales.

Afectan a la población civil al interrumpir servicios básicos como la energía o las comunicaciones. Esto plantea cuestiones éticas en cuanto a la protección de los derechos humanos y la responsabilidad de los Estados en evitar daños innecesarios a la población.

Con respecto a la responsabilidad y atribución, los ataques cibernéticos son difíciles de atribuir a un Estado o entidad en particular, lo que plantea cuestiones éticas en términos de responsabilidad y rendición de cuentas. Es importante determinar quién es responsable de un ataque y tomar las medidas adecuadas para evitar represalias injustas o acciones punitivas innecesarias.

Cuestiones éticas que plantea la Ciberseguridad

La ciberseguridad plantea numerosas cuestiones éticas, especialmente en lo que respecta a los límites de la vigilancia y la privacidad en línea. A medida que aumentan los ataques cibernéticos y se vuelven más sofisticados, muchas organizaciones y gobiernos han ampliado sus medidas de vigilancia para protegerse. Sin embargo, esto plantea el dilema de hasta qué punto es aceptable la vigilancia en línea. Por un lado, la vigilancia puede ser necesaria para detectar y prevenir ataques cibernéticos, identificar a los perpetradores y proteger la seguridad de las personas y las organizaciones. Por otro lado, la vigilancia en línea invade la privacidad de las personas y afectar negativamente sus derechos fundamentales.

Es importante encontrar un equilibrio entre la necesidad de seguridad y la preservación de la privacidad individual. Las políticas de ciberseguridad deben establecer límites claros sobre qué tipos de vigilancia están permitidos, quién tiene acceso a los datos recopilados y cómo se utilizan esos datos. Esto garantizará que la vigilancia se utilice de manera justa y responsable, sin violar los derechos de las personas (Lewis, 2018). Es esencial proteger la integridad de los datos y evitar su mal uso. La seguridad cibernética no solo implica proteger la información personal, sino también garantizar la autenticidad y confidencialidad de los datos en general. La manipulación y el robo de datos tienen consecuencias graves, tanto a nivel individual como en la sociedad en general.

En última instancia, las cuestiones éticas relacionadas con la ciberseguridad deben abordarse de manera integral y considerar tanto la seguridad como la privacidad. Es necesario establecer políticas claras y mecanismos de control para proteger adecuadamente a las personas y las organizaciones de los ataques cibernéticos, al tiempo que se respetan sus derechos fundamentales (Lewis, 2012).

Estrategias y acciones de ciberseguridad a desarrollar frente a los ataques cibernéticos para mitigar las tensiones internacionales

Las tensiones internacionales pueden aumentar el riesgo de ataques cibernéticos, ya que los actores estatales y no estatales pueden aprovechar estas situaciones para llevar a cabo operaciones maliciosas en el ciberespacio. Por consiguiente, la ciberseguridad se convierte en una prioridad en este escenario, y es necesario desarrollar estrategias y acciones para mitigar estos ataques (Marozzi, 2018).

Existen varias ***estrategias de ciberseguridad*** que se pueden implementar para hacer frente a los ataques cibernéticos en un contexto de tensiones internacionales (Mitnick, & Simon, 2005, NATO Cooperative Cyber Defence Centre of Excellence, 2018, Poulsen, 2015, Norton, 2022):

La cooperación y el intercambio de información entre países es esencial para mitigar los ataques cibernéticos. Esto incluye compartir amenazas, vulnerabilidades y mejores prácticas en materia de ciberseguridad. Además, se pueden establecer acuerdos bilaterales o multilaterales para coordinar acciones conjuntas contra actores maliciosos.

Los países deben fortalecer su capacidad para defenderse de los ataques cibernéticos. Esto implica desarrollar sistemas de detección y respuesta temprana, establecer medidas de protección avanzada, como el cifrado de datos, y capacitar a personal en ciberseguridad.

La resiliencia cibernética, es fundamental, es importante que los países sean capaces de resistir y recuperarse rápidamente de los ataques cibernéticos. Esto implica desarrollar planes de contingencia y continuidad del negocio, así como realizar ejercicios y simulaciones para poner a prueba la capacidad de respuesta y recuperación.

Las infraestructuras críticas, como la energía, las comunicaciones y los servicios financieros, son objetivos comunes de los ataques cibernéticos en situaciones de tensiones internacionales. Por lo tanto, es necesario fortalecer la seguridad de estas infraestructuras, implementando medidas de protección y supervisión adicionales.

Los países deben trabajar juntos para establecer normas y reglas internacionales en el ámbito de la ciberseguridad. Esto puede incluir acuerdos sobre atribución de ataques cibernéticos, normas de conducta responsable en el ciberespacio y reglas para la protección de los derechos humanos en línea.

Acciones

Asegúrese de contar con un sistema de seguridad sólido y actualizado, que incluya firewalls, programas de detección de malware y actualizaciones regulares de software.

Brinde capacitación y concientización regular sobre seguridad cibernética a todos los empleados, para que estén informados sobre las amenazas y sepan cómo evitarlas.

Guarde copias de seguridad de sus datos importantes y actualícelas regularmente. Esto ayudará a protegerse contra el ransomware y a recuperarse más rápido si ocurre un ataque.

Garantice que todas las contraseñas sean únicas, complicadas y cambie regularmente las contraseñas. También puede utilizar autenticación de dos factores para una capa adicional de seguridad.

Mantener todos los programas y sistemas operativos actualizados con los últimos parches de seguridad. Esto ayuda a cerrar brechas conocidas que los hackers pueden usar.

Estar alerta a las señales de ataque, capacite a su personal para que esté atento a las señales de un posible ataque, como correos electrónicos sospechosos, actividades inusuales en la red, solicitudes de información confidencial, etc. Reportar cualquier sospecha pronto puede ayudar a prevenir daños.

Establecer políticas de acceso y permisos, solo otorgue acceso a los sistemas y datos necesarios para cada empleado y revíselo regularmente. Esto minimizará el riesgo de que un ataque se propague a través de credenciales comprometidas.

Tener un plan de respuesta a incidentes, desarrolle y practique un plan de acción detallado para responder rápidamente en caso de un ataque cibernético. Esto puede incluir pasos para mitigar el daño, notificar a las partes afectadas y restaurar los sistemas afectados.

Monitorear y auditar, implemente una solución de supervisión y auditoría de seguridad que le permita rastrear y registrar actividades sospechosas en su red. Esto puede ayudarlo a detectar y detener ataques antes de que causen grandes daños.

Contratar servicios de seguridad profesional, si no tiene experiencia interna en seguridad cibernética, considere contratar servicios externos de profesionales en seguridad de la información. Ellos pueden ayudarlo a evaluar y mejorar la seguridad general de su empresa y responder adecuadamente en caso de un ataque.

Mantén tu software actualizado: Actualiza regularmente tu sistema operativo, navegadores web y otros programas para asegurarte de tener las últimas medidas de seguridad implementadas.

Utiliza contraseñas fuertes: Crea contraseñas únicas y complejas que incluyan una combinación de letras, números y caracteres especiales. Evita usar contraseñas obvias o fáciles de adivinar.

Ten cuidado con los correos electrónicos sospechosos, no abra ni descargue archivos adjuntos de correos electrónicos de remitentes desconocidos o sospechosos. Estos correos electrónicos pueden contener malware o intentar engañarte para que reveles información personal.

Utiliza un software antivirus confiable, instala un programa antivirus actualizado y realiza análisis regulares para detectar y eliminar cualquier malware.

Evita acceder a sitios web no seguros, asegúrate de que los sitios web en los que ingresas información personal o financiera tengan un candado cerrado en la barra de direcciones y comiencen con "https" en lugar de "http".

No compartas información personal en línea, evita compartir información personal, como números de seguridad social o contraseñas, a través de correos electrónicos no seguros o en sitios web no confiables.

Sé cauteloso al usar redes Wi-Fi públicas: Evita realizar transacciones financieras o ingresar información confidencial mientras estás conectado a una red Wi-Fi pública, ya que estos puntos de acceso pueden ser inseguros. Si es necesario, utiliza una red privada virtual (VPN) para cifrar tu conexión.

Mantente al día con las últimas noticias y actualizaciones sobre ciberseguridad para conocer las nuevas técnicas de ataque y aprender cómo protegerte de ellas.

Conclusiones

Los ataques cibernéticos representan una amenaza significativa en el ámbito de las relaciones internacionales. La ciberseguridad debe ser abordada de manera integral y prioritaria, promoviendo la cooperación entre países, el intercambio de información y el desarrollo de estrategias conjuntas para hacer frente a esta creciente amenaza. A medida que la dependencia de la tecnología continúa aumentando, es vital que los actores internacionales trabajen juntos para proteger la seguridad y el bienestar de sus naciones.

Los ataques cibernéticos crean tensiones internacionales debido a la naturaleza transfronteriza de estos eventos y la dificultad para atribuir responsabilidades de forma precisa. Estos ataques pueden ir dirigidos tanto a gobiernos como a actores no estatales, lo que los convierte en una amenaza para la estabilidad mundial.

La ciberseguridad se ha convertido en un elemento clave en las relaciones internacionales, ya que los ataques cibernéticos pueden tener graves consecuencias para la seguridad nacional y la economía de un país. Estos ataques pueden afectar sistemas de infraestructura crítica, como energía, transporte y servicios financieros, lo que puede generar un gran impacto no solo en la nación afectada, sino también en sus relaciones con otros países.

Además, los ataques cibernéticos pueden ser utilizados como una herramienta por parte de los estados para obtener información sensible y confidencial de otros países, lo que puede comprometer la seguridad nacional y la privacidad de los individuos. Esto ha llevado a un aumento en la cooperación entre países para compartir información y desarrollar estrategias conjuntas de ciberseguridad.

Sin embargo, a pesar de la necesidad de cooperación internacional en ciberseguridad, también se han visto casos en los que los ataques cibernéticos han sido utilizados como una forma de agresión y guerra cibernética entre países. Esto ha generado tensiones y conflictos entre estados, aumentando la posibilidad de escalada y confrontación.

Referencias bibliográficas

Arquilla, J., & Ronfeldt, D. (1997). The advent of Netwar (No. MR-789-OSD). RAND NATIONAL DEFENSE RESEARCH INST SANTA MONICA CA.

Australian Government Department of Home Affairs. (2020). Cyber Security Strategy 2020. https://www.homeaffairs.gov.au/cyber-security-subsite-2020/Pages/cyber-security-strategy-2020.aspx>

Biersteker, T. (2014). The Politics of Cybersecurity in China: New Dilemmas for a Critical Theory of Security. Security Dialogue, 45(4), 372-389.

Cimpanu, C. (2020). A closer look at cyber espionage and cyberwarfare. ZDNet. https://www.zdnet.com/article/a-closer-look-at-cyber-espionage-and-cyberwarfare/

Clarke, R. A. (2017). Cyber war in perspective: Russian aggression against Ukraine. Journal of Strategic Security, 10(1), 3-18.

Council of the European Union. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/ec/139215.pdf

Council on Foreign Relations. (2019). Digital and Cyberspace Policy Program. https://www.cfr.org/programs/digital-and-cyberspace-policy-program>

Deibert, R., & Crete-Nishihata, M. (2009). Hacking back: Legitimate defense or escalating conflict in cyberspace? International Studies Review, 11(4), 728-736.

Escudero, J. (2016). Los ataques cibernéticos y sus implicaciones diplomáticas. LUSODCI. 7(1), 59-69.

Greenwald, G. (2013). NSA collected US email records in bulk for more than two years under Obama. *The Guardian*.

Heap, R., Valleriani, A., & Ziemer, U. A. (Eds.). (2016). *Critical infrastructure protection in homeland security*.

Herath, T., & Moitra, D. (2019). Geopolitical tensions and international cyberattacks: Understanding attribution, retribution, and punishment. *Journal of Public Affairs*, 19(4), e1900.

Johnson, T.A. (2010). Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare. *CRC Press*.

Kyriakidis, E., Zabbas, V., Papathanasiou, J., & Polemi, N. (2017). Ransomware: a case study on cybersecurity for critical infrastructures in the era of social media. In *The Palgrave Handbook of Cybercrime and Cybersecurity*, pp. 207-237. Palgrave Macmillan.

Landler, M. (2018). As Cyberwarfare Escalates Between U.S. and Russia, Can Digital Detente Be Far Behind? *The New York Times*. https://www.nytimes.com/2018/02/14/world/europe/russia-us-cyber-attacks.html>

Lee, J. (2015). The Sony Pictures hack: a cold war reloaded. Journal of Information Technology & Politics, 12(2), 196-210.

Lewis, J. (2018). Cyber Threats and Economic Warfare. Global Economics Monthly, 1(3).

Lewis, J. A. (2012). Cybersecurity and the threat to national security. *Journal of Homeland Security and Emergency Management*, 9(1), 1-15.

Marozzi, M. (2018). Cyber attacks and international law on the use of force: the case of the 2016 US election interference. International Affairs, 94(2), 337-359.

Mitnick, K.D., & Simon, W.L. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders, and Deceivers*. Wiley.

NATO Cooperative Cyber Defence Centre of Excellence. (2018). The 2007 Cyber Attacks on Estonia: A Problem of Attribution. Recuperado de https://ccdcoe.org/cyber-attacks-estonia-2007-attribute.html

Norton. (2022). What Are Cyberattacks? https://us.norton.com/internetsecurity-malware-what-is-a-cyberattack.html

Poulsen, K. (2015). Inside the hack of the century: how the FBI traced Sony hackers. WIRED. Recuperado de: https://www.wired.com/2015/04/sony-hack-north-korea/

Rand Corporation. (2018). Ataque cibernético contra Sony Pictures: evaluación retrospectiva y lecciones clave. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2349/RAND_RR2349.pdf

Ratti, R. (2017). Critical infrastructure protection in Ukraine in the wake of the 2015 cyber-attacks. European Security, 26(2), 224-241.

Rid, T., & Perez, C. (Eds.). (2018). The Oxford Handbook of Cybersecurity. Oxford University Press.

Schmitt, M. N. (2017). The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. *Cambridge University Press*.

Segerson, S., Huh, J., & Grubesic, T. H. (2016). Spatial analysis and modeling of cyber attacks, international tensions, and war. *Papers in Regional Science*, 95(1), 23-41.

Stuttard, D., & Pinto, M. (2011). *The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws*. Wiley.

Symantec. (2017). 2017 Internet Security Threat Report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

Tsagourias, N., & Buchan, R. (Eds.). (2014). Cyber Security and International Law. *Oxford University Press*.

United States Department of Homeland Security. (2018). National Cyber Strategy. https://www.dhs.gov/sites/default/files/publications/national-cyber-strategy-2018.pdf

Valdés, J. (2021). Guerra cibernética, una amenaza real. Universidad de Colima. https://www.ucol.mx/noticias/general/10653-guerra-cibernetica-una-amenaza-real.

Wright, J. Q. (2019). The Cyber Cold War: China, the United States, and Global Cyber Espionage. *Oxford Research Encyclopedia of International Studies*.