DICERE Revista de Derecho y Estudios Internacionales
Vol. 3 Nº 01 / 2026 / e-ISSN: 3028-886X

La Ciberseguridad como Desafío de la Seguridad Internacional: El caso de Estonia (2007)

Cybersecurity as a Challenge to International Security: The case of Estonia (2007)

DOI: https://doi.org/10.33324/dicere.v3i1.1114

Luis Andrade-Ponce, https://orcid.org/0009-0002-8127-4566 landrade.hcs@gmail.com
Universidade da Beira da Interior, Covilhã, Portugal.

Recibido: 23-03-2026 **Revisado:** 28-04-2026 **Aceptado:** 12-05-2026 **Publicado:** 30-05-2026

Resumen

Las ciberamenazas se han consolidado como un desafío central para la seguridad internacional en el contexto de la creciente digitalización de los Estados y las sociedades. Más allá de su dimensión técnica, estos ataques representan una nueva forma de conflicto que impacta directamente en la estabilidad política, económica y social, afectando tanto a instituciones públicas como a actores privados. El presente artículo analiza la evolución de las amenazas cibernéticas, como los ataques de denegación de servicio (DDoS), el phishing o el ransomware, no solo desde su funcionamiento, sino especialmente desde sus implicaciones en la seguridad estatal. A partir del estudio del ciberataque a Estonia en 2007, se examina cómo este evento marcó un punto de inflexión en la concepción de la soberanía digital y en la necesidad de cooperación internacional en materia de ciberseguridad. Se concluye que la ciberseguridad ha dejado de ser un asunto meramente técnico para convertirse en un elemento estratégico dentro de las relaciones internacionales contemporáneas.

Abstract

Cyber threats have emerged as a central challenge to international security in the context of increasing digitalization of states and societies. Beyond their technical dimension, these attacks represent a new form of conflict that directly impacts political, economic, and social stability, affecting both public institutions and private actors. This article analyzes the evolution of cyber threats—such as Distributed Denial of Service (DDoS) attacks, phishing, and ransomware—not only in terms of their operational mechanisms but, more importantly, through their implications for state security. Using the 2007 cyberattack on Estonia as a case study, the paper examines how this event marked a turning point in the understanding of digital sovereignty and the growing need for international cooperation in cybersecurity. It concludes that cybersecurity has evolved from a purely technical issue into a strategic component of contemporary international relations.

Cómo citar: Andrade-Ponce, L. (2026). La ciberseguridad como desafío de la seguridad internacional: El caso de Estonia (2007). *DICERE Revista De Derecho Y Estudios Internacionales, 3*(1), 34-49. https://doi.org/10.33324/dicere.v3i1.1114

Palabras clave

Ciberseguridad, Seguridad internacional, Soberanía digital, OTAN, Relaciones internacionales

Keywords

Cybersecurity, International Security, Digital sovereignty, NATO, International Relations

1 Introducción

Ciber es un término que se usa desde los años 50, con el cual se referían a los elementos cibernéticos o la ciencia que estudia el movimiento y control de animales y máquinas. Al pasar del tiempo, el término paso a ser un sinónimo de computarizado. Para los años 90, sale a relucir el término ciberespacio, que se refiere a un lugar figurado detrás de la electrónica de una computadora. En la actualidad, es utilizado para describir elementos de seguridad informática. En la actualidad, el concepto es utilizado para describir elementos de seguridad informática. Además, respecto avanzan las cuestiones sobre asuntos respecto al ciber especio y la incertidumbre frente a todo lo que abarca se van definiendo cierto tipo de normas, las cuales son legales y políticas. Donde "El primer grupo está relacionado con el derecho internacional, incluidas las normas que "tienen una obligación legalmente vinculante". El segundo grupo incluye normas que promueven una forma de comportamiento específica sin estar "sujeto a los mecanismos de aplicación legales (Gromilova, 2017, pág. 128)".

Las ciberamenazas, en la actualidad representan un gran malestar a nivel organizacional e individual, ya que la violación de la seguridad en muchas ocasiones se encuentra vulnerable, por lo digital que se ha vuelto el día a día de los seres humanos. Las amenazas online cambian con demasiada rapidez. Por esta razón es necesario reevaluar las distintas herramientas que se han implementado para prevenir dichos ataques.

Para contrarrestar estas ciberamenazas, se cuenta con la ciberseguridad, cuya disciplina tiene que ver con los mecanismos de protección de los datos e información de los equipos que utilizamos diariamente, como son los computadores, móviles, Smart-tv, servidores y todo aquello que se encuentre conectado a una red. Estas herramientas brindan mucha seguridad siempre y cuando se utilicen adecuadamente y los usuarios tengan consciencia de las implicaciones que trae el no tomar previsiones a la hora de utilizar los equipos.

Para Estonia, el año 2007 causo un gran impacto dentro de su seguridad nacional al convertirse en uno de los primeros países en recibir un ciberataque de gran magnitud y a la vez, pasar a ser uno de los pioneros en materia de ciberseguridad, estatutos el cual

1. Se hace referencia a los precedentes autovinculantes, persuasivos y los heterovinculantes conforme lo prescribía el artículo 19 de la Ley de Casación [decisiones ex CSJ].

DICERE Revista de Derecho y Estudios Internacionales
Vol. 3 Nº 01 / 2026 / e-ISSN: 3028-886X

sigue manteniendo hasta la actualidad. Por lo tanto, a partir del año 2007 podemos estar hablando del acontecimiento de una revolución digital en torno a la seguridad de los estados.

2 Revisión de la literatura

Las cyber amenazas son actos maliciosos que se dan en los medios digitales; a través de los cuales se ven perjudicadas la seguridad de las organizaciones, estados y de las personas al robarles información, proveer desinformación, dañar sus datos y por ende afectan la vida digital. Son ataques que van desde infiltraciones a infraestructuras hasta brechas de datos e incluso, pueden llegar a los ataques personales.

Las amenazas son variadas, van desde virus informáticos que implantan en los equipos celulares, electrónicos, así como la información que sustraen que posteriormente es utilizada con fines lucrativos y malintencionados, poniendo en riesgo las operaciones comerciales además de la salud. Estas provienen de fuentes de diversas índoles como son: bandas criminales, hackers, espías, entre otros. Una de las grandes complicaciones relacionadas a las amenazas cibernéticas es el tema de poder rastrear el ataque en base a la dirección IP, la cual no es siempre es originada desde el punto inicial del ataque, ya que puede cambiar constantemente de dirección. Por ejemplo, supongamos que "Una computadora controla el trabajo de defensa aérea de un adversario y no puede localizarlo físicamente. Si lo persigue con un ataque cibernético, ¿qué pasa si se encuentra en una nación neutral? ¿O en su propio territorio? La guerra cibernética complica las materias y los desafíos de las nociones tradicionales de neutralidad y soberanía (Farwell & Rohozinski, 2011, pág. 31)". Todos estos detalles vuelven más complicados el poder capturar a los hackers que inician los principales ataques cibernéticos alrededor del mundo.

2.1 Impacto de las ciberamenazas

Las ciber amenazas están en constante evolución. Por lo que los riesgos de ciberseguridad también han aumentado. Se han visto casos en los que los ataques cibernéticos han ocasionado un colapso en servidores de páginas gubernamentales, donde se han encontrado con programas que se diseñaron para sustraer información muy confidencial. Es por esto que es sumamente fundamental mantenerse en constante actualización, entender cuáles son los tipos de ataques, como funcionan y cuáles serían las medidas que se adoptarían para evitarlos.

Después del contexto de todo lo que engloba y puede ser entendido como una ciber amenaza tenemos que exponer la importancia de nuestro caso de estudio. Para entender mejor las consecuencias del ataque cibernético que sufrió Estonia tenemos que ubicar a este país en el mapa donde podemos contemplar a este territorio como una de las muchas fronteras que tiene Rusia, a partir de ese hecho ya existe motivos nacionalistas, culturales y de xenofobia que den cabida a cualquier otro conflicto mayor. Sin de dejar de lado el pasado que unen a ambas naciones que antiguamente conformaban a la Unión Soviética, se tomó en esta historia un punto de inflexión el cual es un soldado de bronce que representa un sím-

bolo de guerra que trascendió generaciones al estar colocado dentro de la capital Tallin. Aquella estatua militar estuvo a partir de 1947 y representaba la victoria soviética con el nombre de Monumento a los liberados de Tallin. A partir de la independencia de Estonia en 1991 aquel simbolismo continuo en el mismo lugar, pero con otro significado convirtiéndose "En un monumento para todos los que habían caído durante la Segunda Guerra Mundial. Sin embargo, estos cambios no impidieron que la estatua se convirtiera en el foco de disputas. Algunos rusos estonios organizaron celebraciones anuales cerca de la estatua el 9 de mayo, el llamado Día de la Victoria de Rusia, así como el 22 de septiembre, el aniversario de la "liberación" de Tallin (Alenius, Victory in exceptional war: The estonian main narrative of the cyber attacks in 2007. The Fog of Cyber Defence, 78., 2013, pág. 79)".

Con el pasar de los años las tensiones crecían alrededor de aquel soldado de bronce con gran significado de nacionalismo soviético por lo que era cuestión de tiempo para que los disturbios comenzaran. Los manifestantes o grupos conflictivos encontraron en el nuevo siglo y en el internet un nuevo mecanismo para agredir directamente a un país sin verse implicado de forma física con todo lo que representaría organizar un ataque estratégico. Por eso que esta nueva modalidad de ataque causó pánico entre los ciudadanos ya que nadie sabía de donde la agresión provenía, aunque sucedió el ataque de forma virtual produjo un caos enorme. Dejando al alcance de todo el mundo diferentes tipos de ciber amenazas las cuales vamos a explicar a continuación.

2.2 Tipos de ciberamenazas.

El incremento del uso de tecnologías digitales en las últimas décadas ha venido acompañado de una expansión significativa de las amenazas cibernéticas, las cuales ya no pueden ser entendidas únicamente desde una perspectiva técnica, sino como fenómenos con implicaciones directas en la seguridad internacional. Estas amenazas adoptan diversas formas, desde mecanismos sofisticados de intrusión hasta estrategias de manipulación dirigidas a individuos, instituciones y Estados. En este contexto, ataques como el ransomware, el phishing o las operaciones de denegación de servicio distribuido (DDoS) no solo afectan la integridad de los sistemas informáticos, sino que también generan impactos económicos, sociales y políticos que pueden alterar la estabilidad de un país.

Entre las amenazas más relevantes se encuentra el ransomware, el cual ha experimentado un notable crecimiento en los últimos años, especialmente en el contexto de la expansión del trabajo remoto y la digitalización de procesos organizacionales. Este tipo de ataque consiste en el bloqueo o cifrado de información crítica, impidiendo el acceso a sistemas y datos, con el objetivo de extorsionar a las víctimas. De manera complementaria, el phishing representa otra modalidad ampliamente utilizada, basada en el engaño y la manipulación psicológica de los usuarios para obtener información confidencial, como credenciales de acceso o datos financieros. Estas prácticas evidencian cómo las ciberamenazas combinan elementos tecnológicos y sociales, aprovechando tanto vulnerabilidades técnicas como comportamientos humanos.

No obstante, dentro del espectro de amenazas cibernéticas, los ataques de denegación de servicio distribuido (DDoS) adquieren una especial relevancia en el ámbito de las relaciones internacionales, debido a su capacidad para afectar infraestructuras críticas a gran escala. Este tipo de ataque se caracteriza por el envío masivo de solicitudes a servidores, con el fin de saturar su capacidad operativa y provo-

DICERE Revista de Derecho y Estudios Internacionales
Vol. 3 Nº 01 / 2026 / e-ISSN: 3028-886X

car la interrupción de servicios esenciales. Su importancia se refleja claramente en el caso de Estonia en 2007, donde este mecanismo fue utilizado para paralizar sitios gubernamentales, instituciones financieras y medios de comunicación, generando no solo un colapso digital, sino también inestabilidad social, pérdidas económicas y un aumento de las tensiones políticas con Rusia. La complejidad de estos ataques radica en su carácter distribuido, ya que, como señala Haataja (2017), "DDoS, las solicitudes de información fueron enviadas de forma masiva desde computadoras corruptas, teniendo un mecanismo diferente de las legitimateRequests que provienen de usuarios humanos, generando interrupción del funcionamiento de la infraestructura de información de la EstonianEntity" (p. 185). Este tipo de dinámica pone en evidencia las dificultades para atribuir responsabilidades en el ciberespacio, lo cual representa uno de los principales desafíos para el derecho internacional contemporáneo.

Asimismo, existen otras formas de ciberamenazas que, aunque operan a nivel más individual o micro, pueden tener efectos acumulativos relevantes en el plano macro. Entre ellas se encuentran los virus troyanos, que se presentan como software legítimo para infiltrarse en sistemas y permitir el acceso no autorizado; el spyware, orientado a la recopilación encubierta de información sensible; y el smishing, que utiliza mensajes de texto fraudulentos para redirigir a las víctimas hacia enlaces maliciosos. Estas modalidades reflejan la diversidad y adaptabilidad de las amenazas cibernéticas, las cuales evolucionan constantemente en función de los avances tecnológicos y los cambios en los patrones de interacción digital.

En conjunto, la proliferación de estas amenazas demuestra que la ciberseguridad no puede ser abordada exclusivamente como una cuestión técnica, sino como un componente fundamental de la agenda de seguridad internacional. La capacidad de estos ataques para trascender fronteras, afectar infraestructuras críticas y generar tensiones entre Estados subraya la necesidad de enfoques multidimensionales que integren aspectos tecnológicos, políticos y jurídicos en el análisis de la ciberseguridad contemporánea.

3 Metodología

Este articulo aborda el caso de ciberseguridad de Estonia del año 2007 y el impacto que tuvo en el mundo hasta la actualidad para dar a conocer los temas de seguridad en cuanto a los estados relacionados con el ciber espacio. Para entender todos los conceptos que engloba la seguridad dentro del internet se va a exponer los orígenes de este concepto, que se entiende por el termino de ciber seguridad y sobre todo desde un inicio el poder explorar cuales son las amenazas las cuales se puede sufrir en la red bajo esta modalidad de agresión. Es importante el explorar también el impacto de estos ataques cibernéticos debido a que los pueden sufrir desde Estados, organizaciones, empresas hasta el individuo común. Dentro de todos los casos de ciber ataque posibles decidí escoger el de Estonia por ser uno de los casos más importantes que marco la historia de la soberanía y seguridad nacional de un país dentro del internet. También a partir de este caso sucedieron situaciones en los años posteriores similares, que toma-

ron como modelo lo que sucedió en Estonia para poder mitigar los ciber ataques que sufrieron desencadenando estos hechos en la creación del Manual de Tallin dedicado a la interpretación de peligros en la red además de la protección de los estados dentro del ciber espacio.

La metodología del estudio de caso es la más apropiada para abordar el tema de ciberseguridad relacionado con lo que sucedió en Estonia en el año 2007 por lo tanto a través del uso de métodos cualitativos se va poder explorar en profundidad los factores políticos, técnicos y sociales brindando una mejor comprensión dentro de los contextos y las dinámicas subyacentes. El método utilizado será utilizar el análisis del contenido distribuido en base a este caso de estudio donde se buscará obtener un descripción detallada y contextualizada de los eventos que desencadenaron aquel hecho histórico que marco el futuro de la ciberseguridad. Utilizando las medidas que tomo el gobierno de Estonia de aquel entonces para llegar a pensar en otras alternativas en las cuales se pueda defender la soberanía de un estado dentro del internet.

El análisis se va a concentrar en como a partir de leer diversos artículos de diferentes autores los cuales expusieron sus perspectivas y comentarios en base al caso de estudio de Estonia 2007 se puede llegar a emitir comentarios críticos los cuales van a ayudar a fomentar una opinión más orientada sobre el accionar del gobierno de Estonia frente aquella problemática y que recomendaciones se pueden brindar para ayudar a otros estados con menor capacidad de desarrollo en cuento a las tecnologías a no ser vulnerables para estos ataques.

En cuanto a las conclusiones se expondrá las medidas en las que se pueden prevenir los ciberataques también se hará énfasis sobre el porqué Estonia se vuelto en un modelo a seguir en cuanto a la tecnología y la importancia de la cooperación internacional en cuanto a temas digitales para alcanzar un desarrollo avanzado en países en desarrollo.

4 Contexto del Ciberataque a Estonia en 2007+

Todo comienza con la reubicación de una estatua ubicada en la ciudad de Tallin, Estonia; conocida como "Soldado de Bronce de Tallin" la cual representaba al Ejército Rojo soviético. Esto provocó muchas protestas por parte de la comunidad de habla rusa en Estonia, y a la vez a Rusia llegaba información falsa, ya que decían que la estatua había sido destruida, lo que aumentó las tensiones, ya que, para los estonios de habla rusa, esa estatua simboliza la victoria soviética sobre los Nazis, en cambio para los nacidos en Estonia representaba el recordatorio de la ocupación soviética.

El 26 de abril de 2007 comenzaron disturbios y saqueos en la ciudad de Tallin, hubo fallecidos, personas heridas y muchos detenidos. El 27 de abril de 2007, Estonia comenzó a recibir una serie de ataques informáticos, que afectaron su infraestructura digital, y, por ende, al público en general, ya que los ataques fueron dirigidos a sitios web gubernamentales, bancos y medios de comunicación, mediante ataques de denegación de servicio distribuido (DDoS), (Fernandez, 2015), estos ataques se dieron hasta el 19 de mayo.

DICERE Revista de Derecho y Estudios Internacionales
Vol. 3 Nº 01 / 2026 / e-ISSN: 3028-886X

Los atacantes usaron botnets o redes de robots informáticos, con los que inundaron los servidores con tráfico masivo, provocando el colapso de los sistemas en línea. Esto hizo que el gobierno tomara como una medida bloquear todo el tráfico internacional, aislando al país del resto del mundo.

Hay que destacar que, aunque se dice que el ciberataque fue gestado por hackers rusos, realmente la autoría del mismo es un enigma. Luego del ciberataque, la relación entre Estonia y Rusia se ha deteriorado mucho más, sin llegar a algún enfrentamiento militar, manteniendo una buena relación con los demás países miembros de la OTAN.

4.1 ¿Qué medidas de Ciberseguridad abordó Estonia luego del ciberataque?

A raíz del ciberataque, Estonia se ha convertido en líder en el área de ciberseguridad y continúa desempeñando papel importante a nivel mundial. Modernizando gran parte de su territorio dentro de la modalidad virtual, proporcionando red de wifi público, incentivando las transacciones bancarias online y digitalizando la obtención de documentos o de procesos burocráticos. Este país se volvió pionero en cuanto a la tecnología y se puede resaltar la rápida respuesta que tuvieron en cuanto a contrarrestar el ataque cibernético del 2007. La comunidad internacional destaca siempre la manera competente y rápida en la cual "El gobierno pudo coordinar respuestas que solo causaron interrupciones a corto plazo en lugar de daños permanentes a su infraestructura de TI. Dando cabida para que las instituciones estatales puedan emplear su CERT, que coordinó las respuestas de TI entre especialistas gubernamentales y civiles (Gamreklidze, 2014, pág. 213)". Por lo tanto, a través de este ataque Estonia insistió en la importancia de la cooperación internacional frente a este tipo de amenazas y insto a la comunidad internacional que los ciberdelitos deberían ser considerados como un delito penal.

5 Análisis y discusión

5.1 Análisis de las tácticas y técnicas utilizadas en el ataque

Como lo hemos enfatizado durante toda la elaboración del trabajo el ataque cibernético a Estonia del 2007 es considerado uno de los mayores grandes ataques cibernéticos a nivel mundial por lo que es un hito histórico que desencadeno la posterior implementación de medidas de seguridad para combatir además de identificar las diferentes técnicas y tácticas empleadas por los hackers frente aquel suceso histórico del 2007 concentrado principalmente en la capital Tallin. Los ataques fueron implementados a partir de DDoS en donde la estrategia como ya revisamos en la revisión de literatura consistió en sobrecargar los servidores de la red con tráfico masivo para hacer los servidores inaccesibles produciendo un retraso en los servicios. Todo esto fue efectivo debido al uso de botnets (computadoras infectadas con malwere). Este método permitió a los atacantes distribuir las solicitudes desde miles de direcciones de IP diferentes, dificultando el poder encontrar de donde se originó la amenaza.

Al final estos ataques DDoS afectaron de forma perjudicial a los sitios web gubernamentales, bancos, medios de comunicación y otras infraestructuras críticas, provocando el colapso de todos los servicios en línea. Un reflejo de la magnitud de esta serie de

ataques para la población de este país es el completo colapso bancario debido a que "Los estonios realizan más del 98% de sus medios electrónicos bancarios. Por lo tanto, el impacto de los ataques de negación de servicio (DDoS) distribuidos de varias plantas (DDoS) que superaron todas las comunicaciones a la presencia en la web de los dos bancos más grandes del país por hasta dos horas y prestaron servicios internacionales parcialmente no disponibles durante días a la vez (Geers, 2009, pág. 6) ".

El resultado de los ataques demuestra la alta coordinación de los hackers, comenzando durante el 27 de abril del 2007 a partir de la controversia con el monumento soviético del Soldado de Bronce en Tallin. Dentro de este estallido cibernético el uso de proxies y los servicios de anonimato consiguieron el retrasar más de lo debido el poder rastrear la ubicación del origen de los ataques creando desafíos para responsabilizar al grupo de conflictivos. El interrumpir los servicios críticos y atraer la atención global hacia las vulnerabilidades en ciberseguridad causo pánico mundial a los demás estados para mejorar sus sistemas de defensa cibernética.

5.2 Evaluación de la respuesta de Estonia y sus medidas de mitigación

El ataque del 2007 además de poner en sus máximas capacidades la defensa cibernética del país también proporciono importantes informaciones para la gestión y el control de la ciber crisis. La respuesta rápida de este país fue admirable movilizando sus recursos técnicos y humanos para mitigar los efectos de los ataques DDoS. La rápida movilización del equipo CERT-EE fue fundamental gestionar la coordinación interna entre las diferentes agencias gubernamentales y el sector privado ayudo a la no propagación de la crisis cibernética además de restaurar los servicios afectados online. Lo importante es que esta eficacia dentro de la respuesta para controlar la amenaza cibernética ayudo a minimizar el tiempo de inactividad y restaurar la confianza pública en los servicios digitales.

A partir de este ataque Estonia invirtió seriamente en mejorar toda su infraestructura de ciberseguridad, dentro de estas mejoras se encuentran la actualización de los sistemas de seguridad, la adaptación de tecnologías avanzadas para mitigar los futuros ataques. Como una de las principales medidas para controlar las futuras ciber amenazas se creó el centro de excelencia de ciberdefensa cooperativa de la OTAN donde se proporcionó un ambiente para la investigación y el desarrollo en ciberdefensa, cooperación internacional y el intercambio de nuevas prácticas de control. Por otro lado, varias declaraciones por parte del gobierno de Estonia enfatizaron la necesidad de obtener apoyo para rechazar los ciberataques. Debido a esto "La aceleración de la construcción del centro de ciberdefensa de la OTAN en Estonia fue recibida con alegría y, además, existía el deseo de una reforma internacional en relación con la definición de ciberataques. Se consideró que los acuerdos internacionales existentes estaban obsoletos: no tomaban la cuestión lo suficientemente en serio, no tenían en cuenta el desarrollo tecnológico en este campo ni permitían una respuesta jurídica y práctica suficientemente eficaz (Alenius & Warren, 2012, pág. 22)". La creación del organismo CCDCOE posiciono a este país europeo como líder en la materia de ciberseguridad fomentando una relación de cooperación fuerte con los demás estados y organizaciones para fortalecer los mecanismos de seguridad.

5.3 Énfasis en la agenda de seguridad

Dentro del apartado de la agenda de seguridad de forma local se destaca la

DICERE Revista de Derecho y Estudios Internacionales
Vol. 3 Nº 01 / 2026 / e-ISSN: 3028-886X

implementación de la Seguridad Cibernética de Estonia 2014-2017 la cual es una guía para comprender la parte integral de la estrategia de seguridad en la cual incursiono el país. "El objetivo principal de esta estrategia actualizada es aumentar las capacidades de seguridad cibernética y concienciar a la población sobre las amenazas cibernéticas, garantizando así la confianza continua de sus ciudadanos en el ciberespacio. Para hacerlo de manera eficaz, esta estrategia describe varios subobjetivos que incluyen garantizar la protección de los sistemas de información subyacentes a servicios importantes, mejorar la lucha contra el delito cibernético, desarrollar capacidades nacionales de ciberdefensa, gestionar las amenazas a la ciberseguridad y promover y sincronizar la política internacional de ciberseguridad (Wong, Porter, Hokanson, & Xie, 2017, pág. 3)".

A partir de la implementación de la nueva agenda se ratifico la importancia de la ciberseguridad como una prioridad nacional en base a lo ocurrido en el 2007 donde también se busco actualizar la estrategia nacional para contrarrestar los ataques cibernéticos. Esta estrategia de la agenda de seguridad nacional se realizo para alinear las capacidades de ciberseguridad con las prioridades nacionales de defensa, economía digital y protección de datos. Una de las cosas mas destacables que trajo esta agenda fue el asentamiento de bases para la incrementación de la cooperación con otros países y organizaciones en asuntos relacionados al ciber espacio. Incentivando la practica de ejercicios de ciberdefensa como Locked Shields mediante el apoyo de la Unión Europea y la OTAN.

Antes del año 2007 el tema de ciberseguridad no era una prioridad dentro de la defensa nacional de muchos países. Este ataque le demostró al mundo entero la capacidad de los ciberataques para causar colapsos dentro de infraestructuras enteras, enseñando que la defensa de la soberanía nacional a través de la red no es un juego. Por eso en el año 2010, la Comisión Europea lanzo la Agenda Digital para Europa como una de las siete iniciativas emblemáticas de la Estrategia Europa 2020. Lo que se busco con esta medida fue además de impulsar la economía digital el también poder abordar los desafíos de seguridad cibernética en toda Europa. Para fortalecer todo lo relacionado con la ciberseguridad se creo una Agencia Europea de Seguridad de las Redes y de la información (ENISA), esta institución buscaba apoyar a los estados miembros en la prevención y el accionar frente a los ciber ataques. Frente a los objetivos buscaba la creación de la Agenda Digital de la UE se buscaba el crear una plataforma europea conjunta contra el cibercrimen frente a las posibilidades de que el crimen dentro del ciber espacio aumento debido a los factores de la globalización en base a las capacidades de expansión del internet. Bajo esa premisa el jefe del mando aliado de la transformación de la OTAN presento en el año 2012 la creación de un Centro Técnico de Capacidad de Respuesta a Incidentes Informáticos con sede en Mons, Bélgica. Por lo tanto, todas las acciones que tomen la UE y la OTAN en base al tema del ciberespacio son en base para poder conseguir prevenir futuras amenazas de ciber terroristas que buscan afectar a los estados.

Conforme la preocupación sobre lo desconocido del alcance que pueden tener los ciber ataques invadió a los demás países, se incrementó el pánico mundial a tal punto en el año 2011 potencias como Estados Unidos en voz del subsecretario de defensa de esa época Willian Lynn advirtió de forma alarmante tener que discutir las vulnerabilidades de la OTAN frente la mitigación del caso de Estonia, "existe potencial para capacidades que son mucho más destructivo... Estamos en gran medida en la fase de explotación/negación, pero la historia te dirá que alguien lo llevará al extremo (Herzog, 2011, pág. 55)".

5.4 Comparación con otros ciberataques similares

En la primera década del Siglo XXI se desencadenaron otros ataques cibernéticos posterior al caso de Estonia 2007 donde se resaltan los eventos que ocurrieron en Georgia 2008 y Kirguistán 2009 los cuales se ratificaron con más fuerza frente al panorama internacional la incentivación para la creación de forma urgente de algún estatuto que aborde las normas del ciberespacio además de exponer como siempre la cooperación internacional produce buenas resaltados frente a las grandes amenazas.

Dentro del contexto del caso del 2008 en Georgia se expone como este país y Rusia están en enfrentamientos armados debido a las regiones separatistas de Oestia del Sur y Abjasia. Este conflicto ya se venia desarrollando durante algunos años, además de tener raíces profundas en la historia política y étnica de la región incentivándose al momento de Georgia querer recuperar Osetia del Sur lo que provo una intervención militarizada en la zona por parte del ejercito ruso. Se expone como principal acontecimiento que llevo a "Rusia a lanzar tal ataque contra Georgia fue el brindar apoyo a los rusogeorgianos, que son principalmente georgianos de habla rusa y han estado luchando por su autonomía de Georgia desde que declararon su independencia en 1991. Rusia siempre ha sido comprensiva a su curso simplemente por su identidad y afiliación. A lo largo de los años han estallado una serie de conflictos, especialmente en 2004 y 2008 (Odoh, 2021, pág. 8)". Estas consecuencias desencadenaron la guerra cibernética en el territorio georgiano con el fin de que los militares rusos puedan prestar apoyo a las fuerzas de Osetia del Sur. A comparación de Estonia en esa época Georgia tenia una red de internet proporcionalmente desarrollada pero no lo suficientemente fuerte para enfrentar ataques cibernéticos a gran escala.

Las páginas gubernamentales o los medios de comunicación no contaban con una seguridad apropiada para disuadir los efectos producidos por esta especie de ciber terrorismo. El mecanismo de ataque fue igual a lo desarrollado en un año atrás en Tallin porque implementaron la misma modalidad al lanzar DDoS para saturar y derribar principales medios de comunicación, sitios gubernamentales al igual que toda la infraestructura digital disponible en Georgia. Este ataque provoco lo que se conoce como un vacío informativo donde se busco sembrar desinformación y propaganda a la población para que entren en pánico.

Al igual que los otros dos ataques el que se llevo a cabo en Kirguistán en el año 2009 fue también llevado a cabo por motivaciones políticas. En ese mismo año este país se encontraba enfrentando una difícil situación compuesta de inestabilidades políticas y sociales las cuales los hackers aprovecharon para implementar el famoso mecanismo de ataques de DDoS saturando los servidores ISP con tráfico masivo interrumpiendo los servidores de la red de internet nacional. Cabe resaltar que a comparación con los otros casos la infraestructura tecnológica en este territorio era menos avanzada, sin mucha innovación.

Debido a que más que un derecho el poder tener una red estable de internet dentro de este territorio era un privilegio. A pesar de todo esto el internet constituía una parte fundamental para la administración de los medios de comunicación y las paginas gubernamentales. Los ataques, que comenzaron el 18 de enero de 2009, se prolongaron durante dos semanas. "Los atacantes lograron interrumpir 3 de 4 proveedores de servicios de Internet (IPS), incluidos los dos principales IPS de Kirguistán (www.domain.kg, www.ns.kg). Usaron ataques DDoS masivos. Debido a que solo hay 4 IPS en Kirguistán, la mayoría de los servicios de Internet colapsaron. Era imposible enviar correos electrónicos o ingresar a ciertos sitios web

DICERE Revista de Derecho y Estudios Internacionales
Vol. 3 Nº 01 / 2026 / e-ISSN: 3028-886X

y también el uso de teléfonos móviles se vio obstaculizado debido a un ciberataque. Casi el 80% del tráfico de Internet estaba fuera de línea (Kozlowski, 2014, pág. 240)". Debido a que solo una pequeña parte de los ciudadanos en este país contaban con acceso a internet la vida digital no se vio completamente afectada, reafirmando la teoría de que el ataque cibernético no fue dirigido para afectar a la población por lo contrario fue dirigido para afectar al gobierno de turno.

En los tres casos expuestos dentro de este análisis no se llegaron a encontrar responsables directos que hayan participado en la emisión de los ciber ataques debido a la gran dificultad que existe para poder rastrear de donde provienen y al recurrente cambio de IP que no aseguran que la ubicación rastreada sea la correcta de acuerdo con las coordenadas del ataque. Sin embargo, hay una serie de factores interesantes que muestran indicios de quienes o de donde pueden prevenir aquellos ataques. El primer punto es que los tres países expuestos a problemas de ciber seguridad comparten frontera con Rusia, aunque eso no es motivo suficiente para generar un ataque en la red es muy relevante establecer el como estos tres territorios tenían diferentes disputas con esta gran potencia. Problemas que estaban relacionados desde la representación de simbolismos, conflictos históricos en cuanto a territorio y problemas políticos con la toma de decisiones de los gobiernos de ese entonces. Debido a estos motivos y el poder rastrear ciertas direcciones IP que provenían directamente de Rusia se acoso a este mismo país de ser el proveedor del financiamiento de los grupos criminales que atentaron contra la seguridad nacional de los tres estados mencionados. El conjunto de estas situaciones fue muy importante para desencadenar los parámetros a evaluar en torno a lo que se puede ser considerado como una agresión dentro del ciber espacio.

6 Lecciones aprendidas

6.1 ¿Cómo se prepara Estonia para futuros ciberataques?

A partir de este incidente Estonia invirtió grandes cantidades de dinero en tecnología avanzada para detectar y mitigar los ataques cibernéticos, desarrollando capacidades en inteligencia cibernética, análisis forense y en respuestas a casos fomentando la colaboración pública y privada para la recuperación posterior a un ataque cibernético. Además, se ha concentrado en mejorar sus relaciones internacionales con países pioneros en temas de ciberseguridad nacional como lo es los Estados Unidos además de estrechar sus relaciones con fuertes organismos como UE y la OTAM con los cuales comparten intereses en común dentro del tema de seguridad. Estonia al ser miembro de la OTAN, se beneficia de la cooperación con otros miembros en materia de ciberseguridad, en los ejercicios y simulacros que realizan para mejorar la preparación y coordinación en el momento de que suceda algún ataque cibernético.

A partir de la proximidad de estos vínculos se originó la creación del Manual de Tallin el cual aborda los temas del derecho aplicable en relación a la guerra cibernética. Dicho manual fue elaborado en la capital de Estonia por el centro de excelencia cibernética cooperativa de defensa cibernética

de la OTAM. Debido a los acontecimientos recientes en el último trimestre del 2009, "El CCDCE reunión a un grupo internacional de académicos y profesionales legales para escribir un manual que se ocupara de la interpretación del derecho internacional en el contexto de las operaciones cibernéticas y la guerra cibernética (Buresh, 2020, pág. 9)". Este acontecimiento marco un hito histórico con una mirada hacia el futuro del ciberespacio debido a que era la primera ocasión en donde la comunidad internacional abordaba de forma integral las cuestiones cibernéticas para tener una base legal en el manejo de estos casos, a si se evitaría desencadenar situaciones que desencadenen problemas de mayor complejidad. Estonia posee métodos de contingencia de respuesta rápida ante ataques cibernéticos.

La importancia de la creación de este manual se debió a la vulnerabilidad de las infraestructuras digitales dentro de los estados y la necesidad de carácter urgente el poder regular los asuntos relacionados al ciber espacio dentro de un marco legal. Este conjunto de normas sirve para establecer las directrices en cuanto la legitima defensa en el ciberespacio haciendo un énfasis dentro de la cooperación internacional para prevenir futuros ataques. El manual de Tallin trata "El ciberespacio como un dominio físico y, por lo tanto, otorga la soberanía sobre su infraestructura cibernética "y las actividades cibernéticas dentro de [su] territorio". Según este tratamiento del ciberespacio, una incursión en la infraestructura cibernética de otro estado puede considerarse una violación de la soberanía de ese estado. Si bien una violación de la soberanía ciertamente viola el derecho internacional, no justifica en sí misma una respuesta ofensiva (Cal, 2016, pág. 3)". Analizando el caso de estudio de Estonia a través del manual de Tallin se puede evaluar la respuesta de este país frente a los ataques cibernéticos sufridos en el 2007 además de discutir la atribución de la responsabilidad. Las lecciones descritas en este manual demuestran una gran importancia para el manejo de políticas y estrategias en base a las situaciones globales relacionadas con la ciber seguridad

7 Contexto del Ciberataque a Estonia en 2007+

7.1 Aspectos claves para la ciberseguridad dentro de los Estados

Después de las empresas, las organizaciones internacionales o instituciones estatales son el punto focal de los ciber atacantes, razón por la cual en esta sección brindo ciertas recomendaciones básicas como parte de estrategias futuras para tomar las medidas necesarias que ayuden a implementar la ciberseguridad dentro de estos casos.

Seguridad de la Red. Enfocada para proteger las redes de las computadoras contra los intrusos y malware
Seguridad de Aplicaciones. Se busca mantener el software y dispositivos libres de amenazas, así se evita el acceso a datos personales.
Seguridad de la Información. Se protege la integridad y la privacidad de los datos de almacenamiento y de tránsito. Aquí hablamos del cifrado, el control de acceso y las políticas del manejo de datos.

DICERE Revista de Derecho y Estudios Internacionales
Vol. 3 Nº 01 / 2026 / e-ISSN: 3028-886X

Seguridad Operativa. Son los procesos y decisiones para proteger y procesar los archivos de datos. Aquí entran los permisos de los usuarios para acceder a la red, así como los procedimientos donde se almacenan o comparten los datos.
Recuperación ante desastres. Las políticas determinan como las organizaciones reorganizan sus operaciones y datos para volver a su capacidad operativa antes del desastre.
Educación del usuario final. La ciberseguridad debe estar atenta con las personas o usuarios que son las personas encargadas de manejar los sistemas o equipos. Deben ser educados para que eviten introducir accidentalmente un virus, a no conectar unidades USB no conocidas, eliminar archivos adjuntos de correos electrónicos, entre otras.

7.2 Importancia de la cooperación internacional en ciberseguridad

Es importante el enfatizar los acuerdos de cooperación internacional entre gran parte de los estados para contener este tipo de amenazas cibernéticas. Los ciberataques no distinguen fronteras nacionales, por lo que se complica el rastreo de los involucrados. En casos como el de Estonia, aunque atribuya o sospeche que el ataque proviene de Rusia no se puede estar totalmente seguro ya que la IP del ataque se generó desde diversas ubicaciones. Las respuestas para estas amanezcas requieren ser multifacética y coordinada. De acuerdo con el gobierno de Estonia establecen que a partir de los desafortunados ataques del 2007 tratan de basar su política sobre "Defensa cibernética enfatiza la necesidad de que la OTAN y las naciones protejan los sistemas de información clave de acuerdo con sus respectivas responsabilidades; compartir las mejores prácticas; y proporcionar una capacidad para ayudar a las naciones aliadas, a pedido, a contrarrestar un ataque cibernético. Esperamos continuar el desarrollo de las capacidades de defensa cibernética de la OTAN y fortalecer los vínculos entre la OTAN y la autoridad nacional (Shackelford, 2009, pág. 5)".

Esta relación ayudo a mitigar el impacto producido por el ataque y a fortalecer las defensar cibernéticas. Este caso le demostró al mundo que ningún país puede enfrentar solo las amenazas cibernéticas. Ahí es donde entran en juego factores como la solidaridad, resiliencia y la inversión en nuevas tecnologías para poder estar preparados para los siguientes atentados dentro del área del ciberespacio donde mecanismos como el CCDCOE tienen un rol importante para mantener la paz. En el futuro la implementación de la tecnología de la información o seguridad de la información va ayudar a prevenir ciberataques. La principal función de este mecanismo es mantener fuera las posibles amenazas a dispositivos informáticos, sistemas, aplicaciones que contengan datos confidenciales desde personales hasta de ámbito laborales.

8 Conlcusión

Para concluir las ciber amenazas tienen que ser tomadas con especial atención. Pueden ocasionar grandes daños en diferentes niveles, desde simples fallas en los dispositivos diarios como los teléfonos, así como también puede causar fallas en los equipamientos militares, apagones en las ciudades, corromper sistemas informáticos,

violar la privacidad de la población y ocasionar grandes catástrofes que afecten a la seguridad nacional de los estados.

Estonia, a raíz del ciberataque que sufrió el 2007 demostró la vulnerabilidad de sus infraestructuras digitales y lo importante que es la ciberseguridad en este mundo cada día más interconectado. Este incidente, uno de los primeros en el mundo en donde un país entero fue blanco de un ataque cibernético a gran escala. La reivindicación de este país frente a la ciber amenaza logro el que Estonia pueda constituirse en un gran líder mundial en cuanto a la tecnología, además de fortalecer sus defensas y a la vez convertirse en un referente contra los ataques cibernéticos. Esto da pie para decir que una guerra cibernética es algo factible y real, y que los países deben estar preparados y la cooperación internacional es primordial a la hora de proteger la sociedad en esta era tan digitalizada.

El caso del 2007 en Estonia además de otros ejemplos relacionados como el de Georgia y Kirguistán marcaron un antes y un después frente a las consideraciones de lo que engloba un ataque informático, a partir de estas situaciones se pudieron encuadrar a los ataques cibernéticos dentro de las bases legales para ser considerados como delitos penales. También se incentivó a la creación de herramientas para la identificación de estos casos como el manual de Tallin y los diversos organismos derivados de la UE y la OTAN que luchan por mantener un ciber espacio seguro y viable para todos los estados. Dentro de un mundo globalizado que se desarrollo en la era digital casos como el ocurrido en Estonia llegan a ser fundamentales para guiar a las naciones y organizaciones en la construcción de sistemas más seguros y preparados para enfrentar los desafíos del ciberespacio.

Conflicto de intereses

Los autores declaran que no existen conflictos de intereses.

Referencias

Alenius, K., & Warren, M. (2012). *An exceptional war that ended in victory for Estonia or an ordinary e-disturbance? Estonian narratives of the cyber-attacks in 2007*. In Proceedings of the Ecole Supérieure en Informatique, Électronique et Automatique Conference (pp. 1–18).

Alenius, K. (2013). *Victory in exceptional war: The Estonian main narrative of the cyber attacks in 2007*. In *The fog of cyber defence* (p. 78).

Buresh, D. L. (2020). A critical evaluation of the Estonian cyber incident. *Journal of Advanced Forensic Sciences, 1*(2), 7–14.

Cal, N. M. (2016, October). Crossing the Rubicon: Identifying and responding to an armed cyber-attack. In *2016 International Conference on Cyber Conflict (CyCon US)* (pp. 1–7). IEEE. https://doi.org/10.xxxx *(si encuentra el DOI real, agréguelo)*

Cardash, S. L., Cilluffo, F. J., & Ottis, R. (2013). Estonia's cyber defence league: A model for the United States? *Studies in Conflict & Terrorism, 36*(9), 777–787. https://doi.org/10.1080/1057610X.2013.813249

Ciberseguridad. (s.f.). *Estonia*. https://ciberseguridad.com/normativa/europea/estonia/

Davies, P. (2022, May 27). *Estonia: Proteger el ciberespacio frente a las intenciones rusas*. Euronews. https://es.euronews.com/next/2022/05/27/estonia-proteger-el-ciberespacio-frente-a-las-intenciones-rusas

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival, 53*(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Fernández, A. (2015, August 12). *Estonia, baluarte de la ciberseguridad europea*. El Orden Mundial. https://elordenmundial.com/estonia-ciberseguridad-europea/

Gamreklidze, E. (2014). Cyber security in developing countries: A digital divide issue—The case of Georgia. *Journal of International Communication, 20*(2), 200–217. https://doi.org/10.1080/13216597.2014.926278

Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. *Information Security Journal: A Global Perspective, 18*(1), 1–7. https://doi.org/10.1080/19393550802676069

Gromilova, A. (2017). Promoting cyber security: Estonia and Latvia as norm-setters. *Analele Universitatii din Craiova-Seria Istorie, 31*(1), 127–138.

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: An informational approach. *Law, Innovation and Technology, 9*(2), 159–189. https://doi.org/10.1080/17579961.2017.1305907

Herzog, S. (2011). Revisiting the Estonian cyber attacks: Digital threats and multinational responses. *Journal of Strategic Security, 4*(2), 49–60.

Natalucci, F., Qureshi, M. S., & Felix, S. (2024, April 10). *Las crecientes amenazas cibernéticas: Una grave preocupación para la estabilidad financiera*. IMF Blog. https://www.imf.org/es/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability

Kozlowski, A. (2014). Comparative analysis of cyberattacks on Estonia, Georgia and Kyrgyzstan. *COBISS*. MK-ID 95468554.

Shackelford, S. (2009). Estonia two-and-a-half years later: A progress report on combating cyber attacks. *Journal of Internet Law. (Advance online publication o forthcoming; si encuentra volumen/número, agréguelo)*

Odoh, E. M. (2021). Cyber attack as a tool to influence foreign policy: A comparative study of Russia's cyber-attacks on Estonia and Georgia. *University of Nigeria Journal of Political Economy, 11*(1).

OTAN. (s.f.). *La OTAN y el desarrollo de herramientas para la ciberdefensa*. https://otan.es/blog/la-otan-y-el-desarrollo-de-herramientas-para-la-ciberdefensa/

Poggi, N. (2018, December 10). *Ciberamenazas: Qué son, cómo te afectan y qué puedes hacer al respecto*. Prey Project. https://preyproject.com/es/blog/ciberamenazas-que-son-como-te-afectan-y-que-puedes-hacer-al-respecto

Wong, E., Porter, N., Hokanson, M., & Xie, B. B. (2017). *Benchmarking Estonia's cyber security: An on-ramping methodology for rapid adoption and implementation*.