UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
Programa de posgrado en Ciencias Políticas y Sociales
Facultad de Ciencias Políticas y Sociales
Instituto de Investigaciones Sociales
Centro de Investigaciones sobre América del Norte
Centro Regional de Investigaciones Multidisciplinarias
Facultad de Estudios Superiores Acatlán
Facultad de Estudios Superiores Aragón

“El ciberespacio como dominio estratégico para la Organización del Tratado del Atlántico Norte: ciberseguridad y ciberdefensa en el siglo XXI”

T E S I S

QUE PARA OPTAR POR EL GRADO DE:

MAESTRA EN ESTUDIOS EN RELACIONES INTERNACIONALES

Presenta:

Noradilda Calderón Lara

Tutora principal:
Dra. Yadira Gálvez Salvador
Facultad de Ciencias Políticas y Sociales

Ciudad Universitaria, Ciudad de México, febrero, 2024.

Agradecimientos

Gracias a mi maravillosa familia, a mi madre Delfina, a mi padre Felipe, son los mejores, a mi hermana Yereli y a mis hermanos Uriel y Jonathan,
todo es posible gracias a ustedes y por ustedes, les amo profundamente.

Gracias a cada una de mis amigas por ser mi soporte e inspiración de vida: Lesli, Nuria, Lau, Pao, Elsy, Gaby, Zyanya; a mis amigos, en especial a Enrique por su incondicionalidad y motivación en esta travesía; gracias a Fernando por amarme, cuidarme y alentarme, gracias a ustedes por estar.

Gracias a mi directora de tesis, la Dra. Yadira Gálvez Salvador por su cariño, tiempo, dedicación, enseñanzas e invaluable apoyo durante el desarrollo de esta investigación.

Agradezco al Dr. Alejandro Chanona Burguete por su conocimiento y experiencia que compartió en el desarrollo de esta tesis;

al Dr. Jorge Alfonso Monjaráz Domínguez por su rigor y disposición de ayuda en cada una de sus observaciones;

al Dr. Raúl Benítez Manaut por su confianza y compañerismo compartidos para la elaboración de este trabajo y en el aula;

al Dr. Abdiel Hernández Mendoza por su bondad, por su orientación e impulso, en este y en los demás proyectos en los que afortunadamente coincidimos.

Gracias a la Dra. y a los Dres., a cada uno de mis profesores y profesoras, por las charlas, comentarios y observaciones que tuvieron a bien para el enriquecimiento de esta tesis, gracias también por su compromiso con la noble labor que desempeñan, mi admiración y respeto para ustedes.

Gracias al Consejo Nacional de Humanidades, Ciencias y Tecnológicas por su colaboración en favor de los y las estudiantes.

Agradezco a la Universidad Nacional Autónoma de México por ser la casa de estudios en donde se materializan mis sueños y mis metas.

Por mi raza hablará el Espíritu.

Tlazcamati

índice

Índice de tablas

Índice de imágenes

Introducción

Derivado de las características del ámbito cibernético, los Estados, sociedad civil, empresas y organizaciones están cada vez más inmersas en una arena que como el aire, tierra, mar y espacio, es propicio a amenazas que atenten contra la seguridad nacional e internacional. El uso creciente de tecnologías y plataformas digitales genera que las relaciones internacionales se desarrollen en un escenario dinámico y en constante evolución; integrando a la agenda internacional el desarrollo de procesos políticos, sociales, económicos y militares que respondan al reconocimiento del ciberespacio como un dominio estratégico.

El desarrollo de las Tecnologías de la Información y la Comunicación (TIC) facilita las relaciones entre individuos y naciones, aumentando la velocidad en el flujo de información, el Comunicado de prensa de septiembre de 2023 de la Unión Internacional de Telecomunicaciones señala que “el 67% de la población mundial está ya en línea, es decir, unos 5 400 millones de personas” (UIT, 2023), por lo que el auge de las TIC hace que su uso sea cada vez más frecuente y necesario, incluso en los sitios más remotos del globo.

El ciberespacio trasciende las barreras de distancia y tiempo, ofreciendo un sinnúmero de ventajas que permiten trascender fronteras y realizar múltiples actividades a través de dispositivos electrónicos que evolucionan constantemente. Sin embargo, en la otra cara de la moneda se encuentran las naciones con menor desarrollo tecnológico que están en una situación de desventaja tecnológica con respecto de los países con mayor desarrollo en el área. De modo que, las que no cuentan con los recursos suficientes dependen de la tecnología de otros Estados y empresas, por lo que “entre más periférica y subyugada sea su posición en la realidad material -por añadidura- lo mismo será en la realidad digital o virtual” (Arroyo, 2021-presente, 12m20s), es decir, las fronteras geográficas tienden a replicar su comportamiento en el espacio cibernético.

La carrera cibernética avanza a un ritmo acelerado, la innovación es creciente y constante. Sin embargo, los Estados y las Organizaciones Internacionales no poseen las herramientas necesarias para enfrentarse a los ataques en el espacio cibernético, aún a pesar de los esfuerzos para contrarrestar sus efectos. Para las Relaciones Internacionales, realizar un

estudio sobre la integración del ciberespacio en la Organización del Tratado del Atlántico Norte (OTAN) es necesario, pues es un tema coyuntural para la Alianza Atlántica, ya que el avance tecnológico integra nuevos elementos que se perfilan como amenazas potenciales a la paz y seguridad internacionales, no solo al entorno cibernético, sino también al físico ya que ambos están interrelacionados, coexistiendo para el funcionamiento de la sociedad.

Sumado a ello, la pandemia del coronavirus SARS-CoV-2 aceleró el proceso de integración de recursos virtuales al quehacer de los Estados, las organizaciones y las personas. El avance de las TIC e incluso las redes sociales, es y seguirá siendo parte de la cotidianidad, no solo en el escenario político, económico e industrial, sino también en un ámbito tan convulso como lo es la seguridad, por lo que consolidar un marco a seguir en materia de ciberseguridad y defensa en el ciberespacio es una de las necesidades actuales que la comunidad internacional debe atender.

La principales motivaciones y finalidades de los ataques cibernéticos son variadas, tales como: inteligencia, espionaje industrial y financiero, propiedad intelectual, motivos políticos, extremismos, razones económicas, entre otros. Luego del ataque a las computadoras (se presume que fue a través de un dispositivo USB) de control de la central nuclear iraní a través del virus *Stuxnet* en 2010, quedó manifiesto que las infraestructuras críticas (las que permiten el suministro de agua, electricidad, servicios bancarios, las redes en favor de la seguridad y defensa, centrales nucleares, entre otros) son susceptibles a ciberataques, por lo que deben contar con una red de protección técnica y jurídica que prevenga y responda de forma eficaz, puesto que un ciberataque podría causar daños a un país entero y extender su impacto, con una duración indeterminada.

Los ciberataques perpetrados contra Estonia en 2007 y Georgia en 2008 dan cuenta de que el ciberespacio es un sitio propicio para la guerra. El ciberataque contra Estonia se considera dentro de los primeros en su tipo por el nivel de profundidad de los daños causados. Dichos eventos fortalecieron los proyectos encaminados hacia la prevención y respuesta a las actividades que se realizan en el ciberespacio. Es en este contexto que tanto la OTAN impulsa programas/proyectos de ciberseguridad y ciberdefensa con la finalidad de poder hacer frente a estas amenazas, siendo la defensa uno de los ejes más importantes de estos esfuerzos frente a los retos en el ciberespacio.

La OTAN es una organización consolidada, partiendo de su constitución político-militar, se mantiene vigente en temas de seguridad y defensa. Es así como la sinergia de los países miembros, genera competencias funcionales, eficaces y organizadas y, también coloca a los países con menos avance en una posición de desventaja, ya que al igual que los grupos fuera del Estado, “los servicios de inteligencia de los Estados representan una amenaza” (Quintana, 2018) frente a aquellos que no tienen los recursos necesarios para desarrollar capacidades de ciberdefensa en el ciberespacio, lo anterior repercute con un impacto negativo, generando dependencia tecnológica no solo en el ámbito económico, comercial e industrial, sino también en el ámbito militar, esencial para la seguridad nacional.

Así pues, el objetivo central de esta investigación es “analizar la integración del ciberespacio como dominio de operaciones militares en la OTAN y su impacto en la seguridad internacional en el siglo XXI” mismo que se busca responder con la pregunta de investigación: ¿de qué manera integra la OTAN el ciberespacio como dominio de operaciones estratégicas y cuál es su impacto en la seguridad internacional?

A lo largo de tres capítulos, se analizarán múltiples premisas para confirmar o refutar la hipótesis siguiente: “la OTAN considera al ciberespacio como un dominio de operaciones militares y su defensa está integrada en su concepto estratégico de 2022. Esto coloca a la organización como referente para la comunidad internacional en cuanto al desarrollo de capacidades para afrontar los desafíos y amenazas en esta área al tiempo que abre el debate sobre los alcances de la defensa colectiva en este dominio”.

La Teoría de los Complejos de Seguridad Regional (TCSR) de Barry Buzan y Ole Wæver es punto de partida para el desarrollo del capitulado, que retoma los postulados de esta teoría en torno a la correlación que existe a partir de los procesos de securitización en la zona del Atlántico Norte a través de la OTAN y el impacto que tienen a nivel regional e internacional, de manera que los miembros de la Alianza comparten una zona geográfica, pero también los une la identificación del ciberespacio como un entorno susceptible a amenazas que podrían incidir en la seguridad.

El primer capítulo, *El ciberespacio en la agenda de seguridad internacional*, aborda tres conceptos esenciales para una mejor comprensión del tema en cuestión, ya que términos como ciberespacio, ciberseguridad, ciberdefensa y aquellos que de estos se desprenden

no tienen una definición única y estandarizada. El primer apartado tiene la función de identificarlos y clarificarlos tomando en cuenta diversos estudios, artículos y documentos internacionales y así, a partir de los elementos que los conforman, realizar el análisis de estos, integrándolos con la agenda de la Alianza Atlántica y el contexto en el que se sitúa esta investigación.

El estudio del ciberespacio no es reciente, sin embargo, el tema comenzó a tener eco en la comunidad internacional, cuando varios países fueron víctimas de ciberataques mismos que empezaron a diversificarse en cuanto a la frecuencia, objetivos y especialización; con ello la población, las instituciones públicas y privadas y los mismos Estados comenzaron a demandar mayor seguridad en el ciberespacio. Derivado de lo anterior, el segundo capítulo *La OTAN y la defensa colectiva en el ámbito cibernético*, ofrece una revisión histórica de los artículos del Tratado de Washington que podrían ser invocarse o vincularse a los temas relativos al ciberespacio. Asimismo, se retoman los ciberataques a infraestructuras de Estonia, Georgia y Estados Unidos, que fueron parteaguas en la creación de instrumentos frente a los desafíos y amenazas en el ciberespacio, también se describen las capacidades que ha desarrollado la Alianza que van desde el terreno político, jurídico y económico, hasta el sector militar.

El tercer capítulo, *El ciberespacio como escenario de conflicto para la OTAN,* se centra en la identificación de las amenazas al ciberespacio a partir de documentos oficiales de la Organización y sobre la posibilidad de que el artículo de defensa colectiva pueda ser invocado en un escenario de guerra. Así pues, a través de la “operación militar especial” (denominada así por parte del presidente ruso Vladimir Putin) a Ucrania en febrero de 2022, se realiza un análisis de la aplicación y resultados de las capacidades descritas en el capítulo dos; además, se describe brevemente la incidencia que tiene la OTAN con el conflicto, analizando las acciones Rusia y Ucrania ejecutan en el espacio cibernético y la respuesta de la Alianza y la comunidad internacional; ya que este conflicto sienta un precedente debido a la hibridez del mismo, puesto que su desarrollo parte desde ataques tradicionales con armamento convencional, hasta ciberataques que, por ejemplo, tienen efectos en el abasto de energía eléctrica a la población o en el transporte de equipo militar.

La ciberseguridad y la ciberdefensa son temas que cada vez tienen mayor importancia debido a la creciente innovación tecnológica en la que las relaciones entre Estados están

inmersas; la interacción a través de dispositivos electrónicos conectados a una red inalámbrica son parte del día a día del quehacer internacional en diferentes áreas como la: financiera, la militar, la distribución de servicios básicos (como el suministro de agua y electricidad) y la comunicación en sus múltiples vertientes. Las problemáticas que surgen a raíz de las nuevas tecnologías conciernen al estudio de las Relaciones Internacionales al representar un factor que atenta contra la paz y seguridad internacionales, mismas que están presentes incluso cuando hay ausencia de conflicto, por lo que son un elemento que seguirá siendo parte de la realidad internacional.

La sociedad internacional está inmersa en el mundo del Internet y, por lo tanto, depende de los servicios que ofrecen los gigantes tecnológicos, lo cual incrementa la vulnerabilidad de la información que se resguarda en las computadoras y plataformas gubernamentales o de la iniciativa privada. Aunado a lo anterior, las interacciones entre gobiernos y organizaciones internacionales son cada vez más frecuentes a través de plataformas en línea a la que una multiplicidad de actores tiene acceso.

La constante revisión de las estrategias realizadas en favor de la ciberseguridad es necesaria para analizarlas y evaluar los resultados y el alcance de estas; es imperativo incluir a las naciones que se encuentran en desventaja tecnológica ya que el ciberespacio no conoce de fronteras y los ciberdelincuentes pueden servirse de dichas vulnerabilidades para lograr objetivos indirectos. Para los y las internacionalistas representa un tema que sin duda alguna seguirá en constante evolución al tiempo que genera cambios en la escena internacional y nuevos retos para los tomadores de decisiones.

Capítulo 1. El ciberespacio en la agenda de seguridad internacional

La seguridad atraviesa múltiples dimensiones, de ahí la relevancia que tiene para las naciones. En términos generales, la seguridad está presente en distintos momentos: pasado, presente y futuro, es decir, prevención, respuesta y, resiliencia y disuasión. En función de ello, se realizan políticas, estrategias, herramientas y alianzas con actores que inciden en el mantenimiento de la seguridad nacional, misma que está bajo resguardo del aparato estatal.

La integración del ámbito cibernético es proclive a amenazas, por lo que su seguridad es una tarea que para el caso del ciberespacio resulta confusa y trae consigo distintos debates en torno a sus características y alcances. Derivado de sus cualidades, la incorporación del ciberespacio a la agenda política de los Estados se enfrenta a una dinámica distinta a dominios convencionales como tierra, aire y mar. Aún tras los efectos en la seguridad cibernética por la pandemia por el coronavirus SARS-CoV-2, abordar el ciberespacio como un entorno dentro de la seguridad nacional sigue siendo complejo.

Una de las primeras tareas al abordar el tema, se encuentra en el debate conceptual, ya que la delimitación de los elementos que lo componen da certidumbre a quienes elaboran, ejecutan acciones y toman decisiones en función de la seguridad. De esta manera, es posible identificar las necesidades, oportunidades e incluso carencias que poseen los Estados a nivel nacional y la comunidad internacional para enfrentarse a las amenazas a la seguridad en el ciberespacio.

El estudio del ciberespacio y por lo tanto la inclusión a la agenda de seguridad internacional, es una tarea que requiere de la apertura de espacios que permitan el reconocimiento de sus variables en distintos niveles: económico, político, social y militar. Los retos y ventajas en la materia son innumerables, por lo que la comprensión de los elementos que son parte del entorno cibernético facilita su reconocimiento y por lo tanto la creación de instrumentos políticos que acompañen el desarrollo de capacidades operativas en función de la seguridad cibernética.

1.1 El ciberespacio: concepto e integración a la agenda de seguridad

El ciberespacio es el único dominio producto de la acción humana, es decir, su creación está constituida de forma artificial. Con herramientas tecnológicas cada vez más avanzadas, el entorno cibernético hace parte esencial en la cotidianidad de las personas, empresas, organizaciones y Estados. La creación de equipos de cómputo con mayor capacidad operativa, así como la necesidad de infraestructura física en confluencia con Internet, las redes y sistemas interconectados, dan paso a un dominio en que día con día interactúan millones de personas que generando gran cantidad de datos e información.

La Cuarta Revolución Industrial[1] en convergencia con la pandemia por el coronavirus SARS-CoV-2, trajo como consecuencia la aceleración de los procesos de digitalización, generado a su vez, escenarios en donde los países son rebasados por este avance en donde las tecnologías disruptivas y emergentes (inteligencia artificial, impresoras 3d, *blockchain*, asistentes virtuales) continúan en desarrollo y modifican el quehacer de la sociedad y los Estados. Asimismo, el alcance del ciberespacio es resultado de las características que posee, distintas a los dominios físicos, ya que es un entorno libre de fronteras, ubicuo y en constante transformación.

Para el análisis de la relación entre seguridad y ciberespacio, una de las primeras tareas será definir lo que para efectos de esta investigación se entiende como ciberespacio. Epistemológicamente, la voz ciberespacio está ligada a *kibernetes,* vocablo utilizado para refererise a los marinos que se encargaban de conducir los barcos en la antigua Grecia. Posteriormente, el término fue adoptado por los romanos como *kybernan* para indicar la misma acción (Ortega, 2022).

---

[1] Se entiende por Revolución Industrial a los fenómenos tecnológicos y económicos que tienen impacto en el sector productivo y generan cambios en concurrencia con cuestiones demográficas, económicas, políticas, culturales e industriales. La Primera Revolución Industrial surgió a mediados del siglo XVIII, caracterizada por la máquina de vapor y su impacto en la relación de patrón y trabajadores; la Segunda Revolución Industrial tuvo su impulso en el uso de la electricidad, que trajo como consecuencia la producción en masa; la Tercera Revolución Industrial o también llamada Revolución científico-tecnológica emergió con el avance en las tecnologías de la comunicación y el uso de Internet. Castañeda Sánchez, Alfredo (2019) en La Cuarta Revolución Industrial (Industria 4.0). Entre menos trabajo, nuevos empleos y una cíclica necesidad: la protección del trabajador asalariado. En Kurczyn, Sánchez y Mendizábal (Coords.) *Industria 4.0 trabajo y seguridad social* (núm. 872), pp. 33-62, Instituto de Investigaciones Jurídicas, https://archivos.juridicas.unam.mx/www/bjv/libros/12/5645/20.pdf

La primera mención del término ciberespacio, se remonta a 1984 con la obra de ficción del escritor norteamericano William Gibson: *Neuromante* (López de Anda, 2011, p. 69). A partir de este evento, su relación con la cibernética y el prefijo *ciber* se extendió, por lo que su uso comenzó a ser cada vez más común para referirse a todo aquello vinculado con un medio virtual y a los dispositivos informáticos, asociándolo con lo que se conoce como Internet y las acciones que resultan de esta interacción.

Así pues, identificar las características y acepciones desde un punto de vista holístico y estratégico es importante para el desarrollo de esta investigación para comprender y analizar las dinámicas que emanan del ciberespacio de manera integral. Aunado a lo anterior, la relevancia de los debates conceptuales provenientes del dominio cibernético será parte fundamental para identificar su alcance y por lo tanto la forma en la que se integra a las agendas de los países, empresas y organizaciones.

1.1.1 Ciberespacio: términos y elementos

Con el fin de la Segunda Guerra Mundial, surgió un estudio referente a los sistemas de comunicación y su interconexión, sin los que la guerra habría tenido un desarrollo diferente. Además, aludía a nuevas herramientas modernas, en donde entidades físicas y artificiales coincidían en función del tratamiento de la información, su organización, comunicación y sistematización. En 1948 el matemático estadounidense Norbert Wiener, definió a la cibernética como: “el estudio del control y la comunicación en las máquinas y seres vivos” (Wiener, 1964, como se citó en Burtseva, Valentyn y Flores, 2015, p. 44), por lo que con ello nació una disciplina en el contexto de posguerra. Es decir, el origen de la cibernética está ligado una de las necesidades militares básicas: la comunicación.

Para López de Anda, el ciberespacio se concibe como un concepto revisitado, en donde convergen discusiones hacia la búsqueda de la comprensión del espacio digital, o para aludir a este ya sea indagando en sus alcances, mostrando sus limitaciones, para cuestionarlo e integrarlo a los debates en distintas ramas, “se trata de un ‘después’ de producción académica que, paradójicamente, suele recurrir a un ‘antes’ en la comprensión ontológica del concepto de espacio.” (2011, p. 69)

John Perry Barlow, en su *Declaración de Independencia del Ciberespacio* de 1996, al referirse al ciberespacio señala que

> está formado por transacciones, relaciones, y pensamiento en sí mismo que se extiende como una quieta ola en la telaraña de nuestras comunicaciones. Nuestro mundo está a la vez en todas partes y en ninguna parte, pero no está donde viven los cuerpos. (Perry, 1996)

De lo anterior, resalta la particularidad de la ubicuidad del ciberespacio, cualidad que no poseen otros dominios físicos como la tierra, el mar o el aire. Dicha característica es determinante y a la vez problemática en su incorporación en el quehacer de los Estados, puesto que el avance tecnológico configura los dominios de poder en el que la comunidad internacional se enfrenta a amenazas no convencionales, con cualidades que obligan a desarrollar sistemas de seguridad y defensa en el espacio cibernético en un ambiente de incertidumbre por las características de este.

Para Tække, “el ciberespacio es un espacio paralelo al geográfico. Es el receptáculo de todo lo que tiene una extensión virtual” (Tække 2002, como se citó en López de Anda, 2011, p.84). Mientras que, para Sagrario Morán Blanco, “es el nombre por el que se designa al dominio global y dinámico compuesto por las infraestructuras de tecnología de la información -incluida Internet-, las redes y los sistemas de información y de telecomunicaciones” (Morán, 2017, p. 197). Ambas concepciones se refieren a un espacio virtual global que aglutina medios físicos y digitales interconectados donde las Tecnologías de la Información y Comunicación (TIC) son inmanentes al ciberespacio.

Por lo anterior, se entiende que el ciberespacio es inherente al entorno material, puesto que, para que exista es necesario contar con dispositivos electrónicos, mismos que están conectados a redes inalámbricas que pertenecen ya sea a una entidad pública o privada. De manera que ambos entornos, material y virtual, convergen, generando así desafíos distintos a los que emanan de los dominios tradicionales, que irrumpen e inciden en la forma en la que se concibe la seguridad y defensa en un dominio con dinamismo acelerado y constante.

Joseph Nye, habla de un régimen híbrido, señalando que “el ciberespacio es un dominio operativo enmarcado por el uso de la electrónica para (…) explotar la información a través

de sistemas interconectados y su infraestructura asociada" (2010, p.3) de este modo, el poder en el ciberespacio dependerá de la cantidad de recursos físicos y virtuales con los que dispongan las entidades, ya sean públicas y privadas para controlar, crear y comunicar información, además de medios como infraestructura, software, habilidades humanas, incluyendo Internet, intranets y otras tecnologías (Nye, 2010, p. 3).

En ese sentido, el poder en términos del ciberespacio es un elemento que en el ejercicio del Estado requiere de la participación de múltiples organismos y de la colaboración con el sector privado. Dependiendo de la manera en la que los Estados ejerzan este poder, su inserción en la agenda tendrá impacto en las estrategias políticas que se ejecutan en diversas áreas como: las tecnológicas, de investigación y desarrollo, económicas y militares, configurando escenarios que requieren especial atención para que el uso del ciberespacio, sea un entorno que salvaguarde las acciones que en él se ejecutan y a su vez permita al gobierno el aprovechamiento del ámbito cibernético en función de sus intereses.

Tomando en cuenta lo anterior, identificar de donde proviene la definición de ciberespacio, permite dar claridad al Estado que lo aborda, tal es el caso de Estados Unidos de América (EE. UU.) que a través de su Departamento de Defensa señala que el ciberespacio:

> Es un dominio operativo cuyo carácter distintivo y único está enmarcado mediante el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de sistemas de información interconectados y conectados a internet y sus infraestructuras asociadas. (*Department of Defense*, 2022)

De esta definición destaca la forma en la que EE. UU. integra al ciberespacio como un escenario que se perfila como potencial en el campo de batalla, derivado de la multiplicidad de amenazas y actores que convergen en este, por lo que su integración al Departamento de Defensa implica el desarrollo de acciones defensivas y ofensivas que se inscriben en temas que atienden a la seguridad nacional que tienen relación directa con la industria militar estadounidense.

Por su parte, el *Manual de Tallin 2.0* del Centro de Excelencia de la Ciberdefensa Cooperativa (CCDCOE) de la OTAN dice que el ciberespacio es "el entorno formado por componentes físicos y no físicos para almacenar, modificar e intercambiar datos usando

redes informáticas" (*Tallin Manual 2.0*, 2017, p.564), la relevancia de este concepto yace en que el Manual[2] es uno de los documentos más importantes sobre operaciones en el ciberespacio por los países suscritos a este. Dirigido a asesores jurídicos, militares y de inteligencia, refleja la opinión de expertos en la materia para la aplicación del Derecho Internacional en caso de conflictos bélicos en el ciberespacio, pero su debilidad radica en su carácter académico y, por lo tanto, no vinculante para quienes hacen uso de este.

Derivado de lo anterior, se entiende al ciberespacio como: un dominio operativo híbrido que requiere del uso de componentes físicos y virtuales con el objetivo de crear, almacenar, modificar, intercambiar y explotar información en convergencia con redes informáticas y otras infraestructuras asociadas. Sobre esta base, se parte hacia lo que implica el reconocimiento del ciberespacio dentro de los dominios estratégicos, en términos de seguridad nacional e internacional junto con la tierra, aire, mar y espacio.

Elinor Ostorm (2002) habla de los recursos de uso común, mismos que poseen como principal característica su alcance para la población y por lo tanto una difícil exclusión de su uso para la sociedad, ahora bien, ¿se puede incluir al ciberespacio en esta categoría? A pesar de la apertura y accesibilidad del ciberespacio como medio de comunicación, este es un entorno donde, aunque se estima que el 67% de la población mundial ya en línea (UIT, 2023), siguen existiendo sitios que no cuentan infraestructura física y por lo tanto virtual que provea de este recurso. Aproximadamente un tercio de la población, es decir, 2 600 millones de personas, aún no están conectadas a Internet, por lo que la exclusión digital sigue siendo uno de los retos en la agenda de los países, a pesar de las predicciones que señalan un crecimiento anual de 3.5% (DataReport, 2022) que, si bien durante 2020 y 2021 hubo un incremento en la conexión global, con el paso de los años los números han ido a la baja, dejando a un 33% de la población mundial sin posibilidad de acceso a Internet en 2023 (UIT).

[2] El Manual de Tallin es un conjunto de reglas que se enfocan en la aplicación del derecho internacional en una guerra cibernética de manera que plantea conceptos y actores en dicho ámbito. En su versión 1.0 cuenta con 95 reglas y en la 2.0 con 154. Desde 2021 trabaja en su versión 3.0 con una proyección a 5 años para actualizar los tópicos y dar mayor certidumbre en el contexto actual. El Manual es uno de los esfuerzos del Centro de Excelencia de la Ciberdefensa Cooperativa (CCDCOE) de la Organización del Tratado del Atlántico Norte (OTAN), mismo que cuenta con 2 ediciones, la de 2013 y 2017, hoy en día se encuentra en una fase de actualización para una revisión y lanzar así su versión 3.0 (*Cooperative Cyber Defense Centre of Excellence* [CCDCOE], 2022)

Por lo tanto, el ciberespacio se puede considerar dentro de los llamados bienes globales (*global commons*), que de acuerdo con el Derecho Internacional son espacios que no forman parte de la soberanía de un Estado, de manera que su uso no está limitado al poder gubernamental de una nación, lo que apunta a que podría alcanzarse en un futuro un régimen jurídico internacionalizado para los recursos básicos del ciberespacio (Segura, 2017, p. 292) en donde el papel del sector privado será determinante, generando mecanismos que logren maximizar las ventajas de ámbito cibernético y su cobertura a nivel mundial.

A pesar de que la integración del concepto en la agenda internacional continúa en proceso, la falta de estandarización del término es problemática, ya que las dificultades se traslada a los escenarios físicos, en donde el abordaje de las amenazas no posee un marco regulatorio preciso que de certidumbre a la comunidad internacional, de manera que los trabajos en función del ciberespacio con sus alcances y limitaciones, precisan de definiciones claras que integren las variables que la realidad internacional requiere.

Lo anterior da cuenta de los debates entorno a la conceptualización del ciberespacio y como la incorporación de este, forma parte del reconocimiento de lo que Castells (1997) llama la sociedad red, o de lo que Nye (1992, p. 2) llama tercera revolución industrial, en donde el común denominador es la integración de las TIC a través de redes interconectadas en la cotidianidad desde el nivel individual, hasta el que implica el ejercicio del Estado en el ámbito de defensa a través de capacidades militares ejercidas por las fuerzas armadas en aras del mantenimiento de la paz y seguridad internacionales.

1.1.2 Dominio estratégico en la seguridad y defensa

La protección del territorio, soberanía e interés nacional, ante los embates externos e internos que atenten contra la supervivencia del Estado es una de las funciones principales de quienes gobiernan una nación. De este modo, el papel de las fuerzas militares es inmanente a las facultades del Estado para la defensa, por lo que el reconocimiento e integración del ciberespacio como dominio estratégico, requiere de la colaboración del aparato gubernamental con empresas, sociedad, e incluso la academia.

Desde los aportes de Heródoto y Tucídides sobre las causas de la guerra, hasta *El Leviatán* de Thomas Hobbes en donde explica que el estado de naturaleza es inmanente al hombre, mismo que lo lleva a vivir en conflicto a partir de la voluntad, la guerra ha sido una constante en la lucha por el poder, por el territorio y por los recursos, de manera que el conflicto bélico está presente en distintos momentos de la historia de la humanidad.

En ese mismo sentido, la defensa es inherente a la seguridad puesto que, en tanto más y mejores capacidades de defensa se desarrollen, disminuyen las posibilidades de que se vulnere la seguridad. Tradicionalmente, los escenarios de conflicto hacen referencia al espacio terrestre, aéreo, marítimo e incluso espacial (tal como sucedió en el marco de la Guerra Fría en la carrera espacial entre Estados Unidos y la Unión de Repúblicas Socialistas Soviéticas [URSS]), sin embargo, con la integración del ciberespacio en la agenda de seguridad, las posibilidades de conflicto se ampliaron.

Analizar la probabilidad de un conflicto desarrollado en el ciberespacio, no se incluía en la agenda de principios del siglo XX, empero, para 2023 se perfila como un escenario posible y cercano. Un conflicto en el ciberespacio implica tomar en cuenta las características particulares que de este emanan, desde las físicas, hasta las virtuales en donde las fronteras son difusas y la atribución de los ciberataques es incierta, ya que se pueden realizar desde sitios remotos distintos al lugar atacado.

La naturaleza de las características del ámbito cibernético contrasta con los retos a los que los Estados y ejércitos han enfrentado en los dominios tradicionales. Por lo que, la identificación de las características y diferencias es esencial para el ejercicio de las fuerzas armadas, derivado del uso de inteligencia artificial y software especializado frecuente en las operaciones militares que obliga a las naciones a invertir en la investigación, desarrollo e innovación de tecnologías en convergencia con el ciberespacio.

De manera que la identificación de los elementos que son parte del ámbito cibernético es importante para el desarrollo de instrumentos que permitan maximizar su potencial en favor de gobiernos, empresas y sociedad, pero también para generar herramientas y capacidades de defensa, puesto que el carácter híbrido del ciberespacio, lo vuelve susceptible a amenazas tangibles e intangibles que requieren de un enfoque completo en el terreno físico y virtual.

Tabla 1. *Comparación de las características de los conflictos tradicionales y no convencionales.*

Conflictos tradicionales	Conflictos en el ciberespacio
Fronteras delimitadas.	Fronteras difusas.
Alto costo para el acceso del equipo armamentístico.	Bajo costo y acceso a herramientas físicas y virtuales.
La distancia es un factor importante en el desarrollo del conflicto.	La distancia no es una limitante.
Si existe regulación internacional ante la guerra.	Falta de regulación internacional ante conflictos cibernéticos.
Facilidad para identificar a los actores involucrados.	Multiplicidad de actores difíciles de identificar/anonimato.
Necesidad de una gran cantidad de efectivos militares y de reserva.	El personal debe ser especializado pero su cantidad no es determinante.

Fuente: Elaboración propia

Existen diferencias muy claras con respecto a la forma en la que se desarrolla conflicto bélico en el medio físico y en el medio cibernético, como se observa en la tabla 1, van desde el acceso a equipos armamentísticos tales como: tanques, aeronaves, submarinos, helicópteros, vehículos blindados, artillería, misiles balísticos, embarcaciones navales, hasta la cantidad de efectivos militares y de reserva, los cuales son determinantes en los conflictos en tierra, aire y mar, mientras que por su parte un conflicto en el ciberespacio no está determinado por la cantidad de personas involucradas, pero si requieren estar capacitadas para el uso del equipo y la ejecución de las acciones en el ámbito cibernético.

Sumado a lo anterior, la dificultad para atribuir los ataques cibernéticos es uno de los puntos más problemáticos ya que ello trae consigo la necesidad de cooperación con los posibles actores involucrados y sumerge a los Estados en debates en torno a la soberanía, de manera que el anonimato es una de las prácticas más comunes ya que impide la atribución

y por lo tanto la sanción de los ciberataques. Asimismo, la inexistencia de fronteras en el ciberespacio permite a los atacantes ejecutar sus acciones sin necesidad de estar presentes en el sitio vulnerado, de modo que la distancia (determinante en un conflicto en tierra, aire o mar) no es un elemento decisivo.

En ese mismo sentido, la falta de regulación internacional genera incertidumbre jurídica a la forma de enfrentarse a los ciberataques, distinto a los casos de guerra en el entorno físico que cuentan por ejemplo, con los Convenios de Ginebra y sus Protocolos adicionales, además de que las resoluciones emitidas por el Consejo de Seguridad de la Organización de las Naciones Unidas (ONU), mientras que para el ámbito cibernético el único tratado con un carácter similar a los antes mencionados, es el Convenio sobre la Ciberdelincuencia (también conocido como Convenio de Budapest) impulsado por el Consejo de Europa, firmado en noviembre de 2001 y que entró en vigor en 2004.

Existen múltiples factores que generan ambigüedad en el entorno cibernético, por lo tanto "la redundancia, resiliencia y reconstitución rápida se convierten en componentes cruciales de la defensa" (Nye, 2010, p. 5) y su integración a la agenda de seguridad es cada vez más necesaria porque el poder y/o debilidades cibernéticas tiene impacto en todas las esferas, desde la militar hasta la comercial, la política, económica, financiera e industrial.

Es decir, esta situación en el ciberespacio genera el debate y la discusión de un problema complejo con diversas de aristas, ya que cuenta con una serie de vulnerabilidades que ponen en jaque la seguridad de Estados, empresas y personas. Si bien, el ciberespacio se configura como ámbito sujeto al Derecho Internacional, no se ha avanzado en las normas ni tratados generales que puedan incidir en su regulación (Segura, 2017, p. 298).

Sin embargo, ante la creciente necesidad de ampliar los espacios de seguridad, se identifican algunos momentos importantes durante el siglo XX y XXI que definieron la agenda integrando al ciberespacio en la esfera de seguridad y defensa internacional ya sea por representar un evento premeditado o bien involuntario. En el cuadro 2, se observa que si bien los ciberataques no están ligados directamente al desarrollo de tratados internacionales o la creación de organismos que buscan proteger el ciberespacio, si existe una correlación entre estos y también da cuenta de que la celeridad con la que se crean

marcos regulatorios está muy lejos de alcanzar la velocidad a la que escalan los ciberataques.

Tabla 2. *Comparación entre ciberataques destacados y esfuerzos internacionales en la materia.*

Ciberataques	Contexto Internacional
1999 Ataques a la OTAN en la misión de Kosovo.	**2001** Firma del Convenio del Consejo de Europa sobre Ciberdelincuencia (Convenio de Budapest)
2007 Ataques cibernéticos a Estonia. **2008** Ataques cibernéticos a Georgia.	**2004** Creación de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés).
2010 Ataque cibernético *Stuxnet* a la central nuclear en Natanz, Irán.	**2010** Creación del *Cyber Command* en Estados Unidos. • Nuevo Concepto Estratégico de la OTAN.
2014 Ucrania señala a Rusia de perpetrar ciberataques a sus redes.	**2015** La Organización para la Cooperación de Shanghái adopta las Reglas de Conducta en el Área de Seguridad de la Información.
2017 El virus *WannaCry* afecta a 150 países.	**2016** La OTAN proclama al ciberespacio como cuarta dimensión de las operaciones militares junto con la tierra, mar y aire.
2022 En el marco del conflicto entre Rusia y Ucrania, esta última señala ser víctima de ciberataques rusos.	**2022** Brújula Estratégica de UE. • Concepto Estratégico de la OTAN.

Fuente: Elaboración propia

Los ciberataques a Estonia en 2007 y a Georgia en 2008 (eventos que se retoman y explican en apartado 2.1.1), así como el ataque *Stuxnet* en Irán en 2010, fueron parteaguas en la articulación de acciones que contemplaran a los ataques cibernéticos como un tema que debía integrarse en las agendas de seguridad y defensa no solo de los Estados, sino también de organizaciones y entidades privadas, así como en el ámbito personal de la población.

Joseph Nye señala que la era de la información global ha modificado el control de los Estados, modificando las jerarquías burocráticas en donde las entidades privadas tienen

mayor peso, las fronteras se difuminan y se desarrollan nuevas formas de interacción entre la ciudadanía y el gobierno. Cada vez más personas tienen libre acceso al ciberespacio que se configura como un nuevo e importante dominio de poder (Nye, 2010, p. 1). Sin embargo, esto no significa que este pueda reemplazar al espacio geográfico, de manera que la difusión de poder coexistirá en ambos entornos, lo que podría generar problemas por el ejercicio del poder en cada una de las dimensiones (Nye, 2010, p. 2).

Derivado del poder que emana de la información que circula en el ciberespacio es que los actores (Estados, organizaciones, entidades públicas y privadas y la misma población) integran este dominio estratégico como parte de la agenda de seguridad internacional. Por lo anterior, la convergencia entre este dominio con el espacio físico genera nuevas perspectivas desde el ámbito académico, político, económico, tecnológico y por supuesto, militar.

De este modo el ciberespacio ha ganado terreno en las agendas político-militares de los Estados. La pandemia por el coronavirus SARS-CoV-2 aceleró el uso del espacio cibernético, facilitando así la comunicación y el acercamiento en medio del confinamiento que prácticamente duró dos años, pero también generó que los delincuentes se hicieran de un nuevo entorno en el que llevar a cabo sus actividades delictivas, desde el ámbito personal y laboral, hasta el nivel macro en donde los Estados se vieron en la necesidad de generar mejores instrumentos de protección y reacción ante las amenazas en el ciberespacio.

1.2 La ciberseguridad: desafíos en la escena internacional

El prefijo *ciber* está asociado a las actividades relacionadas con la informática y el uso de aparatos electrónicos. Asimismo, hablar del ciberespacio, implica abordar una amplia gama de fenómenos que emergen de este. Tal es el caso de la ciberseguridad, tema que viene de la mano de la integración del ciberespacio a la agenda internacional, lo que trae consigo, tanto la identificación de nuevos factores de riesgo y amenaza, como nuevas oportunidades para las organizaciones y/o Estados de desarrollar capacidades y elementos de poder que les permitan enfrentarse a las necesidades del siglo XXI.

Los sistemas de información y telecomunicaciones, así como la infraestructura crítica[3] tienen una función vital para el funcionamiento de cualquier sociedad. De manera que la prevención, salvaguarda y respuesta ante los desafíos es una de las tareas principales de los tomadores de decisiones para garantizar el uso seguro del entorno virtual, puesto que derivado de la pandemia por el coronavirus SARS-CoV-2 la interdependencia del espacio cibernético con el entorno físico se acrecentó configurando nuevos escenarios en la arena internacional.

La ejecución de acciones en el ciberespacio no se entiende sin la definición de ciberseguridad, así pues, la identificación de esta genera compromiso, en consecuencia, se inserta en las preocupaciones del Estado, por lo que tiene un impacto directo en la sociedad e individuos ya que la ciberseguridad, incluye de manera activa a la población para lograr la protección de instalaciones físicas en convergencia con la información contenida en el espacio virtual.

1.2.1 Acepciones de la ciberseguridad

La ciberseguridad ha cobrado mayor relevancia en el siglo XXI, tanto para el sector público como para el privado. A lo largo de este apartado se analizan diversas acepciones sobre el significado de ciberseguridad, de modo que, a partir de los elementos que componen dicha definición se pueden identificar las preocupaciones y prioridades de los Estados y por lo tanto hacia donde dirige sus esfuerzos y estrategias en la materia.

La Unión Internacional de Telecomunicaciones (UIT) es el órgano de la ONU especializado en las Tecnologías de la Información y la Comunicación (TIC)[4] que para 2024 cuenta con

[3] De acuerdo con la *Cybersecurity and Infraestructure Security Agency* (CISA) la infraestructura crítica son aquellos activos, sistemas y redes que brindan las funciones necesarias para nuestra forma de vida. Hay 16 sectores de infraestructura crítica (sector: químico, de instalaciones comerciales, comunicaciones, de manufactura crítica, de presas, de base industrial de defensa, de servicios de emergencia, energético, de servicios financieros, agroalimentario, de instalaciones gubernamentales, salud y salud pública, de tecnologías de la información, de reactores nucleares, materiales y residuos, de sistemas de transporte, agua y saneamiento) que forman parte de un ecosistema complejo e interconectado y cualquier amenaza a estos sectores podría tener consecuencias potencialmente debilitantes para la seguridad nacional, la economía y la salud pública o la seguridad. (CISA, 2023)

[4] Fue fundada en 1865 con el objetivo de facilitar la conectividad de las redes de comunicaciones internacionales, uno de sus objetivos es lograr el acceso a las TIC para todas las comunidades del

193 Estados parte, sumando más de 900 miembros que incluyen empresas, organizaciones e instituciones académicas. En su Resolución 181 de 2010, la UIT señala que:

> "La ciberseguridad es el conjunto de herramientas políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: *disponibilidad; integridad, que puede incluir la autenticidad y el no repudio*; *confidencialidad*." (UIT, 2010)

Esta definición es relevante por la cantidad de elementos que integra, pero también porque proviene de un organismo con una cantidad importante de países miembros, lo que implica una amplia posibilidad de su aplicación en las estrategias nacionales de ciberseguridad. Otra de las particularidades de este concepto es que contempla dos componentes importantes que abordan la dimensión política que involucra a los tomadores de decisiones y otra que engloba cuestiones técnicas, propias de ámbito cibernético:

- Las cuestiones político-estratégicas: al referirse a las herramientas políticas, conceptos de seguridad, salvaguardas de seguridad, directrices y métodos de gestión de riesgos, implica la participación del gobierno en todos sus niveles.
- Las cuestiones técnico-operativas: cuando involucra acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios, ya que en este punto involucra directamente al sector privado que ofrece servicios de seguridad para redes, dispositivos e infraestructuras.

El Dr. Boris Saavedra, en la Conferencia Hemisférica de Ciberdefensa 2022, señala que "el sector privado es dominante en temas relativos a la ciberseguridad ya que al menos un 90% de datos y comunicaciones son producto del ámbito privado" (Conferencia Hemisférica de Ciberdefensa, 2022). De tal forma que los avances tecnológicos, así como su salvaguarda

---

globo; desempeña un papel fundamental en la aplicación y el seguimiento de la Cumbre Mundial sobre la Sociedad de la información (CMSI).

recaen en gran medida en el sector privado. Una de las empresas internacionales más importantes en seguridad informática es la firma de origen ruso Kaspersky, que señala:

> La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes. (Kaspersky, 2022)

Por su parte, la compañía Cisco, dice que “la ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales” (Cisco, 2022). Mientras que para Microsoft “la ciberseguridad, también conocida como seguridad digital, es la práctica de proteger su información digital, dispositivos y activos. Esto incluye información personal, cuentas, archivos, fotos e incluso el dinero” (Microsoft, 2022). En ese sentido, estas concepciones dan cuenta de la gran incidencia que tiene el sector privado en materia de seguridad informática, ya que no se limitan a ofrecer una amplia oferta en herramientas para mantener la ciberseguridad en distintos niveles, desde el personal, hasta las empresas y gobiernos, sino que su quehacer también se centra en la investigación e innovación.

A su vez, las definiciones coinciden al incluir la protección de los dispositivos físicos y aquellos recursos digitales que se encuentran en el ciberespacio, por lo que, esto confirma la interdependencia de los medios físicos y virtuales. Asimismo, para que la ciberseguridad tenga efecto, es preciso integrar las tareas de prevención, protección y reacción frente a las amenazas que busquen manipular o dar un uso distinto a la información y datos contenidos en el entorno digital.

Si bien, la participación del sector privado tiene primacía en el mantenimiento de la ciberseguridad, es el Estado quien tiene la facultad de garantizar la protección y salvaguarda del ciberespacio, sobre todo cuando se ve comprometida la seguridad nacional. Es por ello que, demostrar su superioridad a través de instrumentos y estrategias gubernamentales e inversión en investigación y desarrollo, es esencial para lograr la confianza de la población usuaria del ciberespacio; de tal forma que potenciar las competencias del Estado en conjunto con el sector privado es una de las tareas más relevantes en el siglo XXI, para enfrentarse a los desafíos en el ámbito cibernético.

Considerando las definiciones anteriores, se entiende a la ciberseguridad es el conjunto de herramientas, estrategias y protocolos políticos y operativos para proteger los sistemas físicos y digitales que dan vida al ciberespacio. Dichas acciones “de carácter preventivo tienen por objeto asegurar el uso propio de las redes y negarlo a terceros” (Sevillano, 2021). De este modo, se parte hacia la descripción de la integración del término en la agenda de seguridad que es parte del quehacer internacional, incorporándose a la escena a través de investigación, alianzas, acuerdos y el desarrollo de instrumentos y capacidades.

Es así como la ciberseguridad cobra fuerza, sobre todo en el sector de la protección de datos e información en el sector público y privado, puesto que el contexto actual ha generado el uso frecuente y obligado de plataformas socio digitales y con ello el aumento de tiempo de uso de dispositivos electrónicos, en donde se realizan distintas transacciones que producen cantidades cada vez más datos cargados de información. Misma que, es importante proteger y gestionar, de manera que quienes busquen hacer uso indebido de ésta sean disuadidos a través de acciones concretas que sancionen los delitos cibernéticos con eficacia.

1.2.2 Incorporación en la agenda internacional

Los escenarios de confrontación en el siglo XXI son diversos y los ámbitos de seguridad y defensa se han multiplicado. Ello trae consigo el desarrollo de instrumentos que favorezcan la aplicación de estrategias y capacidades en torno a nuevos ámbitos en los que las amenazas se hacen presentes, tal es el caso del ciberespacio en el que emergen fenómenos de índole no convencional que requieren particular atención para su protección.

Las amenazas penetran, mutan y se transforman en el ciberespacio poniendo en peligro: las redes, los sistemas informáticos y de telecomunicaciones, la infraestructura de las empresas e instituciones públicas, así como a la información contenida y compartida en los equipos, y por supuesto a los Estados. Los terroristas y la delincuencia organizada hacen uso de las TIC para lograr sus objetivos atentando constantemente contra la seguridad internacional. Así pues, el ciberespacio es un nuevo terreno en donde la posibilidad de que un ciberataque escale a un conflicto de carácter armado, con elementos distintos a los que tradicionalmente conocemos, es cada vez más probable.

Para Barry Buzan y Ole Wæver, las dimensiones de la seguridad son amplias y con un carácter multidimensional, de manera la “seguridad en el ciberespacio que surgió con la aparición de herramientas tecnológicas que son indispensables para la sociedad y su funcionamiento; factores estratégicos de primer orden como las TIC, así los sectores sociales y económicos dependen de ellas” (Morán, 2017, p.196), constituye un tema que le compete a los Estados. Asimismo, la pandemia por el coronavirus SARS-CoV-2 volcó gran parte de las actividades al ciberespacio, por lo que la dependencia de este continúa en aumento, al igual que las amenazas cibernéticas que atentan contra la seguridad nacional.

En ese sentido, existen varios momentos que trajeron como consecuencia la incorporación del ciberespacio en la agenda de seguridad internacional, misma que fortalece y amplía con el paso de los años. Es así como, organizaciones internacionales han integrado la ciberseguridad en su agenda, entre las que se encuentran, la ONU y la UE, y aunque en menor medida, pero con otro enfoque y con un aumento y especialización constante: la OTAN, puesto que sus atribuciones se orientan al ámbito político-militar, tema que se explica en el siguiente apartado.

En 1998, la ONU creó el Departamento de Asuntos de Desarme, mismo que en 1992 cambió su nombre a Centro de Asuntos de Desarme y en 1997 a Departamento de Asuntos de Desarme; finalmente en 2007 fue denominada como actualmente se conoce: Oficina de Asuntos de Desarme de las Naciones Unidas (UNODA por sus siglas en inglés). Dentro de sus atribuciones, aborda “el impacto humanitario de las principales armas convencionales y las tecnologías de armas emergentes, como las armas autónomas” (*Office for Disarmament Affairs*, 2022), de manera que la incidencia de la tecnología en materia de armamento militar cobra importancia y por lo tanto su control y salvaguarda hacen parte de las tareas de la ONU.

En ese mismo tenor, desde 1998, la ONU integró el tema de seguridad de la información en el programa de Naciones Unidas, luego de que la Federación de Rusia puso sobre la mesa la integración de la seguridad de las telecomunicaciones y la información, que más adelante incluiría el ámbito cibernético a la agenda de la organización, reconociendo así las aplicaciones civiles y militares de la tecnología (Oficina de Asuntos de Desarme, 2022). Sin embargo, las diferencias ideológicas entre Rusia y Estados Unidos generaron que el avance

de las resoluciones se viera obstaculizado (Henderson, 2015). Empero, en 2010 Estados Unidos comenzó a co-patrocinar esas resoluciones; así, en la Segunda comisión los países occidentales dieron continuidad con la noción de esas Resoluciones que buscan la creación de capacidades y una cultura de ciberseguridad (Segura, 2017, p. 297).

A partir de ello, la Secretaría General presenta informes anuales con las opiniones de los países miembros sobre el tema, generando la creación de tres Grupos de Expertos Gubernamentales. En 2010 fue publicado el primer informe, la resolución A/65/201 llamado "Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional" (Naciones Unidas, 2022), que planteaba la forma de enfrentar las amenazas en el ciberespacio al igual medidas de cooperación internacional en la materia, destacando lo siguiente:

> El uso creciente de las tecnologías de la información y las comunicaciones en infraestructuras esenciales crea nuevos puntos vulnerables y oportunidades para la desestabilización. Debido a la compleja interconectividad de las telecomunicaciones y de Internet, cualquier dispositivo de las tecnologías de la información y las comunicaciones puede llegar a ser una fuente o blanco de un uso indebido cada vez más refinado. Puesto que estas tecnologías son, por su naturaleza, de doble uso, las mismas tecnologías que apoyan a un robusto comercio electrónico pueden utilizarse también para amenazar la paz internacional y la seguridad nacional. (Asamblea General, 2010)

Lo anterior es un ejemplo del impacto de las TIC en la ONU y la forma en la que son abordadas desde las ventajas que aportan a la sociedad, pero también desde el doble uso que le pueden dar los actores que se sirvan de estas, generando así, un creciente número de amenazas causando inestabilidad y por lo tanto atentados contra la paz y seguridad internacionales.

Por su parte, producto de las conferencias de Guadalajara en 2010, la UIT elaboró la Resolución 130 (UIT, 2010) que señala que:

> la UIT centre sus recursos y programas en aquellos ámbitos de la ciberseguridad que se corresponden con su mandato fundamental y su ámbito de competencia, y más concretamente en las esferas técnicas y del desarrollo, excluyendo las áreas relacionadas con la aplicación de principios legales o políticos por parte de los Estados Miembros en relación

> con la defensa nacional, la seguridad nacional, los contenidos y el ciberdelito, que corresponden a sus derechos soberanos. (UIT, 2010)

Es decir, la Resolución centra sus esfuerzos en el ámbito técnico-operativo, elaborando recomendaciones en ese sentido, invitando también a los miembros “a fomentar la elaboración de programas de educación y capacitación para dar mejor a conocer al usuario los riesgos en el ciberespacio” (UIT, 2010), generando así el uso informado las redes y tecnologías, fomentando la ciberseguridad para reducir las vulnerabilidades a las TIC y a quienes hacen uso de estas. Derivado de este informe, en 2011 fue aprobada la resolución A/RES/66/24 que buscaba dar seguimiento a dichos estudios, para que posteriormente fuera aprobado un nuevo informe 2012/13 que en el documento A/68/98 señala que:

> se reconoce que la aplicación de normas derivadas del derecho internacional vigente que sean pertinentes para el uso de las tecnologías de la información y las comunicaciones por parte de los Estados es esencial a fin de reducir los riesgos para la paz, la seguridad y la estabilidad internacionales. En el informe se recomienda que se continúe estudiando la cuestión a fin de promover un entendimiento común sobre la forma en que esas normas se aplican a la conducta de los Estados y al uso que estos hacen de las tecnologías de la información y las comunicaciones. (Asamblea General, 2011)

Este informe centra sus recomendaciones en la cooperación entre el sector público y privado, así como en la aplicación de normas adecuadas al uso de las tecnologías manteniendo la paz y estabilidad en la escena internacional. Con la aplicación de medidas voluntarias, transparentes y en un entorno de confianza entre los Estados y los demás actores que hacen uso de las TIC, se busca que su uso esté regulado por el derecho internacional a fin de reducir los riesgos y amenazas en el ciberespacio.

En diciembre de 2014 fue aprobada la resolución A/RES/69/28 la cual acogió con beneplácito las recomendaciones del informe de 2013, dando pie a que el Grupo emitiera un informe sustantivo en 2015 en donde entre los principales hallazgos se encuentran:

> En el uso de las TIC, los Estados deben observar, entre otros principios de derechos internacionales, la soberanía del Estado, la solución de controversias por medios pacíficos, y el tema de no intervenir en los asuntos internos de otros Estados.
>
> Obligaciones existentes en virtud del derecho internacional son aplicables al uso de las TIC y de los Estados y el Estado debe cumplir con sus

> obligaciones de respetar y proteger los derechos humanos y las libertades fundamentales.
>
> La ONU debe desempeñar un papel de liderazgo en la promoción del diálogo sobre la seguridad de las TIC en su uso por los Estados, y en el desarrollo de un entendimiento común sobre la aplicación de leyes y normas internacionales, normas y principios para la conducta del Estado responsable. (Naciones Unidas, 2022)

Dado lo anterior, se entiende que las TIC, el ciberespacio y su salvaguarda, no inciden solamente en el mantenimiento de la paz y seguridad internacionales, sino también hace parte de los debates en torno a los principios de soberanía y seguridad nacional en donde el Estado, el "Leviatán de Hobbes tiene la obligación de garantizar la seguridad de los ciudadanos" (Quintana, 2018, p. 57). Sin embargo, la determinación de la jurisdicción en el ciberespacio como se señaló en la Tabla 1, sigue siendo complejo, ya que en el marco del derecho internacional desde el principio de la no intervención y de la soberanía de los Estados, dificulta la delimitación de los alcances de cooperación en la materia que podría entenderse como una transgresión/intervención en las redes físicas y virtuales de las nacionales

En ese mismo tenor, también es importante mencionar el papel de la Oficina de las Naciones Unidas contra el Terrorismo (UNOCT por sus siglas en inglés) que cuenta con un Programa de Ciberseguridad y Nuevas Tecnologías que tiene la tarea de desarrollar y mejorar las capacidades de sus miembros en función de la prevención de ataques cibernéticos provenientes de grupos terroristas. Por lo tanto, la convergencia del ciberespacio y el terrorismo permite a estos grupos servirse de Internet para lograr sus objetivos (McKenna & Bargh, 1998) adaptando sus estrategias al entorno cibernético, vulnerando así la seguridad internacional.

Ligado a ello, Imran Awan señala la relevancia de plataformas de redes sociales como *YouTube*, X (antes *Twitter*) y *Meta* (como *Facebook* e *Instagram*), son utilizadas como herramientas de terror en donde grupos extremistas como ISIS (*Islamic State of Iraq and Syria*) propagan y promueven su mensaje, captando audiencia a través de videos, *tuits, hashtags, links*, comentarios e imágenes (Awan, 2017). Asimismo, la UNOCT cuenta con una serie de iniciativas que incluyen a las redes sociales como elemento fundamental para

la protección de infraestructuras críticas,[5] en donde el evento denominado *Cyber Challenge* tiene la finalidad de abordar actividades terroristas a través de: "ciberataques cinéticos a infraestructuras críticas y/o dispositivos IoT, difusión de contenido terrorista en línea, comunicaciones terroristas en línea y financiamiento del terrorismo digital" (*Office of Counter-Terrorism,* 2022).

En el marco de la ciberseguridad y en concordancia con la ONU, la Agenda sobre Ciberseguridad Global (GCA, por sus siglas en inglés) fue establecida en 2007, la cual "es un marco para la cooperación internacional destinado a mejorar la confianza y la seguridad en la sociedad de la información" (UIT, 2022). Los elementos de confianza y cooperación son una constante en la Estrategia Nacional de Seguridad Cibernética de los países miembros y aliados de la Unión Europea (el tema se desarrolla a profundidad en el apartado 2.4).

La GCA tiene su fundamento en cinco pilares estratégicos, de los que parte para evaluar las estrategias de los países, propiciando la estandarización en materia de ciberseguridad:

1. Medidas legales
2. Medidas técnicas y de procedimientos
3. Estructuras organizacionales
4. Creación de capacidades
5. Cooperación internacional

Cada una de estas medidas es de gran importancia no solo para las acciones de la Agenda, sino también el Índice de Ciberseguridad Global (GCI, por sus siglas en inglés) que es un instrumento "que mide el compromiso de los países con la ciberseguridad a nivel mundial para crear conciencia sobre la importancia y las diferentes dimensiones del problema" (ITU, 2020). La evaluación se realiza con base en la obtención de datos a partir de las estrategias nacionales, generando recomendaciones por parte del GCI, "identificando brechas y

[5] Se entiende por infraestructura crítica a las estructuras físicas que de ser afectadas en su funcionamiento tendrían gran impacto en el quehacer del Estado y por lo tanto de la población, de manera que las actividades esenciales serían interrumpidas, tales como: centrales nucleares y de electricidad, sistemas bancarios, terminales de abastecimiento de agua potable, servicios de transporte y salud.

fomentando la incorporación de buenas prácticas y proporcionando información útil para que mejores sus posturas de seguridad cibernética".[6]

Si bien, la Unión Europea inició con una Comisión en 2001, fue hasta 2013 cuando se adoptó la primera Estrategia de Ciberseguridad que identifica las prioridades en la materia: conseguir la ciberresiliencia, reducir el cibercrimen, desarrollar una política y capacidades de ciberdefensa, desarrollar recursos industriales y tecnológicos y establecer una política internacional de ciberespacio coherente.

Una de las iniciativas concretas es la Directiva 2016/1148/UE, conocida como Directiva NIS sobre seguridad de las redes y sistemas de información. Esta impone obligaciones a los Estados miembros y operadores de infraestructuras críticas y proveedores de servicios de la sociedad (redes sociales, nube, buscadores), siendo una perspectiva que busca adoptar medidas de seguridad y para compartir información "este enfoque prescriptivo resulta novedoso y puede marcar el tono de las estrategias nacionales en materia de ciberseguridad en el plano global" (Segura, 2017, p. 296).

Sobre ese mismo tenor, en 2004 la UE creó la Agencia de la Unión Europea para la Ciberseguridad (ENISA por sus siglas en inglés) que, de acuerdo con datos oficiales, tiene la misión de velar por un alto nivel común de ciberseguridad en toda Europa. Algunas de sus actividades son: capacitar a las comunidades, elaborar políticas en materia de ciberseguridad, cooperar en las operaciones, creación de capacidades y crear soluciones confiables (*European Union Agency for Cybersecurity* [ENISA], 2022).

En ese mismo sentido, el 17 de abril de 2019 nace el Reglamento del Parlamento Europeo y del Consejo relativo a ENISA lo cual le da mayor certidumbre "en el ámbito de la ciberseguridad aportando conocimientos, asesoramiento y actuando como centro de información de la Unión" (Diario Oficial de la Unión Europea, 2019). El documento provee además de las definiciones necesarias, los mandatos, objetivos, directrices, organización de la agencia, estructura de presupuesto entre otros, de manera que con ello se consolidan y legitiman las actividades de ENISA; además a través del Reglamento, se implantó en la

[6] Para más información se recomienda revisar la publicación más reciente del GCI de 2020 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

UE un marco único de certificación para garantizar la aplicación de normas en el ámbito de las TIC el cual busca generar confianza, ampliar el mercado y facilitar el comercio en la UE.

En el contexto de la pandemia por el SARS-CoV-2, en octubre de 2020 los mandatarios de la UE reconocieron la necesidad de mejorar las capacidades para: protegerse contra las ciberamenazas, proporcionar un entorno de comunicación seguro, especialmente mediante la encriptación cuántica y garantizar el acceso a datos a efectos judiciales y policiales (Consejo Europeo – Consejo de la Unión Europea, 2022). Estas solicitudes son relevantes ya que considerando los eventos de la pandemia por el coronavirus SARS-CoV-2 las amenazas en el ciberespacio aumentaron exponencialmente, lo cual obligó a la sociedad y a los Estados a priorizar la seguridad en el ciberespacio.

En ese mismo año, se presentó una nueva Estrategia de Ciberseguridad de la UE por la Comisión Europea y el Servicio Europeo de Acción Exterior, que entre sus objetivos principales contempla el fortalecimiento de la resiliencia ante los embates que puedan afectar a ciudadanos y empresas, buscando que el espacio digital sea más confiable y seguro; esta preocupación va de la mano con la protección de datos personales que cuenta con el Reglamento General de Protección de Datos (RGPD) aplicable desde 2018 el cual considera la protección como uno de los derechos fundamentales de los ciudadanos con respecto al tratamiento de las autoridades.[7]

Asimismo, en marzo de 2021, surgen las llamadas Conclusiones sobre la Estrategia de Ciberseguridad (Consejo Europeo-Consejo de la Unión Europea, 2021) en donde señaló la importancia de construir una Europa resiliente, ecológica y digital. Además, destaca una variedad de ámbitos de acción tales como: crear una red de centros de operaciones de seguridad en los países miembros de la UE frente a los ataques a las redes; definir una unidad informática conjunta; acelerar el proceso de adopción de normas de Internet para elevar la seguridad; desarrollar un cifrado sólido para proteger los derechos fundamentales; aumentar los instrumentos de ciberdiplomacia para combatir los ciberataques; y una de las propuestas más ambiciosas es la de elaborar una agenda para el desarrollo de la capacidad cibernética al exterior de la fronteras físicas de la UE con el objetivo de reforzar la ciberresiliencia y las cibercapacidades en todo el mundo.

[7] Para más información en *La protección de datos en la UE* en: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es

La UE es una de las entidades que cuenta con una gran cantidad de recursos a destacar en favor de la seguridad digital, tales como su estricta privacidad y la importancia de la protección de datos, de tal forma que ello coloca a la Unión como una organización sobresaliente, con redes estructuradas que le dan poder en el ciberespacio ante entidades públicas y privadas (Nye, 2010, p. 10). Todo ello fortalece los ámbitos de acción y reacción, en donde la Brújula Estratégica de 2022 robustece los esfuerzos antes mencionados integrando acciones que incluyen la integración del aparato militar y la ciberdefensa en el ciberespacio (Consejo Europeo, 2022).

Sumado a lo anterior, la UE se ha caracterizado por ser una institución con gran capacidad en materia de seguridad y como se describió a lo largo de este apartado, también en cuestiones de ciberseguridad, empero, la falta de un aparato militar propio genera que el ámbito de la ciberdefensa recaiga en la OTAN. Sin embargo, en el contexto de guerra entre Rusia y Ucrania, la Unión se sitúa en una posición de vulnerabilidad de cara a las amenazas que atenten contra las redes e infraestructura crítica, lo que obliga a esta a desarrollar e implementar nuevas estrategias para enfrentarse a los retos y desafíos sin depender del paraguas de la OTAN, que como se aborda más adelante, cuenta una serie de mecanismos cada vez más sofisticados frente las amenazas cibernéticas.

Asimismo, estudiar a la seguridad y defensa en el ciberespacio implica retomar los postulados de la Teoría de la Securitización de la Escuela de Copenhague, que desde 1990 tuvo un nuevo impulso que allanó el camino hacia el siglo XXI, ya que abrió la puerta hacia nuevas perspectivas en torno al concepto tradicional de seguridad (Hanssen y Nissenbaum, 2009, p. 1156), en donde el Estado es el único actor entendiendo a la seguridad en términos militares y territoriales.

Con el afianzamiento de la tecnología, el ciberespacio se presenta como un nuevo campo de batalla, que permite la utilización hostil de estas tecnologías con características particulares, como son la intangibilidad, la masividad y la auto-replicación, pero que a su vez pueden llegar a ocasionar daños concretos, físicos y económicos (Río Durán, 2011). En el apartado siguiente se desarrolla el concepto de ciberdefensa para ubicar los escenarios de conflicto que emergen del ciberespacio y las necesidades que trae consigo este fenómeno en la seguridad internacional.

1.3 La ciberdefensa: impacto en la seguridad internacional

La defensa se ha ampliado a diversos espacios que pueden ser objeto de amenazas. Así pues, el Estado, como garante de la seguridad nacional, atiende y se enfrenta a amenazas que trascienden fronteras físicas al tiempo que evolucionan. En un dominio como el ciberespacio, la relación con otros países está más allá del terreno geográfico, por lo que para una defensa activa y efectiva frente a los embates en contra de la seguridad internacional en el entorno cibernético, es necesaria la cooperación multilateral, ya que las crecientes amenazas atentan no solo contra infraestructuras críticas, redes y sistemas de información, sino también contra la estabilidad nacional.

Si bien, la comunidad internacional carece de un concepto claro y definido de ciberdefensa, empero, organizaciones como la OTAN poseen elementos que sirven como punto de partida para trabajar hacia la estandarización de sus componentes. De tal forma, la defensa del ciberespacio está ligada a la cooperación, por las características de dicho dominio en donde el actor principal es el Estado y que a través de sus fuerzas armadas ejerce dichas facultades de defensa.

La integración de la ciberdefensa en la agenda internacional trae consigo una serie de debates que van más allá de su definición *per se*. Por un lado, la multiplicidad de escenarios es uno de los principales desafíos para la defensa, y por otro, la diversidad de actores involucrados genera mayor incertidumbre, puesto que la adaptación y transformación de las amenazas evolucionan a un ritmo acelerado que rebasa los esfuerzos nacionales e internacionales.

Las labores de inteligencia, espionaje y contraespionaje hacen parte de la defensa de los dominios de los Estados, sin embargo, en el ciberespacio la configuración del poder se realiza a partir de las capacidades que tienen los Estados y del nivel de avance tecnológico que poseen. Es por ello que, la complejidad de las labores de ciberdefensa depende también de la posibilidad de incidir en la seguridad internacional ya que la interconexión del siglo XXI obliga a los mismos a ampliar sus redes aliadas y su esfera de influencia.

1.3.1 Terminología: de la defensa tradicional a la ciberdefensa

La constante evolución de las tecnologías hace parte de la cotidianidad a nivel global. Es así como estas inciden directamente en el quehacer de los Estados en el nivel económico, administrativo, político y por supuesto el militar que se encarga de la defensa. En un entorno global, dinámico y complejo como el ciberespacio, es necesario que el aparato encargado de su resguardo responda al contexto internacional vigente, puesto que la transversalidad del dominio cibernético genera la emergencia de amenazas sofisticadas y especializadas que afectan el sector civil y militar poniendo en riesgo la seguridad nacional e internacional.

El resguardo de la infraestructura, información y redes va más allá de las herramientas de prevención y protección, por lo tanto, es necesario contar con métodos de defensa apropiados. Una respuesta efectiva para enfrentarse a los desafíos en el ciberespacio requiere de acciones encaminadas a la defensa que necesitan una base sustentada en el ámbito jurídico, pero que también implica contar con herramientas que incluyen a las instituciones de defensa generando así nuevos retos frente a las amenazas en el ciberespacio.

Por mandato de la Organización de Estados Americanos (OEA), la Junta Interamericana de Defensa (JID), a través del Programa de Ciberdefensa, realizó un documento titulado *Guía de Ciberdefensa. Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar* que busca fortalecer las políticas y capacidades en materia de ciberdefensa de los países miembros. Este esfuerzo de 2020 es relevante porque define varios conceptos del ámbito cibernético, además de que tiene vínculos con socios regionales y globales en la búsqueda del desarrollo de iniciativas en cuanto a la ciberdefensa se refiere.

Es así como, dicho instrumento señala que la ciberdefensa es la “capacidad organizada y preparada para combatir en el ciberespacio. Comprende actividades defensivas, ofensivas y de inteligencia” (Junta Interamericana de Defensa, 2020, p. 14). Aunque el concepto es breve, contiene palabras clave que sitúan al mismo en una arena en la que los instrumentos de combate, incluyendo las acciones de respuesta e inteligencia que juegan un papel fundamental para su desarrollo y aplicación, de manera que, con ello, la Junta identifica las directrices a seguir para la ciberdefensa.

Aunado a lo anterior, otro concepto más amplio señala que

> “el término ciberdefensa, que se orienta a las acciones de un Estado para proteger y controlar las amenazas, peligros o riesgos de naturaleza cibernética, con el fin de permitir el uso del ciberespacio con normalidad, bajo la protección de los derechos, libertades y garantías de los ciudadanos, en apoyo a la defensa de la soberanía y la integridad territorial; sin soslayar que en los nuevos escenarios que plantea el ciberespacio, puede incidir en el momento de trazar rutas estratégicas plausibles para el cumplimiento de las diversas misiones militares de ciberdefensa” (Virilio, 1995, citado en Borbúa, V., Herrera, R., & Reyes, R., 2017)

Del concepto anterior, destaca el papel del Estado como garante de las libertades, soberanía y defensa del ciberespacio, por lo que es en esta parte en donde yace una de las principales diferencias con respecto al concepto de ciberseguridad en el que la participación del sector privado es mayor. Sin embargo, en el ámbito de la ciberdefensa, es el Estado el que funge un papel protagónico, puesto que ejerce el monopolio del uso de la fuerza en el ciberespacio como lo hace en tierra, aire y mar, además de los instrumentos que lo habilitan como defensor de este, a través del uso de medio militares, facultades que descansan en las fuerzas armadas.

Sumado a lo anterior, ejemplo de la función del Estado como legitimador de la ciberdefensa, encontramos a España, país que a partir del Ministerio de Defensa (MDEF) con el apoyo del Centro Conjunto de Desarrollo de Conceptos (CCDC), siguiendo la metodología de Desarrollo de Conceptos y Experimentación (CD&E) enlista una serie de puntos relativos al concepto de ciberdefensa, tales como:

> 1) La necesidad de contar con una Terminología Común.
> 2) La definición clara de las Capacidades de Ciberdefensa.
> 3) Las Operaciones militares en el ámbito del ciberespacio.
> 4) La Integración de las capacidades de Ciberdefensa en las operaciones militares conjuntas.
> 5) El marco legal de actuación y políticas Sistemas y Tecnologías de Información y Comunicaciones (CIS/TIC) y Seguridad de la Información (SEGINFO) en el MDEF.
> 6) Una Estructura de Mando y Control clara, ágil y eficaz, en la que estén integrados todos los medios con los que cuenta el MDEF y las FAS en particular.
> 7) La integración con otros actores civiles y militares del ámbito nacional e internacional.

> 8) Las medidas específicas a adoptar en materia de Concienciación, Enseñanza y Adiestramiento del personal.
> 9) Las consideraciones sobre Personal, en lo referente a este concepto.
> 10) Las consideraciones específicas sobre I+D+i[8] y en el campo de los Recursos Materiales. (Ministerio de defensa del Reino de España, 2018, p.6)

Los puntos del Ministerio de Defensa español dan cuenta de cómo es que el Estado posee la atribución de desarrollar acciones "de tipo activo, pasivo, proactivo, preventivo y reactivo que se aplican para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición" (Sevillano, 2021). Por lo que la ciberdefensa se sirve de un marco legal para su ejecución, contemplando resoluciones de índole nacional e internacional en coordinación con los distintos actores para enfrentarse a las amenazas en el ciberespacio (Sevillano, 2021).

El ámbito militar está íntimamente ligado a la ciberdefensa, pues son a las fuerzas armadas (en coordinación con otros órganos estatales), a quienes les corresponde llevar al terreno cibernético las capacidades derivadas de la ciberdefensa. Destaca que entre una de las tareas pendientes para el gobierno español se encuentra la estandarización de la terminología, como se señaló al inicio de este apartado, desde este punto conceptual es que se parte hacia la construcción de elementos que integran a la ciberdefensa.

Uno de los componentes más relevantes de la ciberdefensa, es la integración del ámbito militar (además del sector civil en sus labores de defensa). Por lo que, la defensa del ciberespacio queda a resguardo de la doctrina castrense a través de un sistema de mando, desarrollo de capacidades, todo ello bajo el amparo de instrumentos jurídicos que den certidumbre a la ampliación de labores en este dominio.

Así pues, la combinación de acciones tradicionales junto con acciones no convencionales, como "operaciones de manipulación de la información u otros elementos de presión política, social o económica, son una realidad en el escenario actual" (Ministerio de Defensa del Reino de España, 2018, p.5). De modo que estas son cada vez más frecuentes, vulnerando la seguridad en el ciberespacio y debilitando la estabilidad y confianza en el uso de dispositivos conectados a Internet u otras redes.

[8] Investigación + Desarrollo + innovación

En suma, derivado de que la ciberdefensa ocurre en un terreno distinto al físico, las actividades de monitoreo y simulación de escenarios son parte fundamental de esta; además, el análisis del *big data*[9] es parte fundamental para que se lleven a cabo los ciberataques. Por ello, las operaciones de defensa cibernética se fortalecen con la construcción de estrategias tecnológico-militares, pero también requieren abordarse desde un enfoque preventivo que responda a los desafíos y funcione como instrumento de disuasión frente a las amenazas.

Para Herring y Willett, la ciberdefensa

> incluye tres categorías complementarias: proactiva, activa y regenerativa. Las actividades 'proactivas' fortalecen el entorno cibernético y mantienen la máxima eficiencia para la infraestructura cibernética y las funciones de la misión. Las actividades 'activas' detienen o limitan el daño del adversario cibernético en tiempo cibernético relevante. Las actividades 'regenerativas' restauran la eficacia o la eficiencia de la misión después de un ciberataque exitoso." (Herring y Willet, 2014, p. 46)

En consecuencia, se entiende que la ciberdefensa se realiza en tres momentos: pasado, presente y futuro, ya que no basta con generar estrategias de prevención, sino que de igual manera son necesarias aquellas que respondan a las amenazas, para posteriormente generar lo que se conoce como ciberresiliencia, es decir, la capacidad de superar los daños de los ciberataques sin interrumpir el funcionamiento de las infraestructuras vulneradas, por lo que así se cubren todos los momentos en los que el ciberespacio puede ser atacado.

En ese sentido, el papel de las fuerzas armadas en la ciberdefensa tiene un carácter esencial y necesario, puesto que son estas las que desarrollan y ejecutan las estrategias, capacidades e instrumentos bajo el amparo del aparato estatal. De modo que, la doctrina militar deberá adecuarse a las demandas del contexto internacional en el ámbito cibernético

[9] El *big data* "se refieren a las nuevas tecnologías "analíticas" que organizan y analizan grandes colecciones de datos no estructurados para descubrir información valiosa. Es esta promesa de integrar datos no estructurados, extraer información valiosa de estos y proporcionar nuevas formas de predecir el comportamiento" (Chi, 2017, p.1) lo que ha generado gran interés en todo el mundo, sumado a ello pueden ser tratados prácticamente en tiempo real, de ahí la relevancia del concepto para la seguridad nacional ya que su aplicación implica nuevos desafíos derivado del incremento de amenazas en convergencia con las TIC.

para proteger eficazmente los sistemas físicos y virtuales que coexisten en el ciberespacio, tema que se aborda en el siguiente apartado.

1.3.2 La defensa y las TIC en las fuerzas armadas

La configuración de la seguridad nacional tiene un carácter inherente a las fuerzas armadas. Asimismo, el desarrollo de capacidades militares hace parte del resguardo, protección y mantenimiento de la seguridad nacional en donde el avance tecnológico es una constante para facilitar las actividades e interacciones. Por lo que, la integración del ciberespacio en la agenda de seguridad internacional genera la necesidad de la defensa en su rama cibernética, es decir, la ciberdefensa.

“Desde finales del primer decenio del siglo XXI, prácticamente todos los Estados y los principales organismos internacionales han identificado la seguridad de su ciberespacio como un objetivo estratégico de Seguridad Nacional” (Morán, 2017, p. 220). En consecuencia, las atribuciones de las fuerzas armadas incluyen al ciberespacio, lo cual implica no solo el desarrollo de capacidades en el ámbito cibernético, sino también, la capacitación constante del personal militar especializado para hacer uso y gestión adecuados de las tecnologías.

En ese tenor, tanto el Estado como el sector privado, centra sus esfuerzos en el aumento de la inversión en el área de investigación, innovación y desarrollo de tecnologías, en particular, aquella que atienda a la rama informática ya sea en su modalidad física o virtual.

Los beneficios de la integración de las TIC son vastos, sin embargo, entre los principales podemos señalar los siguientes:

- Rapidez y facilidad para intercambiar información y comunicación, incluso en tiempo real, por lo tanto, la respuesta y reacción puede ser inmediata.
- Ubicuidad y bajo coste. La facilidad con la que se puede tener acceso a dispositivos electrónicos, así como la extensión del uso de redes de Internet incrementa el uso de estas en células criminales.
- El anonimato, por ello los terroristas y delincuentes han trasladado sus actividades al terreno cibernético, en donde la tecnología de cifrado de extremo a extremo puede

dificultar su identificación y por lo tanto detención y sanción. Políticos y responsables policiales reconocen que “usando fuentes abiertas y sin actuar ilegalmente es posible obtener hasta el 80% de la información necesaria sobre el enemigo” (Gutiérrez, 2012, p.10). Así, la dependencia de sistemas cibernéticos complejos para el apoyo de actividades militares y económicas crea nuevas vulnerabilidades en los grandes estados que pueden ser explotadas por actores no estatales. (Nye, 2010, p.4)

- Efectividad e impacto. Hay gran impacto por efecto multiplicador de la propagación del miedo al usarlas como medio de difusión de actos terroristas. Por ejemplo “el sentimiento de terror que generó la visualización, a través de las redes sociales, del degollamiento del periodista norteamericano, James Foley, en agosto de 2014, por un terrorista del Estado Islámico de Iraq y el Levante (ISIS).” (Morán, 2018, p.199)

En suma, las TIC son un medio a través del cual los terroristas y delincuentes pueden afectar el funcionamiento y estabilidad del aparato estatal, de este modo es que una de las metas del uso de las TIC en las fuerzas armadas es la disuasión y contención de dichas amenazas, para generar resiliencia cibernética, resistir y recuperarse tras un ciberataque. Así como también el uso de estas herramientas para hacer frente al uso de las redes digitales por parte de organizaciones criminales y terroristas para llevar a cabo actividades de operación y comunicación, por lo que contar con personal especializado en la materia es uno de los requisitos imperativos en las filas de los ministerios y/o secretarías de defensa.

Entre las principales amenazas a la seguridad nacional a las que se enfrentan las fuerzas armadas que provienen de Internet se encuentran distintas actividades ligadas al prefijo *ciber,* tales como: ciberguerra, ciberterrorismo, cibercrimen/ciberdelito y el ciberespionaje. Sumado a ello, Joseph Nye dice al respecto: “los gobiernos también tienen la capacidad de llevar a cabo ciberataques ofensivos. Por ejemplo, la Décima flota y la Vigésima Cuarta Fuerza Área de Estados Unidos no tienen barcos ni aviones. Su campo de batalla es el ciberespacio.” (Nye, 2010, p.10)

En ese mismo sentido, en Estados Unidos, las aplicaciones de las TIC a programas de la Fuerza Aérea son múltiples, uno de los que destaca es el que se encuentra bajo la Estrategia de Modernización Digital, el Centro de Pruebas de la Fuerza Aérea que aplicó el

uso de tecnología de simulación para realizar evaluaciones para el sistema de armas (*Air Force*, 2022), con ello reduce riesgo en la ejecución en campo de las armas que cuentan con un proceso de toma de decisiones por computadora generando mayor efectividad eliminando los obstáculos en el entorno físico.

Asimismo, uno de los grandes ejemplos de la forma en la que las fuerzas armadas integran la inteligencia artificial, el uso masivo de datos y las redes de interconexión en el siglo XXI, el cual trabaja en colaboración con la Agencia Nacional de Seguridad (NSA por sus siglas en inglés), anunciado el 21 de mayo de 2010, es el Ciber Comando (USCYBERCOM, por sus siglas en inglés) que

> "integra y lleva a cabo operaciones en el ciberespacio, guerra electromagnética y operaciones de información, lo que garantiza llevar a cabo acciones en todos los dominios y asegurar la libertad de acción con sus aliados en y a través del dominio cibernético y la dimensión de la información, negándoles lo mismo a nuestros adversarios" (*U.S. Army Cyber Command*, 2022)

A través de la Secretaría de Defensa, el Ciber Comando cuenta con diez comandos a su disposición en donde el Comando Cibernético del Ejército (ARCYBER, por sus siglas en inglés) es su principal fuerza, compuesta por efectivos militares y civiles con la misión de defender las redes del Ejército bajo operaciones en un entorno multidominio en donde "a mediados de 2015, el cibercomando reconoció abiertamente que el volumen de ataque o intentos contra los sistemas y computadoras de distintas agencia federales o contra el Pentágono superaba los 250.000 ataques por hora." (Hernández, 2015)

En el mismo orden de ideas, la sofisticación del Ciber Comando derivada de sus componentes además del Comando Cibernético del Ejército también cuenta con:

- "El Comando cibernético de Flota/Décima Flota cuya autoridad operativa le permite dirigir y organizar operaciones en el ciberespacio, además de la disuasión cibernética defendiendo la porción de la Marina, ofreciendo así las capacidades cibernéticas necesarias para las fuerzas a flote y en tierra.
- La Decimosexta Fuerza Aérea (Fuerzas Aéreas Cibernéticas) que integra capacidades operativas de inteligencia y vigilancia, para garantizar la ejecución de las operaciones de la Fuerza Aérea, siendo así la primera Fuerza Aérea Numerada en su tipo.

- El Comando del Ciberespacio de las Fuerzas del Cuerpo de Infantería de Marina, el cual es la representación del Cuerpo de Marines, que además brinda asesoría en el despliegue de fuerzas.
- La Fuerza de Misión Nacional Cibernética se encarga de las operaciones ciberespaciales de espectro completo para defender a los equipos de las fuerzas de los EE. UU.
- El Cuartel general de la Fuerza Conjunta - Red de Información del Departamento de Defensa tiene como misión la operación diaria de las redes del departamento, así como su defensa activa de las amenazas, incluyendo al terrorismo integrado en 2016". (U.S. Army Cyber Command, 2022)

La capacidad de operación, planificación y ejecución con los que cuenta el Ciber Comando suma al complejo militar industrial estadounidense, potenciando sus capacidades militares en tierra, aire, mar y el ciberespacio. De este modo, las fuerzas armadas están dotadas de herramientas político-estratégicas, operativas, materiales y económicas que refuerzan su papel e influencia en la defensa de los dominios estadounidenses.

En el caso de la República Popular de China, uno de los medios de difusión chinos (conocido por su posición nacionalista), Global Times señaló en 2011: "China debe desarrollar su capacidad de ciberdefensa. Si no, estará a merced de otras potencias" (Ambros, 2011), en este sentido, el pronunciamiento se ubica posterior a la creación del Ciber Comando estadounidense, por lo que, además de ser una respuesta a las amenazas cibernéticas, fue una respuesta al anuncio del órgano cibernético más ambicioso de Estados Unidos, siendo China el competidor estratégico más importante para la nación norteamericana.

El 25 de mayo de 2011 el Ministerio de Defensa chino confirmó la creación del denominado Ejército Azul Cibernético, el cual sería entrenado para enfrentar los ataques cibernéticos (Sonia, 2015) empero, no existe mucha información acerca de la forma en la que este ejército lleva a cabo sus operaciones. En ese mismo sentido, el Consejo de Estado de la República Popular China, indica que

> "el ciberespacio se ha convertido en un nuevo pilar de desarrollo económico y social, y un nuevo dominio de la seguridad nacional. (…) A medida que el ciberespacio pesa más en la seguridad militar, China acelerará el desarrollo de una fuerza cibernética, y mejorará sus capacidades de conocimiento del ciberespacio, la defensa cibernética, el apoyo a los esfuerzos del país en el ciberespacio y la participación en la cooperación internacional cibernética." (República Popular China, 2015).

Desde 2011 la Organización para la Cooperación de Shaghái (OCS) presentó un borrador para la creación de las Reglas de Conducta en el Área de Seguridad de la Información, que buscan regular, supervisar y aplicar la ley en el ciberespacio, pero no contó con suficiente apoyo internacional, por lo que para 2015 presentó una propuesta revisada ante la ONU (CCDCOE, 2023), misma que continúa sin efecto. Una de las razones de la falta de aceptación, es la idea de que “China y Rusia sugirieron prohibiciones explícitas de lo que denominan armas de información y proliferación de sus tecnologías” (Walter, 2013) siendo la cuestión ideológica un freno para la aplicación de esta propuesta. Dicha organización centra sus esfuerzos en cuestiones de seguridad regional, que si bien, desde su concepción en 2001 no abordaba los temas cibernéticos, con el paso de los años se ha adaptado al contexto.

En Europa, uno de los países pioneros en estudios y desarrollo de capacidades en el ámbito de la ciberdefensa es España, que en 2013 creó el Mando Conjunto del Ciberespacio (MCCE) que está bajo las órdenes del Estado Mayor de la Defensa (EMAD), el cual se coordina con el Mando de Operaciones, la Dirección General de Infraestructuras (DIGENIN) y en los Cuarteles Generales de los Ejércitos terrestre, aéreo y marítimo. Aunado a lo anterior dicha estructura colabora ampliamente con el Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN. Por lo que el país ibérico colabora en conjunto con los ejercicios militares de la Alianza Atlántica, lo que genera un gran intercambio de información clasificada entre el Ministerio de Defensa, la OTAN y la Unión Europea.

Es así como el MCCE es el órgano responsable de planear, dirigir, coordinar, controlar y ejecutar las acciones en función de asegurar la libertad de acción de las fuerzas armadas en el ámbito espacial. A través del Equipo de Respuesta ante Emergencias Informáticas del Ministerio de Defensa será el responsable de definir la concienciación, formación y adiestramiento en la materia. Asimismo, el MCCE tiene a su cargo la gestión del

> espectro electromagnético asignado a las FAS y de coordinar los recursos de órbita-espectro electromagnético de los satélites militares. Realizará auditorías de seguridad en las redes y sistemas de información y telecomunicaciones conjuntos de las Fuerzas Armadas y otras que el JEMAD le encomiende. (Mando Conjunto del Ciberespacio, 2022).

Lo anterior es de gran relevancia puesto que la tecnología satelital hace parte del mando de las fuerzas armadas para atender sus responsabilidades en el ámbito del ciberespacio.

De manera que garantizar la respuesta efectiva ante las amenazas a los órganos de defensa, infraestructura crítica, entre otras, es una de las tareas más importantes del MCCE en el que el uso de la tecnología en todas sus facetas es fundamental para lograr con éxito los objetivos de dicha facultad.

En suma, las TIC se configuran como un elemento que hace posible la ciberdefensa cobrando cada día más relevancia, ya sea para realizar ejercicios militares de simulación, reacción y respuesta ante las amenazas, así como para persuadir al enemigo. El papel de las fuerzas armadas en la ciberdefensa no se entiende sin la aplicación de la tecnología, por lo que incluir al sector privado en coordinación con el Estado también es una tarea fundamental para que las estrategias se fortalezcan y los resultados tengan efectos en la seguridad del ciberespacio.

1.4 Retos y necesidades frente al COVID-19

La dinámica de seguridad tras la pandemia derivada del coronavirus SARS-CoV-2 se modificó en distintos ámbitos de la cotidianidad. Uno de los cambios más significativos que trajo dicha situación fue el aumento en el uso de Internet y otras herramientas físicas y virtuales que ayudaron a sortear los embates de la crisis sanitaria; el ciberespacio permitió la conexión sin importar la distancia y la ola de contagios y muertes (cifras que para noviembre de 2023 siguen en movimiento), empero surgió también un crecimiento exponencial de los ataques cibernéticos, aprovechando la falta de experiencia del sector público, privado y civil, lo cual demanda soluciones integrales, a través de estrategias y herramientas que respondan con eficacia.

La pandemia puso en relieve la necesidad ineludible de proveer seguridad en todos los niveles al ciberespacio. La sociedad incrementó la interconexión en línea, su dependencia tecnológica y la digitalización de forma casi obligatoria; en consecuencia, los delitos transitaron al espacio digital. Los *ciberdelincuentes* aprovecharon esta coyuntura beneficiándose de los vacíos legales y las vulnerabilidades tecnológicas, así como del desconocimiento de protocolos para actuar ante los ciberataques, “se han extendido el espionaje, la destrucción, los delitos, y el robo de secretos militares e industriales” (Instituto Español de Estudios Estratégicos [IEEE], 2012, p.3), la excesiva uniformidad y monopolización de las herramientas digitales disponibles (redes sociales, programas,

servidores, incluso marcas de equipo tecnológico, entre otras), generan que las ventajas de conectividad estén al alcance de una gran parte de la población al igual que las desventajas, de ahí la importancia de la colaboración entre Estados, empresas y a la sociedad en general.

El ciberespacio, la ciberseguridad y la ciberdefensa forman parte de la agenda tanto de Estados como de organizaciones públicas y privadas. De esta forma es que combatir las amenazas en este dominio estratégico, es una tarea necesaria que la comunidad internacional debe atender en un marco de cooperación. Dado que las amenazas se multiplicaron con la pandemia, la consecuencia inmediata es la necesidad de redoblar los esfuerzos y destinar recursos económicos para identificar las debilidades y así responder al fenómeno de la delincuencia en el ciberespacio.

La creación de un entorno cibernético trajo consigo una multiplicidad de ventajas que incrementan con el paso de los años, sin embargo, viene de la mano con su contraparte, es decir, el acceso a redes informáticas también se utiliza como un elemento de poder que se materializa en desafíos en la seguridad de la infraestructura y redes, así como la protección de la información y la privacidad. De modo que el ciberespacio se reconoce como un escenario de poder, influencia y dominio (Lozano y Rodríguez, 2020, p. 76) que configura escenarios endebles que modifican la lógica tradicional de enfrentarse a las amenazas convencionales.

El *Informe de Riesgos Globales 2021* del Foro Económico Mundial (WEF, por sus siglas en inglés) señala que:

> “el progreso hacia la inclusividad digital se ve amenazado por la creciente dependencia digital, la rápida aceleración de la automatización, la supresión y manipulación de la información y las brechas tanto en la regulación tecnológica como en las capacidades y habilidades tecnológicas.” (*World Economic Forum*, 2021).

La aceleración exponencial e incluso disruptiva de la globalización, tiene impacto en el ejercicio del poder. El cambio de paradigma que trajo consigo la revolución de las tecnologías y recientemente la coyuntura por el coronavirus SARS-CoV-2 puso en jaque la seguridad de las instituciones, gobiernos y población en general; sumaron nuevos desafíos en el espacio cibernético al tiempo que “más de 330 millones de personas comenzaron a usar Internet en los últimos 12 meses, lo que elevó el número total de usuarios de Internet

a nivel mundial a 4.720 millones a principios de abril de 2021" (Kemp). Estas cifras cobran mayor relevancia si se considera que dependiendo del país y el grado de afectación que le generó la pandemia, la actualización de los datos podría reflejar un mayor crecimiento ya que el acceso a red de redes se volvió esencial y cobró mayor importancia desde principios de 2020.

En su decimosexta edición, el *Informe Global de Riesgos 2022* señala que entre las implicaciones tras la crisis de COVID-19 está la dependencia digital y las vulnerabilidades cibernéticas. El aumento de amenazas cibernéticas superó la capacidad de los Estados de prevenirlas y enfrentarlas, pues "el uso de *malware* aumentó un 358% en 2020, mientras que el uso de *ransomware* aumentó un 435%, y el valor de las criptomonedas recibidas por las direcciones de *ransomware* se multiplicó por cuatro" (*World Economic Forum*, 2022) por lo que la dificultad de los Estados para regular los ataques en el ciberespacio sumado a la pandemia por el coronavirus SARS-CoV-2 que potenció sus efectos, debilita las estructuras cibernéticas y la confianza de la población usuaria de Internet.

Asimismo, la seguridad cibernética también se perfila como uno de los problemas globales de la agenda internacional, ya que la resistencia del uso de aplicaciones, datos, servicios en línea y comunicaciones generó un aumento de riesgos, transformado la dinámica global. En su *Informe Global de Riesgos 2022*, el Foro Económico Mundial señala que ligado a la seguridad cibernética los principales retos son:

- La ciberseguridad y su regulación
- Disminuir la brecha de habilidades en ciberseguridad
- Ciberdiplomacia y Seguridad Internacional
- Infraestructura crítica y ciberresiliencia
- Gobernanza de riesgo cibernético
- Ciberseguridad y nuevas tecnologías
- Riesgos cibernéticos y cadena de suministros
- Cibercrimen

Existe una marcada interconexión entre los retos que el Foro identifica, es decir, atender los riesgos cibernéticos en la cadena de suministros incide directamente en la prevención y sanción del cibercrimen y, por lo tanto, en la protección de la infraestructura crítica. A pesar

de los beneficios que son parte de la llamada Cuarta Revolución Industrial (expansión del comercio electrónico, educación en línea, trabajo remoto, entre otros), el desarrollo y transformación que esta trae consigo coloca a las amenazas digitales entre las principales preocupaciones de la población, por lo que la ciberseguridad seguirá siendo parte del devenir internacional cobrando cada vez mayor importancia.

Capítulo 2. La OTAN y la ciberdefensa: capacidades estratégicas

Las necesidades en torno a la seguridad y defensa son variables de acuerdo con el momento histórico. Uno de los eventos más relevantes, por su impacto a largo plazo, es la Segunda Guerra Mundial, puesto que este evento que marcó un hito en el devenir de las relaciones internacionales y trajo consigo una reconfiguración de las relaciones de poder, así como de la forma en la que se hace la guerra.

Las necesidades de la comunidad internacional están ligadas a los acontecimientos y fenómenos que surgen con el paso de los años. Por lo que, el desarrollo de tecnologías disruptivas y emergentes, traen a la escena, nuevas formas de confrontación y añaden a los conflictos elementos híbridos que requieren capacidades que respondan a los avances tecnológicos que se usan de forma malintencionada en ataques al entorno físico y virtual en detrimento de la seguridad nacional.

Para el siglo XXI, la OTAN se configura como una Alianza vigente y en constante adaptación. Sus capacidades se extienden al ámbito político y militar, por lo que posee gran cantidad de instrumentos que respaldan y complementan las herramientas técnicas en materia de ciberdefensa. El gasto en el sector militar nutre las áreas de investigación, innovación y tecnología, por lo que, a pesar del acelerado avance de los procesos de digitalización, la Organización cuenta con una amplia gama de competencias para enfrentarse a amenazas tradicionales e híbridas.

La cooperación es una de las fortalezas de la comunidad euroatlántica, ya que la defensa colectiva, amparada en el artículo 5° del Tratado de Washington, respalda las acciones militares nacionales y en conjunto de los países miembros. A su vez, la creación de capacidades cibernéticas le permite a la Alianza posicionarse en la escena internacional como un actor fundamental frente a los ciberataques. Sumado a ello, la OTAN cuenta con instrumentos jurídicos, técnicos y operativos que le permiten dar continuidad a sus objetivos políticos y militares en el tema de la ciberseguridad y la ciberdefensa.

2.1 La OTAN y la defensa colectiva en el ámbito cibernético

La configuración de la OTAN obedece a un contexto en el que los conflictos internacionales determinaron los objetivos de la Alianza. Además, la vecindad geográfica es relevante, ya que juega un papel importante en la interacción de los países miembros. Es así como, la Alianza Atlántica tiene su ámbito de acción en el hemisferio occidental, por un lado, 29 países ubicados en Europa y por otro, en el continente americano Estados Unidos y Canadá.

La Teoría de los Complejos de Seguridad Regional (TCSR), brinda un enfoque desde el que se permite abordar a la OTAN como un complejo formado a partir de la vecindad y el sistema de valores de los países miembros. Barry Buzan y Ole Wæver postulan la teoría que el análisis de la seguridad internacional puede realizarse considerando las variables regionales en interacción constante. Esta teoría encuentra su desarrollo histórico con la Guerra Fría como contexto internacional, por otro lado, tomando en cuenta la geografía de los involucrados, las amenazas identificadas en estos espacios y su relación entre sí, de modo que estas variables son importantes para el análisis del ciberespacio, puesto que la relación centro-periferia es una de los elementos a considerar en los temas de esta investigación en relación con la seguridad, que se extiende a la infraestructuras físicas y virtuales, en concreto, la ciberseguridad y ciberdefensa.

Es así como a través de las particularidades de los miembros de la OTAN conforman un colectivo, en donde su ámbito de acción se encuentra ubicado en el hemisferio occidental derivado de la posición geográfica de sus miembros, que en su mayoría son parte del continente europeo, mientras que Estados Unidos y Canadá se encuentran en el continente americano. En ese mismo sentido, la integración de nuevos miembros a la Alianza obedece que “los cambios de política de un día para otro, y la seguridad en su conjunto, así como sus partes separadas, son cuestiones en constante evolución, lo que significa que la política debe ser capaz de evolucionar con ella” (Stone, 2009), por lo que la expansión regional es uno de los elementos que fortalecen y nutren a la Alianza Atlántica.

El 1983, Barry Buzan definió al complejo de seguridad como “un grupo de estados cuyas principales preocupaciones de seguridad se vinculan lo suficientemente cerca como para que sus valores nacionales no puedan considerarse razonablemente separados unos de

otros” (Buzan y Wæver, 2003, p. 44), sin embargo, en 1998 en colaboración con Ole Wæver, reformuló su definición señalándolo como “un conjunto de unidades cuyos principales procesos de securitización, des-securitización o ambos están tan interrelacionados que sus problemas de seguridad no pueden analizarse o resolverse razonablemente por separado.” (Buzan y Wæver, 2003, p. 44).

En suma, la OTAN cuenta con las características suficientes para analizarse desde el punto de vista regional, puesto que en la práctica y en el discurso, garantizar la seguridad de los países miembros es su objetivo principal. A la luz de las crecientes amenazas, la organización posee cierto grado de interdependencia, sin embargo, también es importante destacar, desde el punto de vista constructivista, que además de la proximidad geográfica, los países miembros también comparten valores, identidades, así como una serie de normas implícitas en sus interacciones.

Las unidades que conforman a la Alianza Atlántica poseen un vínculo que nos permite considerarlos como un Complejo de Seguridad Regional que según Barry Buzan y Ole Wæver “se compone de los miedos y aspiraciones de las unidades separadas (que a su vez derivan en parte de rasgos y fracturas domésticas)” (Buzan y Wæver, 2003, p. 43) por lo que la identificación de dichos elementos y su posterior inclusión en la agenda, es un claro ejemplo de la forma en la que esta organización político-militar actúa en colectivo en favor de la seguridad regional y por lo tanto internacional. La consideración del espacio cibernético como parte del campo territorial de los Estados permite la integración de la ciberseguridad a la TCSR, ya que, para el caso de la Alianza Atlántica, la relevancia del ciberespacio y su inclusión en la agenda de seguridad de los países miembros se ha dado de forma paulatina, posicionándose en el ámbito político y militar.

La cuestión territorial es relevante en la TCSR, el ciberespacio no escapa a la teoría ya que si bien “la mayoría de las amenazas viajan más fácilmente en distancias cortas que sobre las largas” (Buzan y Wæver, 2003, p. 12), el surgimiento de amenazas cibernéticas, su fortalecimiento, mejora y constante presencia en la escena internacional, ha generado que se realicen cada vez más acciones en favor del mantenimiento de la seguridad cibernética, como su integración al Concepto Estratégico 2022 de la OTAN, además de la creación de múltiples herramientas que completan el marco de acción frente a los ciberataques.

La creación de la OTAN emana de la firma del Tratado de Washington, ocurrida el 4 de abril de 1949, tras el fin de la Segunda Guerra Mundial. Si bien, el surgimiento de esta organización sucedió en respuesta a la amenaza que representaba la extinta Unión de Repúblicas Socialistas Soviéticas (URSS), también es verdad que su creación fue parteaguas para evitar el resurgimiento militar nacionalista en Europa, pues desde su nacimiento, la alianza atlántica tuvo objetivos políticos basados en los valores democráticos sobre los que los miembros pueden realizar consultas en temas de seguridad y defensa.

Por otra parte, a razón del objetivo militar, la organización señala que la OTAN:

> tiene un compromiso de resolución pacífica de controversias. Cuando los esfuerzos diplomáticos no dan fruto, la fuerza militar emprende operaciones de gestión de crisis. Estas operaciones se llevan a cabo bajo la cláusula de defensa colectiva del tratado fundacional de la OTAN (Artículo 5 del Tratado de Washington) o por mandato de las Naciones Unidas, por sí sola o en cooperación con otros países y organismos internacionales. (NATO, 2022)

El principio de defensa colectiva, consagrado en el artículo 5° de su Tratado constitutivo, es el pilar de la OTAN, que implica que el ataque a uno o a varios miembros será considerado como un ataque contra todos y por lo tanto la respuesta se dará en el mismo sentido que este. Tras los ataques terroristas a Estados Unidos, el 11 de septiembre de 2001, este principio fue invocado, siendo esta la única vez que el artículo 5° tuvo efecto.

Los ataques que se describen en este apartado, el de Estonia en 2007 y Georgia 2008, tuvieron efectos a escala global. La respuesta por parte de la OTAN no se hizo esperar y quedó materializada en distintos instrumentos que obedecen a los objetivos político-militares y a la piedra angular de su fundación, la defensa colectiva. Sin embargo, la aplicación de este principio en el ciberespacio es un tema que está sobre la mesa de debate puesto que no existe un conflicto armado derivado de ciberataques, ya que estos se han presentado como parte de los conflictos, mientras están en curso utilizando las redes y computadoras como una trinchera adicional a las convencionales.

El análisis de los principales artículos del Tratado de Washington es necesario, para identificar las variables que podrían vincularse al ciberespacio para comprender cuáles son sus alcances y limitaciones en ámbito cibernético. Por otro lado, la identificación de los

instrumentos de cooperación regional e internacional de la Alianza permiten analizar sus capacidades en función del ciberespacio.

2.1.1 Artículo 4°, 5° y 6° del Tratado de Washington

Para 2023 la Alianza Atlántica, que tuvo sus inicios tras el fin de la Segunda Guerra Mundial bajo condiciones de posguerra, está conformada por 31 miembros.[10] En ese contexto, bajo el liderazgo de la extinta Unión de Repúblicas Socialistas Soviéticas (URSS) surgió también otra organización con un carácter similar, el Tratado de Amistad, Colaboración y Asistencia Mutua, mejor conocido como Pacto de Varsovia, que concluyó en 1991.

Por su parte, la OTAN se mantiene vigente, adaptándose al contexto internacional, avanzando en el desarrollo de capacidades para el mantenimiento de la seguridad de sus dominios, así como para el enfrentamiento con el enemigo en cualquiera de sus atribuciones dada la índole militar de la alianza.

Su creación está dada por el Tratado de Washington firmado el 4 de abril de 1949 por 12[11] miembros fundadores en la ciudad del mismo nombre, el cual, a pesar de los cambios en la escena internacional sigue siendo referente del quehacer de la organización. El Tratado se conforma por 14 artículos, por lo que es un documento breve que identifica los elementos que serán considerados a efectos de un conflicto armado, así como las adhesiones señaladas en su artículo 10° bajo el que la Alianza se ha ampliado con el paso de los años.

La relevancia de los artículos 4°, 5° y 6°, yace en que estos proveen los lineamientos de acción de la Organización frente un escenario de conflicto, en donde convergen distintos sectores además de la cuestión militar. El análisis del Tratado permite identificar la posibilidad de que los artículos sean invocados en función de los ciberataques a los países miembros de la OTAN, derivados de las crecientes amenazas en el ciberespacio.

---

[10] 1949: Bélgica, Canadá, Dinamarca, Estados Unidos, Francia, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido; 1952: Grecia, Turquía; 1955: Alemania; 1982: España; 1999: Hungría, Polonia, República Checa; 2004: Bulgaria, Eslovaquia, Eslovenia, Estonia, Letonia, Lituania, Rumanía; 2009: Albania, Croacia; 2017: Montenegro; 2020: Macedonia del Norte; 2023: Finlandia.

[11] Bélgica, Canadá, Dinamarca, Francia, Islandia, Italia, Luxemburgo, Países Bajos, Noruega, Portugal, Reino Unido y Estados Unidos

El artículo 4° señala que: “las Partes se consultarán cuando, en opinión de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes se vea amenazada” (*North Atlantic Treaty Organization*, 2019). Este artículo es que abre la posibilidad de consulta si alguno de los miembros considera que su “integridad territorial, la independencia política o la seguridad” están en riesgo para que de esta manera la Organización decida qué acciones tomar para garantizar la estabilidad.

El 24 de febrero de 2022 el presidente de Rusia, Vladimir Putin anunciaba lo que denominó una “operación militar especial”, evento que desató diversos debates, pues la comunidad internacional, en su mayoría califican al evento como una intervención militar, misma que generó protestas en distintos países en contra de la guerra. Asimismo, países como Estados Unidos, Reino Unido y los miembros de la Unión Europea, manifestaron su apoyo Ucrania y sobre todo en favor de la población que, para junio de 2023, las estimaciones señalan que hay más de 6 300 000 millones de personas refugiadas y más de 5 millones de personas desplazadas por motivos de la guerra (ACNUR). Lo anterior, en el marco de un acercamiento de Ucrania a la UE y por supuesto a la OTAN, situación que generó el descontento de Moscú, mismo que dio paso a un conflicto que para octubre de 2023, sigue vigente.

La relevancia este conflicto está en su desarrollo, en el que convergen características híbridas en donde, si bien, los efectivos militares, las batallas en tierra y la cantidad de armamento siguen teniendo un papel importante, la presencia de los ciberataques en el marco de la guerra destacan por su imprevisibilidad e impacto en la sociedad rusa y ucraniana. De manera que la “nueva modalidad de guerra no implica el fin de las guerras convencionales” (Mazurier y Payá, 2018) aunque, por otro lado, si pone en jaque a los planteamientos tradicionales, ya que elementos como el uso ataques a redes informáticas escapan a estos, generando así incertidumbre al enfrentarse a las amenazas en el ciberespacio.

Ahora bien, en ese sentido, la posibilidad de que el artículo 4° pueda ser invocado en caso de que alguna de las partes considere que los ciberataques ponen en riesgo alguna de las prerrogativas que este señala, de manera que abre la puerta a que países que se encuentren conectados ya sea física o virtualmente a Ucrania, se amparen en este artículo. Un ejemplo del alcance de los ciberataques ocurrió en 2017, en donde “el ataque NotPetya

se insertó una herramienta maliciosa de cifrado de datos en un software legítimo utilizado por la mayoría de las instituciones financieras y gubernamentales de Ucrania" (*National Cyber Security Centre*, 2018), que además de afectar instituciones financieras, gubernamentales y energéticas ucranianas, extendió sus efectos incluso en empresas europeas generando pérdidas por cientos de millones de libras.

El hecho de que *NotPetya* tuviera alcance internacional es alarmante, por lo que frente a la posibilidad de un escenario de guerra en donde algún miembro de la OTAN se viera afectado, es posible que se ponga a consideración la defensa colectiva como lo indica el artículo 4º, ya que el Tratado de Washington no contempla explícitamente a las amenazas en el ciberespacio como motivo de consulta, pero tampoco lo excluye. Por lo tanto, una de las fortalezas del tratado que da vida a la OTAN yace en que, aunque en su contenido no contempla un escenario como el espacio cibernético, si posee mecanismos sobre los que los países miembros pueden someter a consulta para servirse de las capacidades de la Alianza en caso de que así lo consideren.

La defensa colectiva expresada en su artículo 5° es el pilar de esta alianza político-militar, el cuál señala:

> Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudará a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán inmediatamente puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales. (*North Atlantic Treaty Organization*, 2019).

Este artículo da cuenta de la relevancia que tiene para la alianza la reacción ante un ataque, además de que la seguridad y defensa se entienden no solo de forma individual sino colectiva respondiendo de manera conjunta ante las amenazas, sobre esa misma línea está el artículo 6° que dice:

> A efectos del artículo 5, se considerará ataque armado contra una o varias de las Partes, el que se produzca:
>
> - Contra el territorio de cualquiera de las Partes en Europa o en América del Norte, contra los departamentos franceses de Argelia, contra el territorio de Turquía o contra las islas bajo la jurisdicción de cualquiera de las Partes en la zona del Atlántico Norte al norte del Trópico de Cáncer.
> - Contra las fuerzas, buques o aeronaves de cualquiera de las Partes que se hallen en estos territorios, así como en cualquier otra región de Europa en la que estuvieran estacionadas fuerzas de ocupación de alguna de las Partes en la fecha de entrada en vigor del Tratado, o que se encuentren en el Mar Mediterráneo o en la región del Atlántico Norte al norte del Trópico de Cáncer. (*North Atlantic Treaty Organization*, 2019)

El artículo 6°, enfatiza el alcance geográfico que tiene el Tratado de Washington de acuerdo con los países miembros, de manera que las fronteras físicas representan un elemento inviolable sobre el que la Alianza busca proteger en caso de un ataque, la delimitación es clara y permite tener certidumbre sobre las regiones que se encuentran bajo el paraguas de la OTAN. Sin embargo, a pesar de que el ciberespacio no obedece a fronteras geográficas tradicionales, la infraestructura física de los países miembros pueden ser un punto de partida para efectos de este artículo y la determinación del territorio euroatlántico.

En noviembre de 2020, Oana Lungescu, portavoz de la Alianza, señaló que el Compromiso de Defensa con los aliados también abarca al ciberespacio, “un ataque cibernético a un Aliado puede afectarnos a todos. Por eso, fortalecer nuestras defensas cibernéticas es una prioridad para la Alianza” (NATO, 2020b), de modo que el tema ocupa un lugar primordial en la agenda, en donde, por ejemplo, los equipos de defensa cibernética de reacción rápida operan las 24 horas para la protección de las redes informáticas a nivel nacional y de la OTAN.

Ahora bien, relativo a un contexto de conflicto bélico, es cada vez más común que a las agresiones se sumen ciberataques contra infraestructuras críticas, mismas que al ser fundamentales para el quehacer cotidiano de la sociedad y el Estado, podrían tener un impacto similar o mayor al de un ataque militar armado. De ahí que surjan cuestionamientos sobre el tratamiento para dichos eventos, puesto que, dependiendo de la gravedad de los incidentes, la OTAN funge como plataforma “para considerar posibles respuestas colectivas” (OTAN, 2021b) derivado de su incidencia en la seguridad euroatlántica.

La aplicación el artículo 5° en el caso de Estonia no se llevó a cabo a pesar de que el conflicto afectaba la seguridad nacional e independencia política (Instituto Español de Estudios Estratégicos [IEEE], 2010) de la nación báltica, y además derivado de la falta de la definición del carácter militar de un ciberataque, así como de la carencia de un plan de acción adecuado, la invocación de la defensa colectiva habría podido generar que el conflicto escalara más allá de las fronteras de Estonia. Empero, a pesar de que los acontecimientos no implicaron la aplicación de la defensa colectiva, ese evento fue parteaguas en el avance de instrumentos de defensa en el ciberespacio y visibilizó la posibilidad de que el ámbito cibernético puede ser utilizado como campo de batalla y quizá, en algún momento pueda traspasar la frontera física y generar un escenario de conflicto armado.

El Tratado de Washington no excluye al ciberespacio de su ámbito de aplicación (aunque tampoco lo incluye explícitamente), pero abre la puerta a su integración en futuros instrumentos, como el Concepto Estratégico (explicado en el apartado 2.3.2). Sin embargo, a pesar de la importancia de contemplar al ciberespacio como ámbito dentro de la seguridad Atlántica, resulta problemática su aplicación, derivado de la falta de elementos de Derecho Internacional que regulen y limiten los alcances de la OTAN frente a los ciberataques.

En ese mismo sentido para el caso de Estonia, si bien los ciberataques afectaron directamente la infraestructura de este país, la conexión con empresas y otros Estados ha incrementado, por lo que los efectos para la seguridad de la Alianza Atlántica podrían extenderse a otros miembros de la OTAN en escenarios futuros, ya que como señala Stephen Herzog:

> “Internet se ha convertido en una poderosa herramienta asimétrica para grupos transnacionales que se consideran privados de sus derechos y buscan intimidar a los Estados-nación y a otros actores presumiblemente responsables de sus quejas. Se trata de una cuestión de soberanía nacional, ya que las redes digitales y la infraestructura crítica atacadas por los piratas informáticos son propiedad de los Estados-nación o se encuentran en su territorio” (2011, p. 52)

Es por ello que, entre los principales retos para la organización y para la comunidad internacional están en:

1. Precisar y delimitar el alcance de las definiciones relacionadas con el ámbito cibernético, ya que el debate conceptual sigue vigente y su clarificación es fundamental para consolidar las estrategias en torno a estos.
2. Definir los alcances y restricciones del uso de instrumentos cibernéticos ya sea para prevenir, responder o disuadir los ciberataques, para evitar el uso arbitrario de estas capacidades y para dotar de certidumbre frente a los embates en el ciberespacio.
3. Identificar las divisiones, los organismos regionales e internacionales (por ejemplo, ONU, OTAN, UE, OEA, OCS), que podrían incidir en la regulación y cumplimiento del uso de las capacidades cibernéticas, dotándolas de las capacidades jurídicas suficientes, tomando en cuenta los tratados existentes en la materia y el Derecho Internacional, así como las características de cada región.
4. Consolidar las alianzas gubernamentales (dada la naturaleza impredecible y sofisticada de los embates cibernéticos) con el sector privado es imprescindible ya que gran parte de la investigación en el área de la ciberseguridad y ciberdefensa se desarrolla a través de la iniciativa privada, por ello la cooperación de estos sectores, en conjunto con la academia y la sociedad es esencial.

En el caso particular de la OTAN, para 2024 no se ha presentado un ciberataque que escale al nivel de un conflicto armado e impacte en las prerrogativas del artículo 4° o 5°. Sin embargo, con mayor frecuencia se presentan conflictos en donde se hace uso de cibercapacidades, que si bien, no son determinantes, son relevantes para los enfrentamientos y debilitamiento del bando atacado. Dado el avance en el desarrollo de las capacidades tecnológicas de países como Rusia, Estados Unidos, China e Israel, la posibilidad de que los artículos del Tratado de Washington tengan efecto en el ciberespacio es una realidad latente.

Asimismo, también es importante desarrollar estrategias que salvaguarden a otros miembros fuera del ámbito de influencia de la OTAN, ya que, el Tratado de Washington le permite a la Alianza integrar dominios distintos a los tradicionales al ámbito de la seguridad y defensa; de modo principalmente los países del Sur global podrían ver comprometida no solo su seguridad cibernética, sino también su soberanía.

2.2 Ciberataques: retos e implicaciones

La inclusión de millones de personas al ciberespacio y el aumento de actividades se realizan en línea trae consigo fenómenos emergentes de estas interacciones que hacen parte de las amenazas a la seguridad internacional. La forma en la que los Estados y la sociedad se relaciona con las tecnologías se ha transformado, generando cambios en las actividades diarias y relaciones interpersonales, de manera que surgen nuevos desafíos a la paz y seguridad internacionales que requieren de una sinergia entre Estados, organizaciones internacionales gubernamentales y no gubernamentales, iniciativa privada, asociaciones civiles y de la población en general.

Derivado de las amenazas en el entorno cibernético, se identifican los llamados ciberataques, que cuentan con características que los distinguen de otro tipo de agresiones. El *National Institute of Standards and Technology* del Departamento de Comercio de los Estados Unidos los define como

> un ataque, a través del ciberespacio, dirigido al uso del ciberespacio por parte de una empresa con el propósito de interrumpir, deshabilitar, destruir o controlar maliciosamente un entorno/infraestructura informática; o destruir la integridad de los datos o robar información controlada (*National Institute of Standards and Technology,* 2022).

La empresa de tecnología Cisco los define como:

> Un ciberataque es un intento malicioso y deliberado por parte de un individuo o una organización para irrumpir en el sistema de información de otro individuo u otra organización. Usualmente, el atacante busca algún tipo de beneficio con la interrupción de la red de la víctima. (Cisco, 2022)

Entre los principales ciberataques a Estonia y Georgia, se encuentran los dirigidos a la infraestructura crítica y a los servicios gubernamentales de información de inteligencia y también aquellos ataques cibernéticos que desinformaron a la sociedad a partir de *fake news*; de modo que la emergencia de las amenazas en el ciberespacio, genera múltiples preocupaciones con respecto a las TIC en relación con la seguridad y la confianza del uso de Internet y otros servicios vinculados al ámbito cibernético.

Desde 2002 la OTAN trabaja para responder a las amenazas, a través de la creación de organismos e instrumentos jurídicos. Tras los ciberataques a Estonia en 2007 se desarrolló una Política sobre Ciberdefensa y tras la Cumbre de Lisboa 2010 se incorporó esta preocupación al Concepto Estratégico (Segura, 2017, 296-297), (mismos instrumentos que se analizan apartados posteriores). De tal forma que los principios para hacer frente a los ciberataques son:

- Prevención de los ciberataques: a través del desarrollo de capacidades cibernéticas en el ámbito técnico y jurídico, capacitación de personal, así como el refuerzo de la ciberdefensa y la ciberseguridad.
- La resiliencia de las redes: que es la capacidad de recuperación y resistencia ante un ciberataque.

Ambos son responsabilidad de los Estados, puesto que tiene la facultad de proteger su entorno cibernético de las amenazas y funge como primer respondiente a través de sus fuerzas armadas, ministerio de defensa, equipos de respuesta y demás organismos ligados a la protección de la seguridad nacional. En este sentido, la OTAN brinda asistencia e instrumentos de complementariedad a los países miembros a efecto del Concepto Estratégico, el Nuevo Concepto Estratégico y su versión más reciente, el Concepto Estratégico 2022.

La relevancia de la digitalización trajo consigo nuevas oportunidades, pero también nuevos retos que se materializaron en ciberataques. Con la diversificación de las amenazas en el ciberespacio, la Alianza encaminó sus esfuerzos en la creación de instrumentos que avanzan hacia una gobernanza en el ciberespacio. Los ciberataques dan paso a la discusión sobre la necesidad de legislar y enfrentarse a estos con herramientas que permitan disuadir, responder y evitar que las consecuencias de estos alteren el funcionamiento de la sociedad.

Los ciberataques de 2007 y 2008 contra Estonia y Georgia, respectivamente, se abordan en el apartado siguiente. Ambos tuvieron doble alcance: interno e internacional; primeramente, a nivel nacional tuvieron impacto en el gobierno y la sociedad y, por otro lado, su efecto se multiplicó cuando después de estos la comunidad internacional sumó sus esfuerzos para enfrentarse a estos en escenarios futuros.

2.2.1 Estonia

Ubicada en Europa del Este, limitando con Letonia y Rusia, Estonia es el primer país digital del mundo, con alrededor de un 91% de personas usuarias de Internet (Banco Mundial, 2022), se ha logrado posicionar como uno de los países más conectados y avanzados en el rubro tecnológico, siendo el único país que permite al electorado votar de manera virtual incluyendo las elecciones nacionales. Con una gran presencia rusa en su historia, el país báltico guarda estrecha relación con la lengua, religión, cultura y población rusa, en este contexto es que se desarrollaron los eventos que marcaron un hito en el país, la OTAN y la UE.

En 2007, Estonia se vio inmersa en uno de los eventos más icónicos en el ciberespacio. Ese mismo año, el gobierno de la República de Estonia anunció la realización de excavaciones para buscar restos de soldados caídos en la Segunda Guerra Mundial a razón de su identificación y posterior entierro en el cementerio militar ubicado en su capital, Tallin. Dicha excavación sería realizada en la plaza Tornismäe, misma en donde se encontraba la estatua conocida como el *Soldado de Bronce* (originalmente llamada Monumento para los Libertadores de Tallin), instalada en 1947 por autoridades de la URSS.

El *Soldado de Bronce* poseía una carga simbólica distinta para los residentes pertenecientes a la comunidad rusa y para la comunidad nacional de Estonia, a partir de dicho anuncio, las protestas iniciaron tomando en cuenta dos posiciones sumamente divididas:

- Para los primeros representaba la victoria de la Unión Soviética sobre los nazis y,
- para la segunda era un símbolo de la era opresora bajo el mando soviético.

La polarización de las comunidades escaló con el paso de los días, llegando así el 9 de mayo de 2007, cuando las manifestaciones necesitaron de la intervención de la policía puesto que las protestas fueron llevadas al extremo, incluyendo la portación de banderas de la extinta URSS y la bandera de Estonia, de manera que la plaza se convertía en punto de encuentro entre ambas comunidades en un ambiente de agitación que empeoró con el paso de los días.

Así pues, la decisión del gobierno estaba tomada e iniciaron con los preparativos para el traslado. Sin embargo, esto causó mayor indignación y protestas, que llevaron a la llamada *noche de los cristales*, una serie de disturbios en los que "una persona murió, 156 resultaron heridas y hubo 1 000 detenidos" (McGuinness, 2017), mismos en los que la policía no logró tomar control hasta el día siguiente, el 27 de abril de 2007.

En ese contexto, cuando los enfrentamientos seguían en curso, simultáneamente se presentaron hechos que no dejaban duda de que Estonia estaba siendo blanco de ciberataques. Usualmente se señalaba que "los sitios web gubernamentales y bancarios que normalmente recibían 1.000 visitas al día colapsaron después de recibir más de 2.000 visitas por segundo" (Wilson, 2007, p.7), es decir, los sistemas fueron sobrepasados. Por su parte, Nestor Garnuza Artiles (Instituto Español de Estudios Estratégicos, 2011) identifica 2 fases acontecidas entre el 27 de abril y el 18 de mayo de 2007:

- Fase 1. Los ciberataques tenían un componente emocional sin grandes complejidades de carácter técnico y organizativo y sin capacidad para convocar a un gran número de atacantes; en palabras de Lauri Almann, Secretario Permanente del Ministerio de Defensa en ese momento, esta fase se caracterizó por el uso de herramientas de ciberataque rudimentarias y simples, realizadas principalmente por *hacktivistas* que atacaron sitios web de Estonia, especialmente del gobierno, del ministerio de Defensa y de los algunos partidos políticos. Incluso, el mismo secretario señaló que fueron advertidos explícitamente que se encontraban bajo un ciberataque, por lo tanto, se organizó un equipo de respuesta a través del Equipo Nacional de Respuesta ante Incidentes Informáticos (*Estonian CERT*).

- Fase 2. Del 30 de abril al 18 de mayo, en esta fase los ciberataques cobraron mayor complejidad en el aspecto técnico y organizativo. Los ataques a los sitios web de la primera fase seguían siendo atacados, pero esta vez con herramientas más sofisticadas que para su contención requerían de un conocimiento más especializado. Uno de los días más álgidos fue el 9 de mayo, día en el que se conmemora la fiesta nacional rusa, con un aumento del 150% de ataques en el marco de dicha conmemoración.

Este evento da cuenta de la relación entre la situación política que se estaba viviendo al interior de Estonia y los ciberataques perpetrados. La combinación de amenazas en el conflicto iniciado con el traslado del *Soldado de Bronce*, colocó al gobierno de Estonia en una posición en la que, frente a los enfrentamientos en las manifestaciones y a los ciberataques, ambos acontecimientos merecían atención en el mismo sentido, y que si bien, los ciberataques contribuyeron a polarizar aún más a la población, al mismo tiempo estaba siendo manipulada a través de una campaña de desinformación proveniente de medios como el *Baltic News* y el *Postimees*, en donde a partir de la información que daban en ese momento, apunta a la implicación de autoridades del gobierno ruso como autores de los ciberataques.

Entre los tipos de ataques que fueron utilizados en Estonia están los siguientes:

- Ataques de denegación de servicios, mejor conocidos como DDoS
- Ataques de desfiguración de sitios web (*web site defacement*).
- Ataques a servidores de sistemas de nombres de dominio.
- Correo basura (spam).

La convergencia de los ataques, aunado al contexto político de Estonia que en 2004 se adhirió a la OTAN y a la UE, dejó claro que el gobierno ruso buscaba influenciar en la población para generar desconfianza, inestabilidad y un ambiente de incertidumbre que tuvo impacto social, político y económico. El presidente del Parlamento de Estonia, Ene Ergma, dijo “cuando observo una explosión nuclear y la explosión que ocurrió en nuestro país en mayo, veo lo mismo” (Soesanto, 2022), ya que ese evento paralizó varias actividades e imposibilitó al gobierno, que no contaba con capacidades suficientes para enfrentarse a dichas amenazas.

En ese contexto, la invocación del artículo 5° pudo sentar precedente para la OTAN y la comunidad internacional en materia de ciberdefensa, sin embargo, en ese momento la definición de un ciberataque como una acción militar no estaba delimitada en la OTAN (y continúa sin precisarse en el sentido estricto), por lo que la aplicación de la defensa colectiva no fue ejecutada. Si bien, ya existían algunos instrumentos de reacción en caso de ciberataque, la Alianza Atlántica no había desarrollado los Conceptos estratégicos que abordan los apartados posteriores.

Asimismo, una de las consecuencias de estos ataques, fue el establecimiento de “la primera Embajada de Datos en el mundo. La Embajada de Datos es un servidor estonio que se encuentra ubicado fuera del país, pero que está bajo jurisdicción estonia” (Jorge, 2022), lo cual es un ejemplo de ciberresiliencia, ya que esto garantiza que los servicios digitales puedan continuar su función a pesar de ataques cibernéticos, desastres naturales u otra contingencia.

En suma, los ciberataques a Estonia fueron un parteaguas no solo para el país involucrado, sino para la OTAN que a partir de ese evento comenzó a tomar a las amenazas cibernéticas como un riesgo real y latente que debía ser abordado desde distintas perspectivas, la jurídica, técnica, cooperativa, etcétera puesto que los riesgos de las acciones combinadas podrían representar daños físicos para la población.

2.2.2 Georgia

Georgia obtuvo su independencia en 1991, cuando la URSS se disolvió. A diferencia de Estonia, cuenta con un desarrollo tecnológico menos desarrollado y su posición geográfica lo sitúa en un escenario de conflictos geopolíticos. Limita al norte con Rusia por lo que la injerencia del país ruso en el devenir político del país no se extinguió con su independencia. De modo que los ciberataques a Georgia en 2008 se generaron en el marco de un conflicto que tiene como protagonistas a Osetia del Sur y Abjasia, Georgia y Rusia.

El foco del conflicto está enmarcado en un creciente apoyo de Rusia a las regiones separatistas de Osetia del Sur (ubicado en la frontera entre Rusia y Georgia) y Abjasia (ubicada en el Cáucaso limita al norte con Rusia y al sur con Georgia y tiene salida al Mar Negro). De manera que el 7 de agosto de 2008 dio inicio la guerra de Osetia del Sur. Con Georgia por un lado y Osetia del Sur, Abjasia y Rusia por el otro, las fuerzas armadas de Georgia se enfrentaron a los grupos separatistas. Por la cantidad de población rusa en dichas regiones, Rusia respondió y reaccionó con operativos militares situados en territorio de Osetia del Sur el 8 de agosto, extendiéndose así a otras regiones de Georgia y el Mar Negro, por lo que el presidente de Georgia de ese momento, Mikheil Saakashvili declaró estado de guerra el 9 de agosto de 2008.

El caso de Georgia es relevante para esta investigación, porque se considera que fue la primera vez en la que fueron combinadas operaciones militares y operaciones cibernéticas en un contexto de guerra. De modo que fue escenario bélico con características que van más allá de las tradicionalmente conocidas, en donde la mezcla de ataques (armado e informático) tuvo efectos en el devenir del conflicto teniendo impacto en diversos estratos de la sociedad.

Luego de tres días, el 12 de agosto de 2008, el presidente de Rusia, Dmitri Medvédev decretó el fin de las operaciones militares aceptando el plan de paz propuesto por la UE. Bajo estos eventos, Ganuza Artiles (Instituto Español de Estudios Estratégicos, 2011) señala 3 fases de los ciberataques.

- Fase 1. Pre-conflicto armado. De junio de 2008 al 7 de agosto de 2008, los ataques perpetrados tuvieron poco alcance, principalmente fueron ataques de denegación de servicio (DDoS).

- Fase 2. Conflicto armado. Del 8 de agosto al 12 de agosto de 2008, es decir los cinco días del conflicto armado, en donde los ciberataques se realizaron a sitios web del gobierno, instituciones bancarias y agencias de noticias. En esta fase, los ataques debilitaron la confianza entre la población y su gobierno, así como la comunicación entre el entorno político y el militar, pieza clave para enfrentarse al escenario de guerra al que se enfrentaban, además de que los ciberataques también se desarrollaban en el sentido de influenciar en la opinión pública para inclinarla a favor de la causa rusa.

- Fase 3. Post conflicto armado. Del 13 de agosto al 23 de agosto de 2008, aunque los ciberataques se redujeron considerablemente, estos continuaron más allá de la firma del tratado de paz.

Los ciberataques que se presentaron fueron similares a los empleados en 2007 en Estonia, puesto buscaban disminuir la capacidad operativa y de comunicación entre políticos y militares, así como el debilitamiento de la confianza de la población con las instituciones gubernamentales. Entre los tipos de ataques utilizados se encuentran:

- Ataques DDoS utilizando *botnets* con una mayor coordinación y capacidad de daño que los usados en Estonia.
- Ataques de inyección, basados en el reconocimiento de objetivos y su impacto se debe a que son de difícil detección.
- Ataques de *malware*, fueron propagados a través de las redes sociales con el objeto de infectar software.

El debate sobre la pertinencia de contar con un plan de acción a efectos de la ciberdefensa y la ciberseguridad en el ciberespacio incrementó, llevando así a la OTAN a identificar las necesidades, retos y amenazas que pudieran vulnerar el espacio cibernético. Asimismo, se manifestó que en los casos de Estonia y Georgia, Rusia se detenta como el principal autor de los ciberataques, derivado del contexto en el que se realizaron los ciberataques, sin embargo, la falta de cooperación por parte de Moscú para la identificación de los responsables no permitió la obtención de pruebas para identificar a los agresores, por lo que estos eventos dejaron claro que la cooperación en este ámbito requería de estrategias conjuntas que pudieran dar certeza a las investigaciones para poder atribuir los ciberataques y así poder sancionar a quien resulte responsable.

2.2.3 Estados Unidos

Estados Unidos posee uno de los ejércitos más grandes del mundo, así como un complejo militar industrial sumamente desarrollado. Sin embargo, esto no lo vuelve inmune a los ciberataques, puesto que la hiperconexión requiere de redes informáticas, conexión a Internet, dispositivos electrónicos y por lo tanto redes eléctricas que día con día depende aún más del uso de computadoras e infraestructura que garantice la distribución de este servicio.

Hasta 2023, en Estados Unidos el 91.8% de la población tiene acceso a la electricidad (Kemp, 2023), es decir que posee una de la red eléctrica compleja, que derivado de la dependencia que existe entre los sistemas eléctricos y la infraestructura crítica del país, la vuelve blanco de ataques cibernéticos que han irrumpido en el quehacer de la sociedad y gobierno. Es así como, en 2021, la secretaría de Energía señalaba la importancia de la colaboración del sector público y privado en favor del sector energético para enfrentarse a las vulnerabilidades cibernéticas (Duster, 2021).

El departamento de Energía cuenta con una estrategia de ciberseguridad y con una Oficina de Ciberseguridad, Seguridad Energética y de Respuesta a Emergencias que aborda las amenazas emergentes al tiempo que busca proteger las redes energéticas del país (Enegy.gov, 2023). En diversas ocasiones, el país norteamericano señaló que fue víctima de ataques cibernéticos a sus redes eléctricas, en donde la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA por sus siglas en inglés) China, Rusia, Corea del Norte e Irán, mismas a las que señala como actores estatales que amenazan a la infraestructura crítica estadounidense (CISA, 2023).

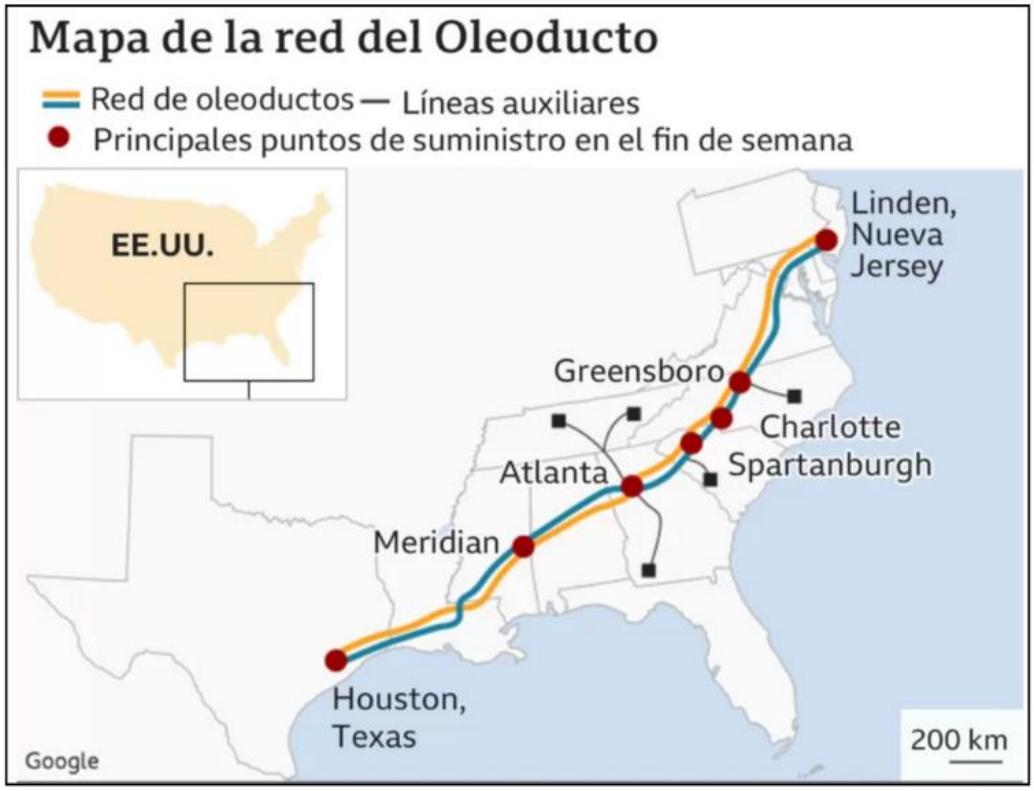
Los ciberataques también han sido dirigidos a la red de oleoductos. En mayo de 2021 el *Colonial Pipeline Company* sufrió uno de los cortes más importantes en el país, ya que tuvo impacto en el precio del combustible en alrededor de 18 entidades, generando un estado de emergencia, puesto que la población y el gobierno tuvieron que tomar medidas ante el cierre, generando así incertidumbre ante la falta de combustibles (BBC, 2021).

Los daños provenientes de los ciberataques se expandieron a través de la red de oleoductos. Entre las principales consecuencias se encuentran: las económicas, como el alza de precios del combustible y las sociales, ya que la población se vio afectada en el uso de vehículos y políticas, incluso el mismo gobierno vio afectado el suministro a aeronaves, aunado a ello los daños físicos de la infraestructura que se vio comprometida.

> Un aviso conjunto del DHS y el FBI confirmó que en el ataque se utilizó el ransomware DarkSide. Este aviso explicaba que para garantizar la seguridad del oleoducto, la empresa había desconectado proactivamente ciertos sistemas que monitorean y controlan las funciones físicas del oleoducto para que no se vieran comprometidos. Hasta el 12 de mayo, no había indicios de que estos sistemas operativos hubieran sido violados. Sin embargo, la desconexión de estos sistemas resultó en una suspensión temporal de todas las operaciones del oleoducto. (*U. S. Goverment Accountability Office,* 2021)

La imagen 1 señala el impacto geográfico que tuvo el ciberataque, en donde las afectaciones en Georgia, Carolina del Norte, Carolina del Sur, Virginia y Washington provocaron en la población civil, compras de pánico que trajeron como consecuencia un alza en los precios de la gasolina, es decir, el ciberataque tuvo impacto en el sector gubernamental, privado y en la sociedad, por lo que la transversalidad de los ciberataques es imprevisible.

Imagen 1. Red del Oleoducto



Fuente: BBC New Mundo (2021) EE. UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país, https://www.bbc.com/mundo/noticias-internacional-57033536

A pesar de que para 2021, el Ciber Comando estadounidense ya estaba en funciones, no fue suficiente para anticiparse al ciberataque a una infraestructura crítica que suministra gasolina y otros productos derivados en el sureste de EE. UU. La respuesta del Departamento de Energía coordinó al sector privado y estatal para reanudar las operaciones del oleoducto, incluyendo a la Administración Marítima, la Administración Federal de Ferrocarriles, la Administración Federal de Carreteras y la Administración de Seguridad de Materiales Peligrosos y Oleoductos, y para el 13 de mayo, Colonial Pipeline reanudó su sistema de tuberías. (*Office of Cybersecurity, Energy Security, and Emergency Responce*, 2023).

Como en el caso de Estonia, el ciberataque apuntó a un actor ruso, no se realizó una atribución oficial, es decir, la dificultad para identificar a los actores es una constante en el devenir de los ataques cibernéticos. A corto plazo, no se vislumbra un instrumento u organismo que provea de certidumbre para la identificación de los grupos o individuos que

atentan en el ciberespacio, sin embargo, el desarrollo de instrumentos regionales e internacionales por parte de la OTAN y sus aliados permite crear un entorno cibernético con mayor capacidad de respuesta y resiliencia.

2.3 Transformaciones y respuestas en el ámbito político-estratégico

En consecución de sus objetivos políticos y militares, la Alianza Atlántica complementa los acuerdos, tratados e informes con el desarrollo de evaluaciones anuales basados en métricas que le permiten a los países miembros identificar las vulnerabilidades y trabajar en ellas. La prevención, detección y respuesta frente a los riesgos en el ciberespacio necesitan de instrumentos técnicos, políticos e incluso militares.

En este sentido, la capacitación del personal, a través de ejercicios cibernéticos en tiempo real tiene la función de prevenir los embates a la seguridad; por su parte, los equipos de respuesta rápida y los centros especializados están en constante evolución, ya que los avances en el sector tecnológico son acelerados. Desde su creación, la OTAN desarrolla nuevas capacidades periódicamente, adaptándose a los requerimientos de los países miembros y el contexto internacional.

La multiplicidad de actores estatales y no estatales en el escenario cibernético representa un problema persistente que en diversas ocasiones no permite la aplicación del Derecho Internacional. Empero, los avances de la OTAN se materializan en una estructura robusta y sólida que descansa en estrategias, herramientas y organismos que favorecen el mantenimiento de la estabilidad en el ciberespacio, misma que brinda de una ventaja tecnológica e incluso jurídica a la Organización y sus miembros

Los efectos políticos, económicos y sociales de los ciberataques, exigen a los Estados incorporar los debates académicos y políticos en el desarrollo de elementos que respondan a las amenazas. Como dominio de operaciones en el siglo XXI, el ciberespacio abre la puerta a conflictos híbridos en un campo multidominio, que condicionan los daños a partir del nivel de respuesta de los involucrados, por lo que el incremento de capacidades en materia de ciberdefensa y ciberseguridad podría determinar la estabilidad en la escena internacional.

2.3.1 Política de ciberdefensa

La integración de la ciberdefensa en la agenda de la OTAN es relevante, ya que, con la incorporación de este concepto y su posterior ejecución, comenzaron a desarrollarse cibercapacidades en el ámbito político y militar. Así pues, la coordinación de la agenda política con la militar a nivel interno se consolida, al tiempo que sienta las bases de cooperación internacional de la alianza, de esto modo se robustecen las acciones en favor de la seguridad y defensa en el ciberespacio para enfrentarse a los desafíos y amenazas en este dominio.

En marzo de 2011 la Alianza Atlántica adoptó un Concepto de Ciberdefensa en el que define la protección de las redes de la OTAN como una responsabilidad fundamental de los aliados (Ministerio de Defensa del Reino de España, 2011) siendo uno de los primeros ejemplos en donde la OTAN da cuenta de la necesidad de incorporar al entorno cibernético como parte de sus preocupaciones. Lo anterior, derivado de acontecimientos como los ataques terroristas a EE. UU. y los ciberataques a Estonia en 2007.

Asimismo, los miembros han “adoptado políticas y planes de acción, estableciendo comités, agencias y centros operativos con el propósito de integrar el dominio cibernético tanto en las operaciones como en el desarrollo de capacidades de los aliados” (Marrone y Sabatino, 2021). Sin embargo, al interior de la Alianza se diferencian dos enfoques de ciberdefensa:

- Enfoque de defensa activa y ofensiva, que es perseguido por países como Estados Unidos, Reino Unido y Francia, que se proclaman en favor de una mayor inversión en la materia y participación de la Alianza en la escena internacional.
- Enfoque defensivo, en el que podemos encontrar a Alemania (Marrone y Sabatino, 2021) que por cuestiones históricas y sociales ha optado por posicionarse a través de instrumentos de cooperación.

En la Cumbre de Varsovia de 2014 se creó la Política Reforzada de la OTAN sobre Ciberdefensa (Mele, 2019) y posteriormente en la Cumbre de Varsovia de 2016, el ciberespacio se reconoció como un nuevo dominio militar equiparable a tierra, aire y mar. Este evento es clave para el tema ya que, con la integración del ciberespacio en la agenda de esta alianza político-militar, la ciberdefensa aumentaba su importancia contribuyendo a

las tres tareas centrales del Concepto Estratégico de la OTAN: defensa colectiva, operaciones de gestión de crisis y seguridad cooperativa (*North Atlantic Treaty Organization,* 2012).

La Cumbre condujo también a la firma del Compromiso de Defensa Cibernética en 2016 "que busca establecer una plataforma común para mejorar la defensa nacional y sus capacidades de resiliencia frente a un ciberataque" (*North Atlantic Treaty Organization,* 2016). Dicho compromiso tiene como objetivo garantizar el desarrollo de capacidades ante las amenazas cibernéticas y "reforzar la resiliencia de la región, así como la cooperación en defensa cibernética, al tiempo que genera conciencia, capacitación, seguridad y capacidad cibernéticas" (*North Atlantic Treaty Organization*, 2016).

De acuerdo con el artículo 3° del Tratado de Washington los miembros:

> "A fin de lograr más eficazmente la realización de los fines del presente Tratado, las Partes, actuando individual y conjuntamente de manera continua y efectiva mediante la aportación de sus propios medios y prestándose asistencia mutua, mantendrán y acrecentarán su capacidad individual y colectiva de resistir a un ataque armado." (*North Atlantic Treaty Organization*, 2019)

Por lo que bajo el Compromiso de Ciberdefensa la organización señala que busca el desarrollo capacidades y la asignación de los recursos adecuados para llevar a cabo dicha encomienda, incluyendo en su labor una mayor comprensión de los fenómenos del ciberespacio.

En un entorno en donde los ciberataques son cada vez más frecuentes, complejos y destructivos (*North Atlantic Treaty Organization*, 2019) en la Cumbre de Londres de 2019 la alianza tuvo un impulso político-estratégico para sus actividades. El secretario general Jens Stoltenberg declaró que "el ciberespacio es el nuevo campo de batalla y hacer que la OTAN esté preparada cibernéticamente (con buenos recursos, bien entrenada y bien equipada) es una máxima prioridad" (*North Atlantic Treaty Organization,* 2019).

Asimismo, año con año, la Alianza realiza distintos trabajos para identificar los desafíos emergentes que puedan socavar la seguridad de los países miembros, generando así instrumentos y acciones que se adapten al contexto. Ante la volatilidad geopolítica y los

retos que se han ido presentando, en junio de 2021 en el Comunicado de la Cumbre de Bruselas señala:

> “nos enfrentamos cada vez más a entornos cibernéticos, híbridos y otras amenazas asimétricas, incluidas las campañas de desinformación y por el uso malicioso de tecnologías emergentes y disruptivas cada vez más sofisticadas. Los rápidos avances en el dominio espacial están afectando nuestra seguridad.” (NATO, 2021)

El peso que tienen las tecnologías para la OTAN se visibiliza en su integración a la agenda política y posteriormente en la aplicación al ámbito militar, puesto que de estas emergen amenazas que ponen en jaque a la seguridad, ya sea en conflictos en donde participen Estados, grupos terroristas o en situaciones en las que delincuentes cibernéticos busquen obtener algún beneficio económico ya sea de instituciones gubernamentales, empresas o de la sociedad usuaria del espacio cibernético.

2.3.2 Evolución del Concepto Estratégico

La relevancia del Concepto Estratégico de la OTAN yace en que este provee a la Alianza y en general al concierto internacional una valoración sobre el estado actual de la seguridad internacional ya que identifica desafíos y amenazas, así como nuevas formas de enfrentarse a ellas, reconociendo la necesidad de cooperación, diálogo y la ampliación de capacidades políticas y militares.

En ese mismo sentido, el quehacer de la OTAN se da en función de distintos elementos que convergen en el desarrollo de sus conceptos estratégicos de acuerdo con sus objetivos fundacionales:

> Políticos: la OTAN promueve valores democráticos y permite que los miembros se consulten y cooperen cuestiones relacionadas con la defensa y la seguridad para solventar problemas, fomentar la confianza y, a largo plazo, evitar conflictos.
>
> Militares: la OTAN tiene un compromiso de resolución pacífica de controversias. Cuando los esfuerzos diplomáticos no dan fruto, la fuerza militar emprende operaciones de gestión de crisis. Estas operaciones se llevan a cabo bajo la cláusula de defensa colectiva del tratado fundacional de la OTAN (Artículo 5 del Tratado de Washington) o por mandato de las

> Naciones Unidas, por sí sola o en cooperación con otros países y organismos internacionales. (NATO, 2022)

En función de los objetivos político-militares, la Organización desarrolla instrumentos para mantener la seguridad de los miembros. El Consejo del Atlántico Norte (NAC) es la autoridad encargada de adoptar los documentos estratégicos de la OTAN que se adoptan en consenso, en donde se pueden identificar tres periodos históricos de pensamiento estratégico:

- Guerra Fría. Durante este periodo se desarrollaron cuatro conceptos estratégicos en donde además de la identificación de las estrategias de defensa y las amenazas nucleares, la URSS representaba una de las principales amenazas a la organización.
- Post Guerra Fría. Durante este periodo, podemos decir que representó uno de los mayores retos para la Alianza pues el enemigo principal se extinguía, por lo que la incertidumbre se cernía sobre los miembros, generando nuevas dinámicas en torno a la seguridad internacional.
- 2022 vino con un nuevo entorno estratégico, de manera que “con el Concepto Estratégico 2022, la OTAN se está adaptando a otro período, caracterizado por una competencia geoestratégica renovada como resultado del comportamiento agresivo de Rusia y el ascenso de China.” (NATO, 2022b)

La tabla 3, ofrece una síntesis de los conceptos estratégicos, señalando el periodo al que se circunscriben, la fecha, el momento histórico que enmarcó su creación, así como los temas principales que abordó de acuerdo con sus objetivos. La identificación de los Conceptos estratégicos se entiende a partir de las amenazas internacionales y por la forma en la que aborda temas que, incluso para 2024 continúan vigentes. Con el análisis de los antecedentes de la OTAN y de las acciones que desarrolla en el marco del conflicto entre Rusia y Ucrania, se puede comprender en enraizamiento de su influencia en la región, pues tiene papel en materia de seguridad y defensa.

Tabla 3. Evolución de los Conceptos estratégicos de la OTAN.

Periodo	Concepto Estratégico	**Contexto internacional**	**Temas relevantes**
Guerra Fría	6 enero de 1950	Creación de la OTAN	Concepto estratégico general, así como guía de defensa estratégica para su uso en la planificación de defensa integral.
	3 de diciembre de 1992	Guerra de Corea	Eficacia de las estructuras militares y las fuerzas de alianza
	23 de mayo de 1957	Represalias masivas	Capacidad frente a agresiones menores y en caso de agresión nuclear.
	16 de enero de 1968	Destrucción mutua asegurada	Flexibilidad y escalamiento en las dimensiones política y militar, integrando la noción de disuasión y distención.
Post Guerra Fría	8 de noviembre de 1991	Fin de la Guerra Fría	Seguridad de los miembros ampliando la misma a través de la asociación y cooperación.
	24 de abril de 1999	Guerras en la ex Yugoslavia	Definición amplia de la seguridad, identificando nuevos riesgos: terrorismo, conflicto étnico, abuso a los derechos humanos, inestabilidad política, proliferación de armas nucleares, biológicas y químicas.
	17 de mayo de 2010	Ataques terroristas 11-s	Identificación de amenazas tales como: terrorismo, ataques cibernéticos y problemas ambientales, adaptando estructuras militares y capacidades militares ampliando sus asociaciones
Nuevo entorno estratégico	29 de junio de 2022	Conflicto armado entre Rusia y Ucrania	Ampliación de las amenazas: terrorismo, cambio climático y aceleración de avances tecnológicos. Competencia estratégica renovada.

Elaboración propia con datos de North Atlantic Treaty Organization, (2022) Conceptos Estratégicos, https://www.nato.int/cps/en/natohq/topics_56626.htm

Con el fin de la Guerra Fría la supervivencia de la Alianza fue tema de debate, ya que uno de sus principales retos era dar certidumbre a los países miembros de que esta seguiría funcionando. El periodo inmediato al fin de la Guerra Fría la OTAN amplió sus miembros hacia el Este de Europa, generando así nuevas dinámicas en torno a la seguridad, puesto que satélites ex soviéticos ahora pasan a las filas de la OTAN, además de que se configuraban otros escenarios en los que la seguridad ampliaba sus horizontes.

A partir de 1991 la OTAN tuvo un enfoque más amplio de seguridad, sin dejar de lado los enfoques tradicionales, en donde, si bien los términos militares seguían siendo parte de esta, los referentes de la Escuela de Copenhague impregnaron su visión de la seguridad a partir de la integración de nuevos elementos que integraban factores no convencionales, tales como la seguridad humana.

Desde el Concepto Estratégico de 1999 la definición de seguridad fue ampliando sus alcances y se le dio más peso al diálogo y la cooperación, mientras que “de 1949 a 1991, la geopolítica internacional estuvo dominada por la confrontación bipolar entre Oriente y Occidente” (News, R., 2022). De manera que esto condujo a una carrera armamentista en la que el gasto en defensa era prioridad para los Estados. Sin embargo, los ataques terroristas del 11 de septiembre de 2001 a EE. UU., cambió el escenario puesto que este evento generó una vuelta a que la dinámica militar.

Los ataques terroristas trajeron como consecuencia la invocación del artículo 5° por primera vez en el seno de la OTAN, por lo que el terrorismo pasó a ser la amenaza principal, generando una serie de eventos que recrudecieron el conflicto y los conceptos de seguridad. De este modo, el Concepto estratégico de 2010 identificó al terrorismo como una de las principales amenazas, sin embargo, el camino recorrido en los noventa se hace visible puesto que los problemas ambientales pasaron a ser parte de la agenda junto con la búsqueda por el establecimiento de nuevas asociaciones y la necesidad de cooperación para enfrentarse a los desafíos de ese momento, integrando así también las amenazas híbridas, ello derivado de los ciberataques a Estonia en 2007 y Georgia en 2008.

El Concepto estratégico adoptado en Madrid en junio de 2022 surge en un contexto en el que Rusia pasó de ser un socio estratégico (para temas de terrorismo, control de armamento, medidas de confianza mutua a construcción de paz) a considerarse amenaza

para la paz. El octavo Concepto estratégico incluye entre sus desafíos el conflicto armado entre Rusia y Ucrania y reconoce la importancia del ciberespacio como un dominio de gran peso en la escena internacional.

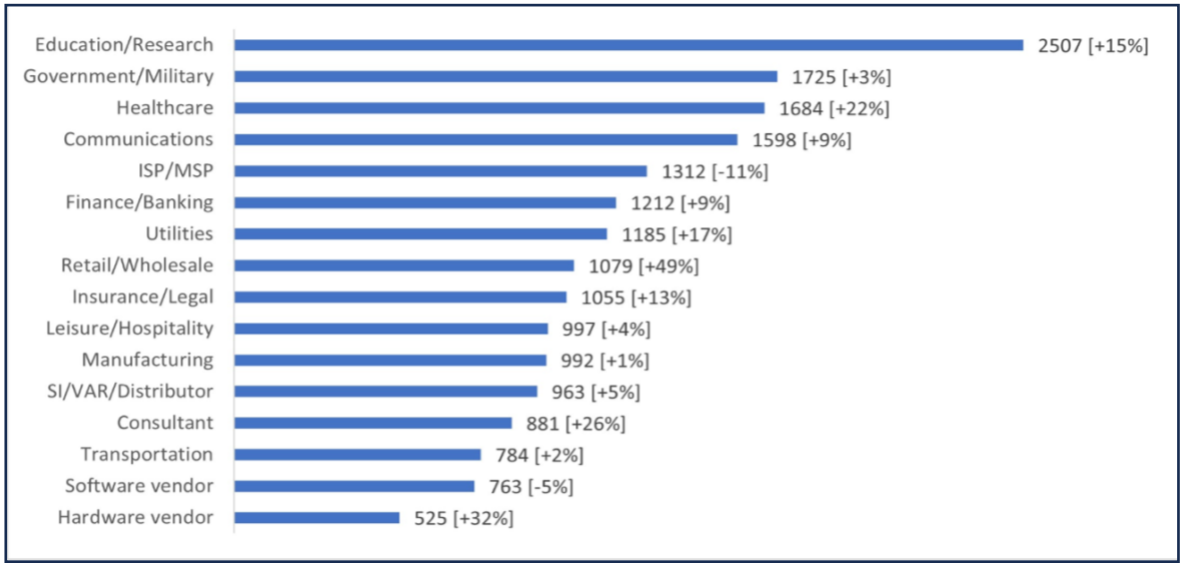
Asimismo, la Alianza señala una competencia estratégica renovada, en donde el autoritarismo y la inestabilidad generalizada se han potencializado, la amenaza del terrorismo persiste y tras la pandemia por el coronavirus SARS-CoV-2 los ciberataques en el espacio cibernético también aumentaron. El documento de abril de 2020 de la INTERPOL, *Panorama mundial de la ciberamenaza relacionada con la Covid-19*, señala que dicha pandemia dio un nuevo impulso a un gran número de delincuentes, por lo que hubo un aumento de ciberataques de diversos tipos, tales como:

- Dominios maliciosos: En Internet se registró un número importante de dominios con los términos relativos al Covid-19 para llevar a cabo campañas de correos no deseados o ataques de phishing.
- *Malware:* Una las actividades más comunes de los delincuentes cibernéticos es la integración de *malware, spyware* y troyanos en sitios web destinados a dar información sobre el coronavirus.
- *Ransomware:* Derivado de la dependencia de las conexiones en línea, los ciberdelincuentes lanzaron ataques de *ransomware* contra infraestructura del sector salud, puesto que la necesidad del funcionamiento de estos sistemas genera mayor probabilidad de que la víctima pague el rescate solicitado, sin embargo, esta práctica continua en ascenso.
- Ataques de Denegación de Servicio (DDoS): Si bien estos no buscan sustraer información, obstaculizan el funcionamiento de los sistemas comprometidos, generando así incertidumbre y desconfianza del uso de servicios en línea

Asimismo, en su informe *Ciberdelincuencia: Efectos de la Covid-19*, de agosto de 2020, identifica a la desinformación como uno de los principales ciberataques asociados a la Covid-19, en donde “el 27 % de los países que han contestado a la encuesta mundial sobre ciberdelincuencia han confirmado la circulación de información falsa sobre la COVID-19 entre su población y el 21 % ha manifestado una preocupación creciente ante esta tendencia” (INTERPOL, 2020b), siendo las redes sociales como *WhatsApp, Meta (Facebook)* y *X* (antes *Twitter)* los medios más usuales para difundir dicha desinformación.

En 2021 las tendencias sobre estos ciberataques no disminuyeron, siendo el *ransomware* el que tuvo mayor aumento en ese año, generando la necesidad de desarrollar múltiples capacidades para enfrentarse a la creciente diversidad de amenazas. Como se observa en la imagen 2, en donde se muestra el aumento de ataques, figurando el sector de la educación/investigación como el más afectado con 2507 ataques por semana, seguido del gobierno en el ámbito militar con 1 725 ataques y el sector salud con un promedio de 1684 ataques. En general hubo un incremento en todas las áreas, mismas que son indispensables para el funcionamiento de la sociedad, incluidos el sector de las comunicaciones, el sector salud, financiero y de transporte (*Check Point Software Technologies*, 2023).

Imagen 2. Promedio de ataques semanales por industria (comparación 2022-2023)



Fuente: *Check Point Software Technologies* (2023), *Global cyberattacks continue to rise with Africa and APAC suffering most,* https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

En ese mismo sentido, uno de los ataques de *ransomware* más destacados fue el perpetrado contra la estadounidense *Colonial Pipeline* a pesar de la inversión y desarrollo tecnológico que posee EE. UU. Los ataques dirigidos al sector energético destacan por su relevancia en diversas áreas como el abastecimiento a la sociedad en general, pero también en la industria militar, sobre todo en Estados Unidos, el cual como miembro de la OTAN no está exento ante esta modalidad de ciberataques.

La pandemia por el coronavirus SARS-CoV-2, representó un momento histórico importante para el desarrollo e incremento de ciberataques, mismos que potenciaron la necesidad de crear instrumentos que lo integren e identifiquen como amenazas a la seguridad nacional. La constante evolución de los ataques transformó los escenarios de conflicto, reforzando la posibilidad de utilizar al ciberespacio como campo de batalla, en donde la adaptación de los instrumentos como el Concepto Estratégico de la OTAN representa una fortaleza para la Alianza y sus miembros.

Desde 2014 (momento en el que el conflicto entre Rusia y Ucrania ya estaba presente) la OTAN había reforzado significativamente su postura de disuasión y defensa, mejorando la preparación de sus fuerzas. El conflicto armado que inició en 2022 requiere no solo de capacidades militares y aumento en el gasto de defensa, sino también de la voluntad política de los países miembros para que dicho conflicto llegue a su término, puesto que la organización ha manifestado su postura con respecto a la integración de Ucrania a la alianza, lo cual aumentó la tensión política con Rusia.

Es así como las 3 tareas fundamentales que se señalan en el Concepto estratégico de 2022 son:

- Disuasión y defensa.
- Prevención y gestión de crisis.
- Seguridad cooperativa.

Tomando en cuenta los Conceptos estratégicos anteriores a 2022 de la OTAN, la disuasión y defensa se mantienen y cobran fuerza debido al entorno actual, sin embargo, la prevención y gestión de crisis, así como la seguridad cooperativa se suman a ello dando a la Alianza una plataforma más amplia para enfrentarse al conflicto que se cierne en las fronteras de Europa. El conflicto entre Rusia y Ucrania provee de nuevas oportunidades para que la organización continué vigente al tiempo que también funciona como impulso hacia los países miembros que aún no alcanzan el 2% de gasto en defensa, tema duramente criticado durante la administración del ahora aspirante a la candidatura por la presidencia de los Estados Unidos, Donald J. Trump.

El Concepto estratégico integra nuevas amenazas al tiempo que propicia que la OTAN fortalezca el desarrollo de capacidades militares, jurídicas, económicas, técnico-operativas,

entre otras para alcanzar sus objetivos. La Alianza se presenta con múltiples enfoques en su forma de mantener la seguridad y defensa, ya que, si bien desarrolla y fortalece sus capacidades ofensivas, por otra parte, también incorpora temas como la seguridad energética y cambio climático, desastres naturales y atención a crisis migratorias, lo cual da cuenta de que la seguridad tiene múltiples dimensiones que es necesario atender.

Con el nuevo Concepto y la inclusión de la ciberdefensa dentro de las líneas de la OTAN, se amplió el espectro de operaciones y por lo tanto ello demandó nuevas áreas de acción, capacitación y por lo tanto la creación de fuerzas de reacción que respondieran a dichas necesidades en materia de ciberdefensa. Asimismo, el reconocimiento del ciberespacio como dominio de operaciones militares para la OTAN, abre la posibilidad a que en un futuro el artículo 5° pueda ser invocado a razón de un ataque cibernético, si bien aún existen vacíos legales en cuanto a cómo sería abordado tal caso, la realidad apunta a que los escenarios de conflicto evolucionan de forma acelerada, sin embargo, el Tratado de Washington facilita a Alianza la posibilidad de que, ante los ciberataques al entorno cibernético los países miembros puedan ampararse en la defensa colectiva.

2.2.3 Avances en la creación de instrumentos técnicos

La OTAN es una organización que a pesar de los cambios en la escena internacional se mantiene vigente. Su capacidad de adaptación y actualización le permite incidir e influir en la zona del Atlántico Norte y en general a nivel internacional. La estructura de la Organización está dotada de organismos que se encuentran en capacitación constante a través de ejercicios cibernéticos, que se adecuan al contexto fortaleciendo las capacidades de la Alianza y de sus miembros.

Los Centros de Excelencia (*CoEs-Centres of Excellence*) fueron creados con la finalidad de evitar duplicidad de funciones o gastos. Por su parte, el llamado Equipo de Reacción Rápida, creado en 2011, ofrece asistencia en caso de ciberataques en menos de 24 horas pasado el incidente cibernético; y en 2012 se creó el centro principal de la alianza responsable de la ciberdefensa, el Equipo de Respuesta a Incidentes de Seguridad Informática (*NCIRC, NATO Computer Incidents Response Capability Technical Centre*) que es responsable de proveer de capacidades para la protección de las redes de la OTAN.

La *NATO Communications and Information Agency* (NCI), creada en julio de 2012. Esta agencia cuenta con la participación de civiles y militares, en asociación con la academia y organizaciones sin fines de lucro; siendo la primera línea de defensa en caso de ataques cibernéticos, ya que está dotada de capacidades tecnológicas y cibernéticas que complementan los trabajos de la Alianza en materia de ciberseguridad y ciberdefensa. En octubre de 2023, la Agencia NCI realizó el *Exercise Steadfast Jupiter*, mismo que fue realizado por computadora que entrenó las "habilidades bélicas frente a un escenario de área operativa multidominio y multiconjunto basado en una simulación de crisis del artículo 5°." (*NCI Agency*, 2023)

Asimismo, la participación de Bélgica, Alemania, Italia, Países Bajos, Noruega, Reino Unido y Estados Unidos, en la colaboración con otros organismos, como el *NATO Cyber Security Centre* (que funciona 24 horas al día, 7 días a la semana), brinda a la Alianza de seguridad cibernética y de capacidad de respuesta y defensa. Además, a través de la *Cyber Security Collaboration Network* y el *National Computer Emergency Responce*, dota a los países socios y aliados, de mayor certidumbre y capacidad estratégica frente a las amenazas en el ciberespacio.

En la Cumbre de Madrid de 2022, el secretario general de la OTAN señaló la importancia de que para 2024, 19 países más se sumen a la lista de miembros que dedican el 2% del PIB al gasto en defensa (Martínez, 2022), dicho incremento se favorece a la red de Centros de Excelencia acreditados, al que pertenece el Centro de Defensa Cibernética Cooperativa (CCDCOE por sus siglas en inglés) que se formó a raíz de los ataques contra Estonia en 2007.

El CCDCOE colabora con los países miembros a través de investigación, entrenamiento y ejercicios de ciberdefensa, trabajando sobre cuatro enfoques: tecnología, operaciones, estrategia y ley. El Centro con sede en Estonia, posee un Comité Directivo se compone de un representante por nación y entre sus funciones están orientar, controlar y decidir en torno a la administración, políticas y funcionamiento (CCDOCOE, 2023), mismo que tiene la estructura jerárquica que se observa en la imagen 3.

Imagen 3. Estructura de CCDCOE

Fuente: CCDCOE (2023), About us, https://ccdcoe.org/about-us/

El CCDCOE realiza ejercicios de simulación, prevención y capacitación en el ciberespacio, tales como:

- *Coalition Warrior Interoperability eXercise* (CWIX): las partes comparten tácticas, técnicas y procedimientos en la búsqueda de fortalecer sus capacidades a la hora de rastrear los ciberataques, para que las consecuencias sean las menos posibles, atendiéndolos de manera rápida y eficaz. (*NATO Modelling & Simulation Centre of Excellence*, 2022).
- *Trident Juncture:* es el más grande de la organización, puesto que se llevó a cabo en el aire, tierra, mar y ciberespacio, en donde a través de distintos ejercicios se ponen a prueba las capacidades ante ciberataques a infraestructuras críticas. (*Exercise Trident Juncture* 2018, 2023).
- *Trident Jaguar:* este ejercicio se realizó en 2018, a través de este, las partes entrenaron y evaluaron las operaciones de respuesta en ejercicios de simulación asistida por computadora identificando vulnerabilidades en las infraestructuras. (*Agency,* N., 2023).
- *Cyber Coalition*: es un ejercicio anual, mismo en el que participan los países miembros, además de la industria y la academia, de manera que busca capacitar a las fuerzas de la Alianza para defender las redes de la OTAN y las redes nacionales. (*NATO's ACT*, 2022)

La creación del Centro de Excelencia y la realización de ejercicios señalados, dan cuenta de la capacidad ofensiva y defensiva de la OTAN. De manera que la organización vela por el cumplimiento de sus objetivos políticos y militares, materializando sus cibercapacidades a través de ejercicios de simulación, capacitación de personal, innovación y desarrollo de tecnología, entre otros.

Aunado a lo anterior, los ejercicios *Locked Shields* y *Crossed Swords*, realizados en abril y diciembre de 2023 respectivamente, son simulaciones interactivas en el mundo real que dotan a expertos en seguridad cibernética de herramientas para mejorar sus habilidades en la defensa de la infraestructura crítica de la Alianza Atlántica (NATO, 2023e). Con operaciones cibernéticas defensivas y ofensivas, incluyendo a países miembros y no miembros de la OTAN, los ejercicios tienen como objetivo la planificación y operación táctica y técnica frente a ciberataques, lo cual impulsa a la Alianza en la capacitación de su personal frente a los embates en el ciberespacio.

La Cumbre de Vilna de julio de 2023 sumó la creación de la *Virtual Cyber Incident Support Capability* (VCISC) que busca apoyar a los países miembros a mitigar los daños de las actividades cibernéticas maliciosas, lo cual dota a las naciones de una herramienta que provee nuevas capacidades de respuesta, en donde tras un ciberataque la recuperación y resiliencia cibernética son fundamentales. De manera que este instrumento técnico fortalece y complementa las acciones políticas, como el Compromiso de Defensa Cibernética de 2016.

La Alianza Atlántica posee ventaja tecnológica en tecnologías emergentes y disruptivas que se encuentra en constante proceso de evaluación y mejora, que a su vez reduce riesgos y costes asociados a los ataques cibernéticos. Además, sumado a los esfuerzos internacionales que buscan mantener la estabilidad en un ámbito multidominio, en colaboración con la industria, academia, organizaciones y el sector civil y militar, las capacidades de la OTAN continúan ampliándose, diversificándose y fortaleciéndose en tierra, aire, mar, espacio y ciberespacio.

2.4 Asociación estratégica entre la OTAN y la Unión Europea

La cooperación es fundamental para lograr enfrentar con éxito los desafíos y amenazas en el ciberespacio. Una de las grandes necesidades de cara a las ciberamenazas, para lograr la atribución de los ciberataques, es el trabajo conjunto, tal es el ejemplo de Estonia, en los que la negativa del gobierno ruso a cooperar impidió que el atentado pudiera ser aclarado y sancionado. Sin embargo, aunque a nivel estatal los debates en torno a la soberanía en la materia siguen vigentes, existen instrumentos regionales e internacionales en los que, a través de la colaboración, los países miembros pueden tener mayor certidumbre en un dominio tan dinámico como lo es el ciberespacio.

El 12 de noviembre de 2018, en el marco del Foro de la Paz de París, se pronunció el *Llamamiento de París para la confianza y seguridad en el ciberespacio* que cuenta con la participación de más de 1 200 (*Paris Call,* 2021) participantes, incluidos 80 Estados. Una de las característica principales es que el *Llamado* no incluye solamente a Estados, sino que se apoya también en empresas y asociaciones profesionales y organizaciones de la sociedad civil, de modo que permite la aproximación desde múltiples enfoques al tiempo que reconoce la relevancia y responsabilidad de diversos actores, pues como Celestino del Arenal señala que “en términos generales, se puede decir que desde el siglo XVII hasta la fecha relativamente reciente un único paradigma ha dominado absolutamente en el campo del estudio de las relaciones internacionales” (Del Arenal, 1989) refiriéndose a la primacía que detenta el Estado en el tema de la seguridad y defensa.

El *Llamamiento* cuenta con nueve principios (*Paris Call*, 2021) en los que centra sus esfuerzos y aunque no se trata de un acuerdo vinculante, pone sobre la mesa una diversidad de temas que sin duda seguirán siendo parte de las preocupaciones concernientes al ciberespacio y por lo tanto a la ciberseguridad de los Estados.

1. Proteger a las personas y la infraestructura crítica de prácticas cibernéticas maliciosas.
2. Proteger la accesibilidad e integridad de internet.
3. Defender los procesos electorales a través de la cooperación
4. Defender la propiedad intelectual.
5. Prevenir la proliferación de software y programas maliciosos

6. Incrementar la seguridad del ciclo de vida de procesos, productos y servicios digitales.
7. Promover la higiene cibernética para todos los actores.
8. Prevenir ciberdelitos de actores no estatales y privados.
9. Fortalecimiento de normas internacionales para generar confianza en el ciberespacio.

Asimismo, que desde su unión en 2019, las principales empresas sobre las que el *Llamamiento de París* se sostiene son: *Microsoft*, *Kaspersky*, *Siemens*, *Google*, Meta (*Facebook)* y *Huawei* (*France diplomacy,* 2021), lo cual da cuenta de que la ciberseguridad requiere de esfuerzos que no descansan exclusivamente en Estados u organizaciones internacionales, puesto que la sinergia con la iniciativa privada es una necesidad para generar un entorno cibernético seguro, en donde la convergencia de múltiples perspectivas suman a las iniciativas y regulaciones en el ciberespacio.

Por otro lado, la UE es una organización supranacional en constante adaptación a las necesidades internacionales. A través de su alianza con la OTAN ha logrado potenciar sus capacidades con respecto a la seguridad en el ciberespacio evitando duplicidades. Sin embargo, derivado de la guerra entre Rusia y Ucrania, ante la necesidad de generar nuevos instrumentos para enfrentarse a aquellas formas que atentan contra la seguridad internacional, la Unión diversifica su campo de acción, incluyendo el ámbito cibernético.

En el Concepto estratégico de 2022, la OTAN señala la relevancia que tiene la asociación estratégica con la Unión, generando una defensa europea más fuerte en la que ambas organizaciones se nutran. Frente al conflicto entre Rusia y Ucrania, la Alianza Atlántica señala la importancia de “las iniciativas para aumentar el gasto en defensa, desarrollar estrategias coherentes y reforzar mutuamente las capacidades, al tiempo que se evitan duplicaciones innecesarias, son clave para nuestros esfuerzos por hacer más segura la zona euroatlántica.” (Concepto Estratégico, 2022)

Es así como la relación entre la OTAN y la UE fortalece a ambas organizaciones, derivado sus acuerdos, evitan la duplicidad de gastos y capacidades. En relación con las Estrategias Nacionales de Ciberseguridad (ENC) de los países miembros de la Unión, en el portal de ENISA se puede observar que incluso aquellos que no son miembros de la UE tienen

alineados 21 objetivos encaminados a mejorar sus esfuerzos en el tema de la ciberseguridad.

Las medidas adoptadas por los países miembros de la UE, así como los aliados estratégicos en sus ENC, son los siguientes:

1. Abordar el delito cibernético.
2. Adoptar estándares de seguridad de la información.
3. Equilibrio de la seguridad con la privacidad.
4. Conciencia ciudadana.
5. Protección de la infraestructura de información cibernética.
6. Desarrollo de planes nacionales de contingencia crítica.
7. Cooperación internacional.
8. Establecer una asociación público-privada.
9. Establecer una capacidad de respuesta a incidentes.
10. Establecer una forma institucionalizada de cooperación entre organismos públicos.
11. Establecer e implementar políticas y capacidades de regulación.
12. Establecer requisitos de seguridad básicos.
13. Establecer mecanismos de reporte de incidentes.
14. Establecer mecanismos confiables para compartir información.
15. Fomentar la I + D.
16. Organizar ejercicios de ciberseguridad.
17. Proporcionar incentivos para que el sector privado invierta en medidas de seguridad.
18. Enfoque de evaluación de riesgos.
19. Establecer una estructura de gobierno clara.
20. Fortalecer los programas de capacitación y educación.
21. Mejorar la ciberseguridad de la cadena de suministro

Los puntos de las Estrategias incluyen a la sociedad en general, con la búsqueda por el desarrollo de la conciencia ciudadana y fortalecer los programas de capacitación y educación; y con el establecimiento de una asociación público-privada, fomentando la investigación y desarrollo, y proporcionando incentivos para que el sector privado invierta en medidas de seguridad. El ámbito privado tiene un peso importante en la ciberseguridad

por lo que, las alianzas entre empresas y gobierno son indispensables para lograr que las ENC de los países europeos y sus aliados pasen del papel a la práctica.

La actualización de los objetivos de las ENC europeas en 2023, es un ejemplo de la forma que la especialización y evolución de los ciberataques determina la forma en la que, en este caso, la UE, se adapta e integra nuevos puntos importantes a considerar por los países miembros. Asimismo, en un contexto de conflicto, como el que se desarrolla entre Rusia y Ucrania, los ciberataques han afectado las cadenas de suministro, mismas que son esenciales para el funcionamiento de la sociedad y gobierno, que en este caso requiere de una robusta capacidad operativa en el sector militar y humanitario.

En la tabla 4 se observa que los puntos críticos de las ENC, están ligados al uso de estándares relevantes para la protección frente a las ciberamenazas, el establecimiento de estructuras nacionales acordes al Reglamento de la Ley de Ciberseguridad de la Unión Europea, la cooperación e intercambio de información entre países a largo plazo y en tiempo real, el establecimiento de políticas específicas para incentivar al sector privado a mejorar los niveles de ciberseguridad y en la realización de evaluaciones de riesgos para mantener la ENC actualizada. La falta de certeza frente a un entorno dinámico como el ciberespacio, frena el avance de las Estrategias, que se enfrentan a diversos obstáculos ligados a la incertidumbre, el temor por la pérdida de soberanía y la carencia de estándares conceptuales, técnicos y jurídicos, con respecto al alcance de los instrumentos políticos y militares.

Tabla 4. Objetivos del análisis de la Estrategia Nacional de Ciberseguridad por país y sus aliados europeos

	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21
1. **Finlandia** 21.01.2013	✓		✓	✓	✓	✓	✓	✓	✓			✓	✓		✓	✓	✓			✓	
2. **Austria** 20.03.2013	✓				✓	✓	✓	✓	✓	✓		✓	✓		✓	✓				✓	
Islandia* 01.04.2015																					
3. **Croacia** 07.10..2015	✓		✓				✓		✓			✓	✓		✓						
4. **Francia** 10.10.2015	✓		✓	✓	✓	✓	✓		✓	✓		✓	✓		✓	✓				✓	
5. **Eslovenia** 01.02.2016	✓		✓	✓	✓		✓		✓	✓			✓			✓				✓	
6. **Bulgaria** 18.07.2016	✓		✓	✓			✓		✓				✓		✓					✓	
7. **Malta** 26.09.2016	✓			✓			✓		✓				✓							✓	
Reino Unido** 29.11.2016		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
8. **Italia** 01.03.2017	✓		✓	✓	✓		✓		✓	✓		✓	✓		✓	✓				✓	
9. **Suecia** 22.06.2017	✓		✓	✓	✓	✓	✓	✓		✓					✓	✓					
Suiza*** 18.04.2018	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓			✓				✓	
10. **Hungría** 21.03.2018					✓	✓	✓		✓	✓		✓	✓			✓				✓	
11. **Países Bajos** 21.04.2018		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
12. **Lituania** 13.08.2018	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓			✓	✓		✓		✓	
13. **Letonia** 01.01.2019	✓		✓	✓	✓	✓	✓		✓			✓								✓	
Noruega*** 31.01.2019	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓			✓	
14. **España** 01.04.2019	✓		✓	✓	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓			✓	
15. **Estonia** 09.05.2019	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓		✓	
16. **Portugal** 06.06.2019	✓		✓	✓	✓		✓		✓	✓		✓	✓		✓	✓				✓	
17. **Polonia** 31.10.2019	✓			✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓				✓	
18. **Irlanda** 27.12.2019		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
19. **Chipre** 12.03.2020	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
20. **Grecia** 12.07.2020	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
21. **República Checa** 01.01.2021		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
22. **Eslovaquia** 07.01.2021	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
23. **Dinamarca** 12.01.2021	✓			✓	✓	✓	✓		✓			✓	✓		✓	✓				✓	
24. **Alemania** 09.09.2021	✓			✓	✓	✓	✓		✓	✓		✓								✓	
25. **Bélgica** 20.05.2021	✓			✓	✓		✓	✓	✓	✓			✓		✓	✓				✓	
26. **Luxemburgo** 11.10.2021	✓			✓	✓	✓	✓	✓	✓	✓		✓	✓			✓				✓	
27. **Rumania** 30.12.2021	✓			✓	✓	✓	✓	✓	✓			✓	✓		✓					✓	✓

*Cuenta con una Estrategia Nacional de Ciberseguridad con objetivos diferentes a los catalogados en esta tabla, sin embargo forma parte del mapa interactivo del que se extrajeron los datos.
**No es miembro de la Unión Europea, ni miembro EFTA, sin embargo fue miembro de la UE y siguen compartiendo algunas formas de trabajo.
***Miembro EFTA (European Free Trade Association).

Elaboración propia con datos del mapa interactivo de las Estrategias nacionales de seguridad cibernética, 10 de agosto de 2023, disponible en: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

El 21 de marzo de 2022, el Consejo Europeo aprobó la Brújula Estratégica que se enfoca en dotar a la UE de un plan que fortalezca la política de seguridad y defensa hasta 2030. De forma complementaria con la OTAN, la Unión busca contar con mecanismos que incrementen sus capacidades a través de un aumento en el gasto en defensa y el mejoramiento de las estrategias que inciden en el proceso de toma de decisiones ante las amenazas.

La relevancia de la Brújula Estratégica radica en que integra a la agenda de la UE a la anticipación, disuasión y respuesta frente a las amenazas híbridas y los ciberataques. A través de instrumentos de ciberdefensa y ciberdiplomacia la Unión, se enfoca en concretar sus competencias en la arena internacional y regional incluso frente a la manipulación de la información (*fake news*), que potenciaron tras la pandemia y que continúan presentes en el contexto de la agresión militar de Rusia contra Ucrania.

De tal forma que tomando en cuenta los puntos frágiles que aún no se integran a la mayoría de las ENC dentro de los principales retos para la UE y para la comunidad internacional se encuentran temas ligados a la soberanía nacional y al uso de información gubernamental para identificar el origen de las agresiones. A pesar de la cooperación es uno de los pilares para que las estrategias de ciberseguridad y ciberdefensa funcionen, también es importante que al interior del país las reglas sean claras con al marco de actuación definido, por lo que, si no existe claridad a nivel nacional, difícilmente la tendrán con sus pares regionales e internacionales.

Capítulo 3. El ciberespacio como escenario de conflicto para la OTAN

El dinamismo de los escenarios de conflicto en el siglo XXI es una variable inevitable para los análisis en materia de ciberseguridad y ciberdefensa. La velocidad de los avances tecnológicos incide directamente en el desarrollo de los enfrentamientos bélicos, llegando a ser incluso determinante. No obstante, las circunstancias en el espacio cibernético responden a características distintas a las que tradicionalmente se conocen para los dominios como tierra, aire y mar.

En el ciberespacio coexiste lo virtual y lo físico, en donde este último es esencial para que el ciberespacio sea parte de la realidad material. De este modo, surge una arena intangible en donde las fronteras virtuales son difusas al tiempo que son parte de la cotidianidad de empresas, la sociedad, el Estado y sus instituciones, pero también del crimen organizado, grupos terroristas, delincuentes cibernéticos, entre otros.

Las amenazas en el ciberespacio son dinámicas, multidimensionales y evolucionan a una velocidad que no le permite a los Estados desarrollar instrumentos que interfieran con los ciberataques sin causar daños. Una de las mayores fortalezas que posee la Alianza (además de la multiplicidad de capacidades con las que cuenta) está en el nivel de resiliencia, puesto la magnitud de los daños depende del tiempo de respuesta, como un elemento fundamental y de la posibilidad de reestablecer los servicios de la infraestructura vulnerada. A pesar del avance en la creación de capacidades cibernéticas, la OTAN no está exenta de ser víctima de ciberataques, ya sea en infraestructura y redes colectivas o de los países miembros a nivel nacional.

Por su parte, el conflicto entre Rusia y Ucrania está ligado a los intereses de la Alianza Atlántica, de manera que la cooperación OTAN-Ucrania en materia política, social, económica, militar y cibernética es imprescindible. Además, la participación del sector privado y el sector civil es relevante, puesto que las amenazas cibernéticas cubren un amplio espectro de posibilidades en donde un incidente cibernético puede extender su impacto fuera de los límites ucranianos, por lo que, si los daños afectaran a algún miembro de la OTAN, la aplicación del artículo 5° sobre defensa colectiva es cada vez más probable.

3.1 Amenazas cibernéticas a la seguridad euroatlántica

El uso de las TIC se consolidó, sobre todo hacia el siglo XXI, a partir de la necesidad de conexión y el aumento de dispositivos electrónicos en el mundo, la sociedad está cada vez más inmersa en el ciberespacio. En ese mismo sentido, con las tecnologías de la información los Estados impulsan su poder militar, ya que las integran para fortalecer a las fuerzas armadas y por ende al equipo militar, por tanto, las agresiones militares se vuelven más precisas, eficaces y destructivas. Al vulnerar las redes informáticas y de comunicaciones, la población civil puede ser afectada, derivado de que “las tendencias muestran también que muchas actividades civiles y militares en un mundo virtual y conectado van unidas” (Wegener, 2012, p.146) es decir, la incidencia del ciberespacio en los conflictos es cada vez más frecuente y determinante.

Los conflictos tradicionales requieren de manera obligatoria de equipo tangible como: tanques, aeronaves, submarinos, vehículos blindados, misiles, embarcaciones navales, incluidos el personal militar, los números son importantes e incluso determinantes para el éxito o fracaso de una operación militar. En el espacio cibernético también se requiere de personal capacitado, empero la cuestión cuantitativa con respecto a los efectivos militares no es decisiva porque se trata de una forma no convencional de conflicto que se aleja a los conceptos clásicos de seguridad y defensa, en donde los daños y consecuencias por ciberataques “son intangibles en su acción, pero tangibles en los eventuales daños.” (Lazar, 2018, p.158)

El poder en el ciberespacio escapa a los parámetros habituales de medición, ya que las capacidades cibernéticas determinarán, en conjunto con la infraestructura física y virtual, el éxito o fracaso de las operaciones. En ese mismo sentido, el poder cibernético, según Joseph S. Nye es “un régimen híbrido único de propiedades físicas (infraestructuras, los recursos, las reglas de soberanía y jurisdicción) y las propiedades virtuales que dificultan el control del gobierno sobre las primeras” (Klimburg y Faesen, 2018, p. 3).

Para 2024 no existe un evento que pueda categorizarse dentro de lo que Lazar señala como *ciberguerra*, es decir, que el origen de un conflicto armado provenga de ciberataques y que sus consecuencias necesiten de la aplicación del Derecho Internacional Humanitario (Lazar, 2018, p. 163). Sin embargo, como se señala en el capítulo 2, los ciberataques a Georgia en

2008 se realizaron en el marco de un conflicto armado con Rusia con ataques simultáneos en varios dominios. Tras ese caso, se vislumbra un escenario en donde los conflictos tienden hacia a hibridez ya no como excepción a la regla, sino como la regla (Mazurier y Payá, 2018, p.22).

La pandemia por el coronavirus SARS-CoV-2 aceleró un proceso que se venía gestando desde inicios del siglo XX: la Cuarta Revolución Industrial, caracterizada por el incremento del comercio electrónico, la expansión de la educación en línea y el trabajo remoto, y la digitalización de procesos en diversos sectores, incluyendo el militar. Sin embargo, la migración digital abrió la puerta a que el entorno cibernético se viera vulnerado por crecientes amenazas que con el tiempo han intensificado la frecuencia de sus ataques y la su eficacia.

El año 2024 de cara al conflicto entre Rusia y Ucrania, frente a un escenario en donde los ciberataques en sus distintas modalidades son parte de los enfrentamientos, genera nuevos retos a los que la comunidad internacional aún se encuentra en ciernes en materia de ciberdefensa. Por lo tanto, la capacitación y adaptación son variables indispensables ante las vulnerabilidades cibernéticas puesto que su efecto puede ir más allá del espectro militar y extenderse más allá de las fronteras geográficas.

Asimismo, el reconocimiento de las amenazas cibernéticas en la agenda de seguridad y defensa sitúa al ciberespacio como un entorno que es preciso proteger, las cuales se integraron en el Concepto estratégico de 2022. El presente capítulo se centra en el análisis de los retos y amenazas que la OTAN reconoce en el dominio cibernético, considerándolo como un objeto de disputa permanente, en el que, junto con las tecnologías emergentes y disruptivas, buscan atender, reforzando su postura de disuasión y defensa en conjunto con los aliados y el sector privado.

Las ciberamenazas pueden ser igual o más peligrosos que las balas o las bombas, ya que la hiperconectividad maximiza su alcance. Las consecuencias de estas afectan directamente a la sociedad civil, en donde se genera la imposibilidad para acceder a servicios bancarios y servicios básicos (como la electricidad, agua potable y servicios de salud), la comunicación de aeronaves y otros medios de transporte.

En este tenor, durante el periodo de pandemia se presentaron diversas afectaciones en el área cibernética con respecto a sectores relativos a la salud. En un inicio, los ciberataques buscaban obtener información sobre el desarrollo de vacunas. Si bien, la conectividad y dependencia de los hospitales no es la misma en todo el mundo, para la OTAN, este tipo de ciberataques representaron una amenaza seria; países como Estados Unidos, España y Reino Unido, se enfrentaron a ciberataques en sus sistemas sanitarios.

Los ciberataques se multiplicaron con el avance del confinamiento, como lo señala el Ministerio de Defensa del Reino de España:

> El año 2020 comenzó con el final del soporte de Microsoft5 a sistemas Windows 7 y Windows Server 2008. Esto supuso un nuevo revés para las infraestructuras de hospitales (muchos de ellos todavía con dispositivos Windows XP), que les dejaba expuestos ante nuevas vulnerabilidades y actores dispuestos a explotarlas. (2021, p.28)

Lo anterior destaca porque cuando los sistemas digitales se encontraban amenazados, los pacientes no podían ser atendidos con la prioridad requerida, problemática que en 2022 y 2023 continúo en aumento. La empresa *Check Point Software Technologies* realizó un estudio “revelando que el sector sanitario experimentó una media de 1684 ataques semanales en el primer trimestre de 2023, lo que supone un incremento interanual del 22%” (2023), lo cual da cuenta de que este sector se mantiene como uno de los principales objetivos en el ámbito cibernético.

La transformación y constante evolución de las amenazas es uno de los temas principales en la agenda de la OTAN. Asimismo, el fortalecimiento de instrumentos basados en el Derecho Internacional en el ciberespacio es una de las tareas pendientes que la Alianza está desarrollando, con el establecimiento del Centro de Excelencia de Ciberdefensa Cooperativa, la *NATO Communications and Information Agency* y el *NATO Cyber Security Centre*, la Organización mantiene una posición de liderazgo que dota a los miembros de ventajas estratégicas el ámbito cibernético.

El capítulo 2, abordó el Concepto estratégico adoptado en junio de 2022 que sienta las bases hacia la consolidación del reconocimiento de las amenazas cibernéticas, generando nuevos debates, ya que las amenazas están interconectadas y sus afectaciones son de índole global. En el documento señala que entre las principales amenazas se encuentra a

la Federación Rusa como la más importante y directa, derivado de la invasión al territorio ucraniano. El terrorismo, la inestabilidad en África y Oriente Próximo, Norte de África y el Sahel, así como las "políticas coercitivas de la República Popular de China" (NATO, 2022, p.5) son otras de las amenazas a la seguridad y valores euroatlánticos que señala la Alianza.

Respecto al ciberespacio, la OTAN señala que, este "es objeto de disputa permanente. Los actores malignos pretenden degradar nuestras infraestructuras esenciales, injerirse en nuestros servicios gubernamentales, extraer información de los servicios secretos, robar propiedad intelectual y obstaculizar nuestras actividades militares" (NATO, 2022, p.5), de modo que la Alianza tiene una postura de defensa híbrida, en donde combina fuerzas convencionales, espaciales y cibernéticas.

La pandemia por el coronavirus SARS-CoV-2 trajo como consecuencia una aceleración al proceso de transformación digital, por lo que la adaptación tuvo alcance en todo el globo. Con ello vinieron un sinfín de oportunidades, pero también de amenazas, pues las tecnologías están al alcance de delincuentes cibernéticos que se sirven de estas para incidir en la escena internacional, "alterando el carácter de los conflictos, adquiriendo una mayor importancia estratégica y convirtiéndose en escenarios clave de la competencia mundial. La primacía tecnológica tiene cada vez más influencia sobre el éxito en el campo de batalla". (NATO, 2022, p.8)

Ya desde el informe anual de 2020, la OTAN menciona que las amenazas no convencionales se encuentran los ataques cibernéticos señalando que podrían "afectar a las naciones aliadas por debajo del umbral de un ataque armado, mientras que la información hostil podría desestabilizar comunidades políticas sin la necesidad de que un soldado cruce una frontera" (NATO 2020b, p. 27) La Alianza también identificaba la desinformación, la piratería y el espionaje como las principales amenazas (NATO 2020b, p.23), ya que durante la pandemia las actividades en línea se volvieron clave, sin embargo esto tuvo como consecuencia que los delincuentes cibernéticos explotaran las vulnerabilidades del ciberespacio.

En el informe posterior de 2021, indica que los ataques de *ransomware* aumentaron, mismos que provienen de actores estatales y no estatales, afectando principalmente

infraestructura crítica y cadenas de suministro de los países miembros (Informe anual 2021, p. 30) por lo que, con la Política Integral de Defensa Cibernética convergen los esfuerzos políticos, militares y técnicos para hacer frente a las ciberamenazas. Por lo tanto, los aliados se comprometieron también a invertir en capacidades defensivas y desarrollar nuevas estrategias militares y no militares en el ámbito cibernético.

En ese mismo sentido, el informe de 2022 manifiesta el aumento de las amenazas cibernéticas en donde "los actores malignos buscan degradar la infraestructura crítica, interferir con los servicios gubernamentales, extraer inteligencia, robar propiedad intelectual e impedir las actividades militares" (NATO 2022c, p.38), sumado a ello, estas amenazas cobraron mayor importancia derivado del conflicto entre Rusia y Ucrania, puesto que se presume de una combinación de ataques militares convencionales y no convencionales, generando una mayor cooperación entre los aliados para reforzar las capacidades cibernéticas frente a las amenazas híbridas, que la OTAN señala, provienen principalmente de Rusia y China.

El Concepto estratégico de 2022 recoge esa identificación y reconocimiento de las amenazas en el ciberespacio y en función del fortalecimiento de la disuasión y defensa menciona:

> Aceleraremos nuestra transformación digital, adaptaremos la estructura de mando de la OTAN a la era de la información y mejoraremos nuestras ciberdefensas, redes e infraestructura. Promoveremos la innovación y aumentaremos nuestras inversiones en empresas emergentes y tecnologías disruptivas para mantener nuestra interoperabilidad y nuestra ventaja militar. (Concepto Estratégico 2022, pp. 9 y 10)

Este compromiso se suma a los instrumentos con los que la organización ya cuenta, como son los ciber ejercicios anuales, las capacitaciones y las alianzas internacionales. Las labores de la Alianza Atlántica están en constante proceso de adaptación para enfrentarse a los retos, desafíos en el ciberespacio, ya que las amenazas cibernéticas poseen características intrínsecas que requieren de herramientas y procesos particulares, para evitar que estas socaven la estabilidad y confianza de la sociedad.

Por su parte, el 11 y 12 de julio de 2023, se llevó a cabo la Cumbre de Vilna, misma que centró sus discusiones en torno a la disuasión y defensa y en el apoyo de los aliados de la

OTAN a Ucrania. De dicho evento, destaca la participación de Finlandia como país miembro y de Suecia con una membresía que espera la ratificación del parlamento turco. Asimismo, con respecto al ciberespacio, el comunicado oficial de la Cumbre señala que "un conjunto único o acumulativo de actividades cibernéticas maliciosas podría alcanzar el nivel de ataque armado y podría llevar al Consejo del Atlántico Norte a invocar el Artículo 5 del Tratado de Washington," (NATO, 2023b) de manera que reafirmó su compromiso con la ciberdefensa que requiere de cooperación civil-militar y con el sector privado, para mitigar los daños frente a las amenazas cibernéticas.

En ese mismo sentido, se realizó la primera Conferencia anual de Ciberdefensa, el 9 de noviembre de 2023 en Berlín, que reunió a los tomadores de decisiones en la materia en el nivel político, militar y técnico, que, en palabras del secretario general de la OTAN, Jens Stoltenberg:

> "Políticamente, significa enviar un mensaje fuerte a los adversarios potenciales de que habrá consecuencias si nos atacan.
>
> Militarmente, significa tener las capacidades necesarias para operaciones cibernéticas defensivas y ofensivas. Y defender activamente nuestra parte del ciberespacio, incluidas las propias redes de la OTAN.
>
> Técnicamente, significa desarrollar resiliencia en nuestras sociedades. En particular, necesitamos sistemas de comunicaciones fiables y seguros, incluidas las redes 5G." (NATO, 2023e)

Además, señaló también la importancia de la creciente competencia estratégica en donde la incursión de Rusia y China en el ciberespacio difiere de los valores e intereses de la Alianza; también mencionó la relevancia de la protección de las personas y redes, así como del trabajo conjunto con el sector privado.

Los esfuerzos y compromisos de la Alianza en torno al ámbito cibernético cubren diferentes áreas, ya que este dominio opera en el sector económico, político, social y militar, por lo que las necesidades son diversas. Empero, el enfoque está en abordar las amenazas en el ciberespacio en los distintos momentos en los que se puede desarrollar para tener un campo más amplio de actuación. La prevención, disuasión, defensa y la resiliencia cibernética son relevantes a la hora de consolidar las estrategias, ya que, dependiendo de su objetivo político, podrá complementar su quehacer con herramientas militares y técnicas.

3.1.1 Escenarios de conflicto de la OTAN en el ciberespacio

La fronteras físicas y políticas que en 1648 marcaron hito en la creación de los Estados, derivado de la naturaleza del ciberespacio, para 2023 son difusas y endebles, por esta razón el alcance de los conflictos abarca más de un dominio. A consecuencia de la hiperconexión, el espacio cibernético también es trastocado y tiene incidencia innegable en el curso de estos, es decir, los conflictos poseen cualidades globales, multidimensionales y asimétricas.

Frente a ese panorama, uno de los retos a los que se enfrenta la Alianza Atlántica yace en el debate que existe frente al peligro de que las amenazas cibernéticas se materialicen en ciberataques que escalen a conflictos armados, mismos que a su vez generarían consecuencias otros dominios. A pesar de que es un caso hipotético, la emergencia de las tecnologías y su aplicación en el sector militar, pone sobre la mesa la posibilidad de que el espacio cibernético origine un conflicto armado a escala global.

El *Informe anual de 2020* de la OTAN señala que frente a un ciberataque grave podría llevar a invocar el artículo 5° del Tratado de Washington, por su parte, el informe de 2022 señala que “los aliados también reconocieron que un conjunto único o acumulativo de actividades cibernéticas maliciosas podrían alcanzar el nivel de ataque armado y llevar al Consejo del Atlántico Norte a invocar el artículo 5.” (NATO, 2022c, p.23)

Las consideraciones que tiene la Organización frente a los embates en el ciberespacio abren la puerta a la aplicación de la defensa colectiva. Las amenazas en el ciberespacio ponen en jaque a la seguridad internacional ya que vulneran estructuras digitales, físicas, económicas y políticas, por ello Alianza suma importancia al tema con el paso de los años.

El Concepto Estratégico de 2022 entre sus compromisos señala:

> Invertiremos en nuestra capacidad de preparación, disuasión y defensa contra el uso coercitivo de tácticas políticas, económicas, energéticas, de información y otras tácticas híbridas por parte de agentes estatales y no estatales. Las operaciones híbridas contra los aliados podrían alcanzar el nivel de ataque armado y llevar al Consejo del Atlántico Norte a invocar el Artículo 5 del Tratado del Atlántico Norte. Seguiremos apoyando a nuestros socios para hacer frente a los desafíos híbridos y maximizar las sinergias

> con otros actores relevantes, como la Unión Europea. (Concepto estratégico, p. 12)

La variable cibernética en un conflicto armado es esencial ya que su alcance no se ciñe solo al ámbito de operaciones, sino también al político, económico y por supuesto a la sociedad civil. Derivado de ello, las posibilidades de que los ataques cibernéticos escalen a nivel de un conflicto armado están presentes en la agenda internacional, por ello la relevancia de la protección de las infraestructuras críticas y el fortalecimiento de la capacidad de respuesta frente a los ciberataques.

La Conferencia anual de Ciberdefensa de noviembre de 2023, reforzó los compromisos de la OTAN con el ciberespacio, señalando que:

> Lo cibernético es parte de la tarea central de disuasión y defensa de la OTAN y la guerra de Rusia contra Ucrania ha puesto de relieve el uso de lo cibernético en los conflictos modernos. La Alianza trabaja para proteger sus propias redes, opera en el ciberespacio, ayuda a los Aliados a mejorar su resiliencia y proporciona una plataforma para la consulta política y la acción colectiva. (NATO, 2023d)

Por lo anterior, se observa que el conflicto entre Rusia y Ucrania trajo consigo el reconocimiento del entorno cibernético como un campo de batalla en donde los ciberataques tienen un rol importante en el devenir del conflicto. Aunado a ello, la potencia de las amenazas cibernéticas tiene efectos directos en el curso de los conflictos, ya que como se aborda en el apartado siguiente, el sector militar depende de las comunicaciones para la ejecución de sus operaciones, asimismo, la infraestructura crítica, al ser vulnerada puede traer consigo consecuencias a gran escala. Si bien, para 2024, la ciberguerra no existe, en la realidad el espacio cibernético se ha convertido en un campo de batalla determinante para el curso de los conflictos a los que la OTAN y la comunidad internacional se enfrentan.

El ciberespacio, por su naturaleza posee características que escapan a las definiciones tradicionales sobre seguridad y defensa, por lo que sus requerimientos no se sostienen en un ingente número de cuadrillas armadas, ya que se encuentran fuera de los márgenes clásicos del ejército. Si bien, el desarrollo de los conflictos se sostiene principalmente en las capacidades militares convencionales con las que cuenten las partes involucradas, el

espacio cibernético es un entorno que podría ser, incluso, determinante en el éxito o fracaso de los embates.

3.2 El ciberespacio y la OTAN en el marco del conflicto Rusia-Ucrania

En 2014 el conflicto entre Rusia y Ucrania se convirtió en el foco de atención para la comunidad rusa. Las disputas entre una facción en favor de una relación más cercana a la Unión Europea, con la posibilidad de llegar a ser parte de la OTAN, y otra que prefería mayor acercamiento al gobierno ruso, terminaron con la anexión a Rusia de una región de importante valor geoestratégico: la península de Crimea. A través de un referéndum realizado el 16 de marzo de 2014, en el que se presume que un 96% (*Deutsche Welle*, 2014) de la población votó en favor de la adhesión a Rusia.

Además de los eventos políticos, económico y militares que desencadenó la anexión de Crimea a Rusia, en el ámbito cibernético también se produjeron ataques. El portal BBC menciona que el jefe de seguridad de ese entonces, Valentyn Nalivaichenko, señaló que se perpetraron ciberataques a la red de telecomunicaciones, “produciendo un ataque a miembros del parlamento de Ucrania” (Lee, 2014), incluso hay señalamientos que dicen que también se presentaron intervenciones físicas en infraestructura asociada a las redes manipulando el cableado de fibra óptica.

En diciembre de 2015, los ciberataques a la red eléctrica ucraniana causaron un apagón que afectó a más de 230,000 hogares (*Council on Foreign Relations*, 2015) durante más de 6 horas en algunas zonas. Un año más tarde, en 2016 los ministerios de finanzas, de defensa y la Tesorería de Ucrania sufrieron alrededor de 6,500 ciberataques (Zinets, 2016), por lo que la estrategia rusa se hizo presente por varios frentes, incluido el cibernético, aunque con efectos que hasta ese momento no traspasaros las redes y fronteras de Ucrania.

A razón de lo anterior, en septiembre de 2015, se creó la Representación de la OTAN en Ucrania conformado por Centro de Información y Documentación de la OTAN creado en 1997 y la Oficina de Enlace de la OTAN inaugurada en 1999 (NATO, 2023c). A través de dichas instancias, se facilita la cooperación, en particular en el desarrollo de capacidades de comunicaciones estratégicas y el mejoramiento del diálogo político y práctico entre

autoridades militares y civiles de la Alianza y Ucrania. De manera que el contacto y acercamiento con los ministerios, instituciones, agencias y la sociedad ucraniana favorece la identificación de amenazas a la seguridad euroatlántica y el suministro de equipo de apoyo frente a las amenazas híbridas.

En ese mismo sentido, en 2017, el gobierno del Reino Unido señaló que Rusia fue el responsable del ciberataque conocido como *NotPetya*. “El ataque demostró un continuo desprecio por la soberanía de Ucrania. Su imprudente publicación perturbó a organizaciones de toda Europa y costó cientos de millones de libras” (*National Cyber Security Centre*, 2018), ese ciberataque tuvo impacto fuera de la nación ucraniana, demostrando que los ataques en el ámbito cibernético podrían tener efectos incluso en otros países, vulnerando empresas, gobierno y sociedad. Dado el impacto de los ciberataques a Ucrania, el tema generó diverso debates y estudios a nivel internacional.

La complejidad de los ciberataques y la relevancia del dominio cibernético tuvieron efectos directos en el quehacer de la OTAN, que reforzó sus políticas, estrategias e instrumentos de acción, frente a nuevos escenarios de conflicto. Desde los incidentes de 2014 y 2015 a la red eléctrica, Ucrania comenzó con un proceso de descentralización digital; posteriormente, en febrero de 2019, la asamblea parlamentaria de Ucrania aprobó incluir la adhesión a la OTAN y la UE como objetivos dentro de la Constitución y en ese mismo año se creó el Ministerio de Transformación Digital de Ucrania, mismo que está ligado a *IT Army of Ukraine* (que se aborda en el apartado 3.2.1).

En 2016 la OTAN reconoció al ciberespacio como domino militar equiparable a tierra, aire y mar, y en ese mismo año, con el Compromiso de Defensa Cibernética los miembros de la Alianza Atlántica se comprometieron a desarrollar nuevas medidas en materia de ciberdefensa, tema que está ligado al artículo 3° del Tratado de Washington. Asimismo, estos eventos trajeron como consecuencia que en 2017 la organización creara “como parte de la nueva Estructura Adaptada de Mando, un nuevo centro de operaciones del ciberespacio para integrar en todos los niveles las ciberdefensas nacionales, en la planificación y en las operaciones aliadas” (Fuente, 2022 p. 89).

En ese contexto, las amenazas en el entorno cibernético aumentaron, sobre todo durante la pandemia por el coronavirus SARS-CoV-2, en donde el periodo que va de 2020 a 2021

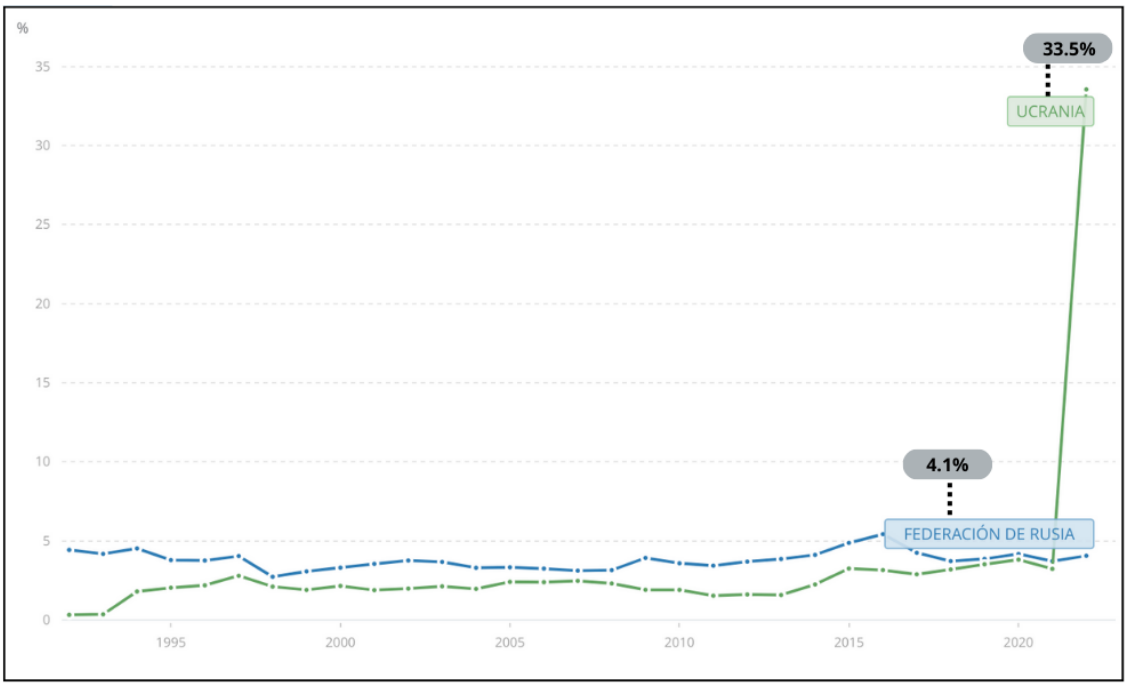
fue un escenario convulso no solo en el sector salud, sino también en el ciberespacio. Los esfuerzos se enfocaron en la creación de vacunas y tras el confinamiento, la migración digital era parte del día a día de la sociedad, organizaciones, empresas y el Estado.

El 24 de febrero de 2022 el mundo atestiguó el inicio de la invasión de Rusia a Ucrania, denominada “operación militar especial” por el presidente Vladimir Putin, un hecho que, para el cierre de esta investigación, sigue en curso. Dicho evento, señalado como una agresión por la mayor parte de la comunidad internacional, comenzó con el ejército ruso cruzando la frontera con Ucrania sirviéndose de armamento como tanques, vehículos de combate de infantería, cañones autopropulsados, entre otros, surgiendo así un conflicto en el que la OTAN y los países de la UE han tenido incidencia desde distintos frentes.

Este evento modifica los parámetros tradicionales de los conflictos internacionales y ofrece una configuración con variables cibernéticas que siguen generando incertidumbre a nivel internacional. Además, trajo consigo diversos debates en torno al gasto militar, posturas geopolíticas y hacia cuestiones de índole energética derivado de la relación entre Rusia y la Unión Europea. La relevancia del gasto en armamento tradicional como: naves, aeronaves, submarinos, tanques, vehículos blindados, embarcaciones navales, municiones, entre otros, incluida la cantidad de efectivos militares, es una constante, además de que la capacitación del personal y de la sociedad, la innovación, la adaptación y la inversión son elementos de gran importancia para lograr que los ciberataques tengan el menor impacto posible. Así pues, la variable de los ciberataques se ha convertido en pieza fundamental en el devenir del conflicto, generando nuevas formas de debilitar a las fuerzas armadas, al gobierno y por lo tanto a la población.

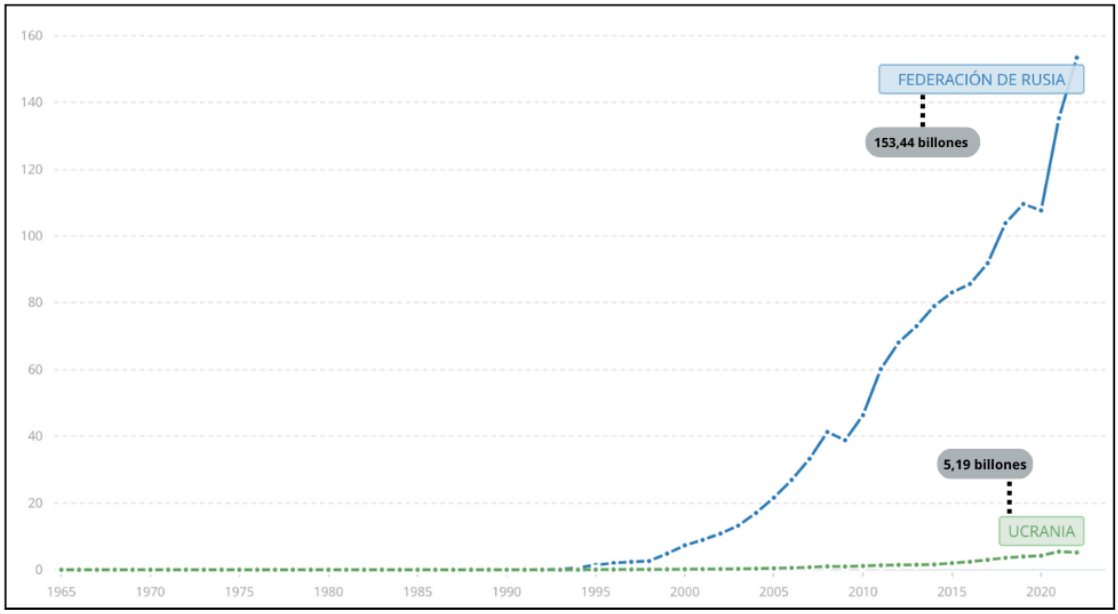
Datos del Banco Mundial señalan que, en 2022, Rusia tuvo un gasto militar del 4.1% de su PIB anual, frente a un 33.5% para Ucrania (tabla 5), lo que significa que casi una tercera parte del total del producto interno bruto ucraniano que equivale a 5,19 billones de dólares está destinada al sector militar, mientras que Rusia posee 153,44 billones de dólares (tabla 6). De manera que la cooperación internacional y en particular, el apoyo de la OTAN es fundamental para el aprovisionamiento de las fuerzas ucranianas, ya que, a pesar del aumento en el sector militar, Rusia es uno de los países con mayor gasto militar a nivel mundial, por lo tanto, esto favorece la continuidad del conflicto, ya que, aunque las fuerzas rusas no se han doblegado, tampoco han vencido.

Tabla 5. Gasto militar (% del PIB) 2022. Rusia-Ucrania



Fuente: Banco Mundial (2023) Gasto militar (% del PIB), https://datos.bancomundial.org/indicador/MS.MIL.XPND.GD.ZS?locations=RU-UA

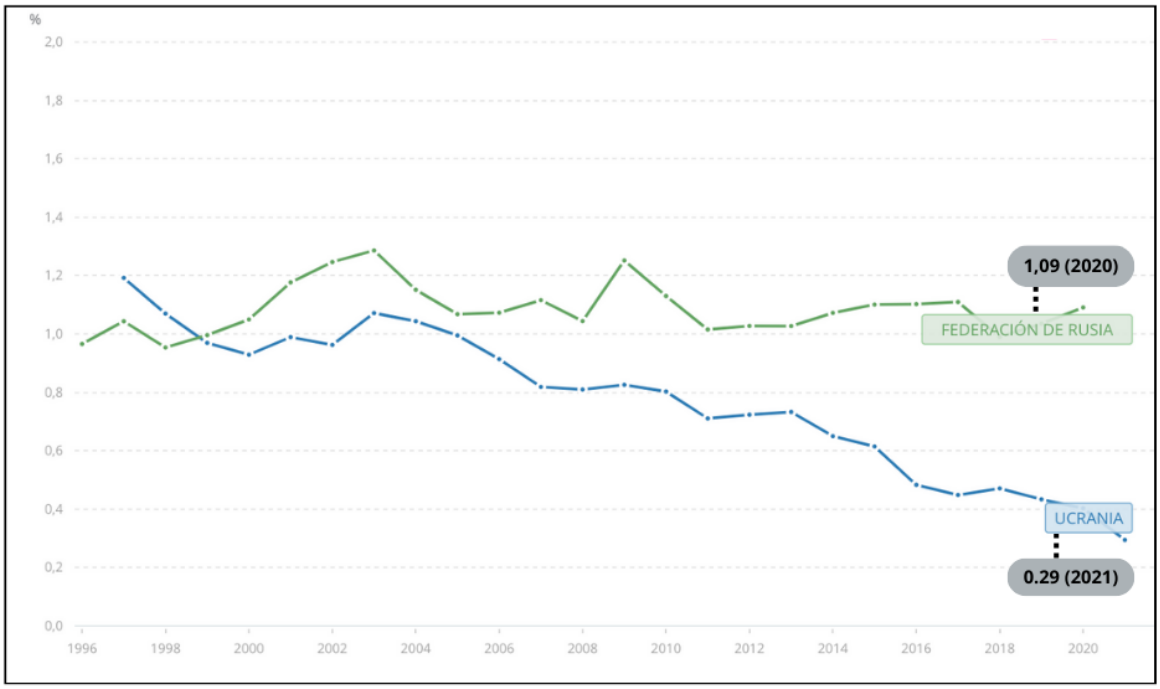
Tabla 6. PIB (UMN a precios actuales) 2022. Rusia-Ucrania



Fuente: Banco Mundial (2023), PIB (UMN a precios actuales), https://datos.bancomundial.org/indicador/NY.GDP.MKTP.CN?locations=RU-UA-MX

Una de las lecturas adicionales que se pueden hacer, tomando en cuenta el PIB de ambos países y el gasto militar, es la que se refiere a la disminución del presupuesto en sectores clave para la sociedad y la nación. Como se observa en la tabla 7, el porcentaje del gasto en investigación y desarrollo, mismo que tiene impacto en la educación, pero también en la innovación, ciencia y tecnología, así como en la industria militar, ha disminuido considerablemente. Por lo tanto, la cooperación entre la OTAN y Ucrania es indispensable durante el conflicto, pero también lo será posterior a este para impulsar aquellos sectores que han sido rezagados. Por su parte, Rusia con 1,09% de su PIB en la materia, gasto que le ha permitido continuar con el impulso la industria militar manteniendo estabilidad en ese sector sin retrocesos como lo que presenta Ucrania.

Tabla 7. Gasto en investigación y desarrollo (% del PIB) 2022. Rusia-Ucrania



Fuente: Banco Mundial, Gasto en investigación y desarrollo (% del PIB), https://datos.bancomundial.org/indicador/GB.XPD.RSDV.GD.ZS?end=2021&locations=UA-RU&start=1996

Es así como la OTAN tiene un papel fundamental en el devenir del conflicto. En particular, la cooperación destaca en el área política, económica, militar y social, ya que su presencia en los dominios tradicionales como aire, tierra y mar, y en el ciberespacio como escenario que permite la presencia de amenazas híbridas, se consolida cada vez más con la creación de instrumentos políticos y técnicos que acercan a Ucrania a los miembros de la Alianza.

En consecuencia, una gran cantidad de países han enviado ayuda a Ucrania, el portal *Statista* la divide en ayuda financiera, humanitaria y militar, en la que enlista a los siguientes 40 países: Estados Unidos, instituciones de la UE, Reino Unido, Alemania, Canadá, Polonia, Francia, Países Bajos, Noruega, Japón, Italia, Suecia, Dinamarca, Austria, República Checa, Portugal, Australia, España, Lituania, Finlandia, Letonia, Estonia, Bélgica, Suiza, Bulgaria, Eslovaquia, Grecia, Corea del Sur, Luxemburgo, Irlanda, Taiwán, Eslovenia, Hungría, Croacia, Nueva Zelanda, Rumania, Chipre, China, India, Malta (Statista, 2023), de los cuales 27 pertenecen a la OTAN, solo con excepción de Albania, Islandia, Macedonia del Norte y Montenegro. Además de que la ayuda militar proviene precisamente de miembros de la OTAN: Estados Unidos, Reino Unido, Polonia, Alemania y Canadá.

En la Cumbre de Varsovia de 2016, se implementó el Paquete de Asistencia Integral (PAC), diseñada para dar apoyo a Ucrania con el objetivo de establecer mejoras en el área de seguridad y defensa. A su vez, la OTAN brindó asesoramiento y capacitación a través de programas que generaron el desarrollo de capacidades para el mantenimiento de la seguridad frente a los ciberataques. Los fondos fiduciarios proporcionados por la Alianza se centraron (además del sector médico y militar) en el apoyo en la cuestión de mando, control, comunicaciones y computadoras (C4) para reestructurar y modernizar su infraestructura ligada al ámbito cibernético de índole civil y militar.

En ese mismo año, derivado del uso de ciberataques, desinformación, divulgación de noticias falsas y otras actividades ligadas al ámbito cibernético, se creó la *NATO-Ukraine Platform on Countering Hybrid Warfare,* misma que se estableció como un mecanismo de apoyo para identificarlas (NATO, 2023c). Además, esta plataforma desarrolla proyectos de investigación en la materia y provee a Ucrania de asesoría y capacitación para enfrentar la desinformación. También se establecieron estrategias en conjunto con el *Resilience Advisory Support Team* (RAST) frente a las tácticas híbridas de actores estatales o no estatales que buscan debilitar las instituciones gubernamentales, infraestructura crítica y desestabilizar a la sociedad en el marco del conflicto con Rusia.

Asimismo, en diciembre de 2022, el Consejo de la UE adoptó un paquete legislativo para “proporcionar ayuda financieramente a Ucrania por un importe de 18 000 millones de euros a lo largo del 2023” (Consejo de la UE, 2022), mismos que tendrán un “periodo de gracia”

de diez años. Los préstamos financieros, las sanciones hacia Rusia y los “apoyos militares”, no refleja únicamente el compromiso con esta nación, sino también son parte de los intereses geopolíticos, políticos y militares que los países occidentales tienen en Ucrania.

Este contexto el 29 de junio de 2022 en el marco de la reunión de Madrid la OTAN adoptó un nuevo concepto estratégico que señala que:

> el ciberespacio es un dominio central en la guerra de agresión de Rusia en Ucrania. En las horas inmediatamente anteriores a que las fuerzas rusas cruzaran la frontera el 24 de febrero de 2022, los ciberataques afectaron a los departamentos del gobierno, el ejército y los servicios de emergencia de Ucrania. Este ataque también causó daños más allá de Ucrania afectando turbinas eólicas e interrumpiendo el acceso a Internet de decenas de miles de personas en toda Europa. Desde entonces continúan los ataques de borrado de datos, apuntando al gobierno de Ucrania y a los sectores comerciales y energéticos. (Concepto Estratégico, p. 38)

El reconocimiento del espacio cibernético como un dominio central en este contexto es importante porque el escenario abre la puerta a que, en este y otros conflictos venideros, el ciberespacio sea incluso determinante. La identificación de la OTAN sobre el uso de medios convencionales, cibernéticos e híbridos por parte de la Federación Rusa la coloca como la principal amenaza a la paz y seguridad de la zona euroatlántica, sumado a la posición estratégica de Ucrania para los países occidentales.

Por su parte, en la Cumbre de Vilna de julio de 2023, la OTAN señaló que, “la guerra de agresión de Rusia contra Ucrania ha puesto de relieve hasta qué punto lo cibernético es una característica del conflicto moderno. Estamos contrarrestando las amenazas cibernéticas sustanciales, continuas y crecientes, incluso a nuestros sistemas democráticos y nuestra infraestructura crítica” (NATO, 2023b), de modo que el reconocimiento del ciberespacio como un dominio que hace parte del conflicto implica también cooperación en la materia, por lo que el Fondo de Asistencia Integral provee a Ucrania de fondos fiduciarios y programas para el desarrollo de capacidades en áreas como la ciberdefensa y amenazas híbridas.

El comunicado de la Cumbre dice: “el futuro de Ucrania está en la OTAN” por lo que la asistencia del presidente ucraniano Volodimir Zelensky fue fundamental. Derivado de la importancia de Ucrania para la seguridad euroatlántica, se realizó la reunión inaugural del

Consejo OTAN-Ucrania, reemplazando a la Comisión OTAN-Ucrania (1997-2023), en donde los aliados reafirmaron su compromiso y cooperación para la integración de Ucrania a la Alianza (tema que fue acordado en la Cumbre de Bucarest de 2008) a través del Programa Nacional Anual adaptado que incluye reformas en el sector democrático y de seguridad, eliminando el requisito de crear un Plan de Acción para la Membresía (MAP).

También se acordó el fortalecimiento del Paquete de Asistencia Integral (CAP) para Ucrania (establecido en 2022) que incluiría 500 millones de euros (NATO, 2023b) proporcionados por miembros y aliados, mismo que pasará a un formato plurianual con la finalidad de aumentar las operaciones entre fuerzas ucranianas y de la OTAN en el marco del conflicto con Rusia. Además, a través de programas y asesoramiento personalizado, la Alianza busca fortalecer la capacidad y resiliencia en seguridad y defensa de Ucrania.

En ese mismo sentido, en octubre de 2023, el Parlamento Europeo aprobó mejoras al mecanismo de 50 000 millones de euros de Europa para la recuperación, reconstrucción y modernización de Ucrania a partir de 2024 (Parlamento Europeo, 2023). Por lo que, el paquete de ayuda de las naciones aliadas mantiene a la nación ucraniana con posibilidades para continuar en la batalla frente a Rusia, lo cual genera que el conflicto se mantenga vigente y sin la posibilidad de una tregua a corto plazo.

En ese tenor de ideas, también se encuentra la reciente adhesión de Finlandia a la OTAN, misma que fue solicitada desde mayo de 2022 y que se concretó el 4 de abril de 2023, convirtiéndose así en el miembro 31 de esta organización. Con la integración, se duplican los aproximadamente 1200 km de frontera que suman Polonia, Noruega, Estonia, Letonia y Lituania con la Federación Rusa, aumentando los 1,340 km tras el ingreso de Finlandia, “en lugar de menos OTAN, ha logrado lo contrario. Más OTAN. Y nuestra puerta permanece firmemente abierta” (Comunicado de prensa, 2023), señaló el secretario general Jens Stoltenberg en el comunicado de bienvenida a Finlandia. La vecindad de país nórdico con Rusia y los temores derivados del conflicto con Ucrania, fortalecen a la Alianza Atlántica con una expansión que con la ratificación del Parlamento turco incluirá también a Suecia.

Las motivaciones para que la Alianza Atlántica sumen sus fuerzas en apoyo a Ucrania no se limita a cuestiones geopolíticas, ya que, desde el inicio del conflicto, los ciberataques rusos representan una amenaza a la seguridad internacional.

> Estos representan una gama de objetivos de espionaje estratégico que probablemente estén involucrados en el apoyo directo o indirecto de la defensa de Ucrania, el 49 por ciento de los cuales han sido agencias gubernamentales. Otro 12 por ciento han sido ONG que, por lo general, son centros de estudios que asesoran sobre política exterior o grupos humanitarios que brindan ayuda a la población civil de Ucrania o apoyo a los refugiados" (Smith, 2022)

La imagen 4 se basa en un informe de Microsoft que ubica los principales objetivos internacionales blanco de ciber espionaje, principalmente a gobiernos aliados en donde figuran varios países miembros de la OTAN, lo cual intensifica las operaciones que buscan proteger infraestructura militar, de comunicaciones, energética y gubernamental de la Alianza, de modo que se observa el alcance de las capacidades cibernéticas rusas y sus intereses, mismos que han tenido impacto en miembros de la Alianza y el otras regiones que se han manifestado a favor de Ucrania o tienen alguna relación con la nación invadida.

Imagen 4. Países que han sido blanco de espionaje cibernético ruso desde el inicio del conflicto entre Rusia y Ucrania.

Fuente: Smith, B. (2022), *Defendig Ukraine: Early Lessons from the cyber war*, Microsoft on the issues, https://aka.ms/June22SpecialReport

Derivado de lo anterior, el 20 de diciembre de 2023, Estados Unidos, Canadá, Dinamarca, Estonia, Francia, Alemania, Países Bajos, Polonia, Suecia y Reino Unido formalizaron la creación del *Tallinn Mechanism to Coordinate Civilian Cyber Assistance to Ukraine* (U.S. Department of State, 2023). El Mecanismo, tiene como objetivo la cooperación para el desarrollo de capacidades cibernéticas en la defensa del ciberespacio ucraniano, en el nivel

civil y militar con la colaboración de miembros de la UE y la OTAN, así como del sector privado y actores no gubernamentales.

Por su parte, la *Virtual Cyber Incident Support Capability* (VCISC) de 2023, se suma a las capacidades de la OTAN en el ciberespacio. Por lo que, en coordinación con las capacidades nacionales para contener las amenazas cibernéticas, la OTAN refuerza las estrategias de ciberdefensa y ciberseguridad nacionales en el área de respuesta y resiliencia cibernética. Es así como la cooperación entre la OTAN y Ucrania suma nuevas oportunidades frente a los ciberataques rusos, estatales y no estatales en el marco del conflicto.

Los conflictos armados tienden cada vez más hacia la hibridez y la posibilidad de que los ciberataques tengan un efecto destructivo y determinante es creciente. El enfrentamiento entre Rusia y Ucrania no solo se ciñe a sus fronteras geográficas, ya que las capacidades cibernéticas son fundamentales para la protección de infraestructura que tiene impacto en la cotidianidad de la población, las empresas, organizaciones, del gobierno, instituciones y países vecinos. Los Estados se enfrentan a escenarios geopolíticos en donde la tecnología abre la puerta a que las amenazas aumentan y se fortalezcan, por lo que la ciberseguridad y la ciberdefensa tienen mayor peso e incidencia en la agenda de seguridad y defensa de la comunidad internacional.

3.2.1 Ucrania

En el conflicto entre Rusia y Ucrania no solo la seguridad nacional está en juego, ya que las relaciones políticas, comerciales y sociales se extienden más allá de la región. Aunado a ello, la población sufre las consecuencias de la invasión en donde la infraestructura crítica es blanco de ciberataques, misma que está inmersa gran parte de los aspectos de la sociedad civil, que al ser vulnerada tiene un impacto directo en el quehacer del país.

La combinación rusa de ataques tradicionales con ciberataques ha tenido impacto principalmente en el sector energético y de transporte, el informe de Microsoft, *A year of Russian hybrid warfare in Ukraine*, de 2023, señala que el ciberataque a través del *wiper* IRIDIUM:

> lanzó varias campañas de phishing para obtener acceso a cuentas en bases industriales de defensa y organizaciones del sector energético en Ucrania. Durante este mismo periodo, se implementó una nueva variante del *malware Caddywiper* contra un importante medio de comunicación ucraniano. (*Microsoft Threat Intelligence*, 2023).

Por lo tanto, la digitalización de las infraestructuras críticas requiere de protección especializada para disminuir la vulnerabilidad,[12] de esta manera la cooperación se vuelve fundamental para evitar una interrupción en el suministro de agua, electricidad, así como en los sistemas de control y mando de las fuerzas armadas.

Frente a los posibles ataques cibernéticos a Ucrania, el Servicio Estatal de Comunicaciones Especiales y Protección de la Información tiene un papel esencial para la salvaguarda de la información que podría verse vulnerada y afectar directamente tanto a la población como al gobierno de Volodimir Zelensky.

Tras la anexión de Crimea, en 2014, Ucrania inició un proceso de centralización de los "centros de datos como en cableado submarino, un activo a través del cual viaja el 99% del tráfico mundial de internet a nivel global" (Jorge, 2022), por lo que la concentración de infraestructura digital en la capital del país le permite al gobierno un mayor control y protección en caso de ataques que busquen interrumpir las comunicaciones y la conexión a Internet.

En ese mismo sentido, en 2014 se presentaron gran cantidad de ciberataques hacia Ucrania en donde Rusia es el principal sospechoso; en diciembre de 2015 empresas de distribución de energía se vieron comprometidas, lo que "provocó un corte de energía para más de 230,000 residentes" (*Council on Foreign Relations*, 2015) que duró aproximadamente 6 horas en la capital Kiev, que a su vez, está vinculado a *Sandworm*; en 2016, el sistema de distribución de electricidad e infraestructura financiera fueron atacadas, en donde "la empresa cibernética *iSight Partners* identificó al perpetrador como un grupo

[12] Ejemplo de ello son los ciberataques a la red eléctrica ucraniana en 2014 y 2015. Por su parte, el informe de Microsoft, *A year of Russian hybrid warfare in Ukraine* de 2023, señala que las fuerzas rusas lanzaron numerosos ataques de recopilación de inteligencia contra el sector del transporte ucraniano, además de ciberespionaje contra organizaciones que brindan asistencia militar o humanitaria, asimismo llevaron a cabo múltiples campañas de phishing a organizaciones de ayuda humanitaria, lo cual tiene un impacto directo en la población entorpeciendo las labores humanitarias en favor de la población.

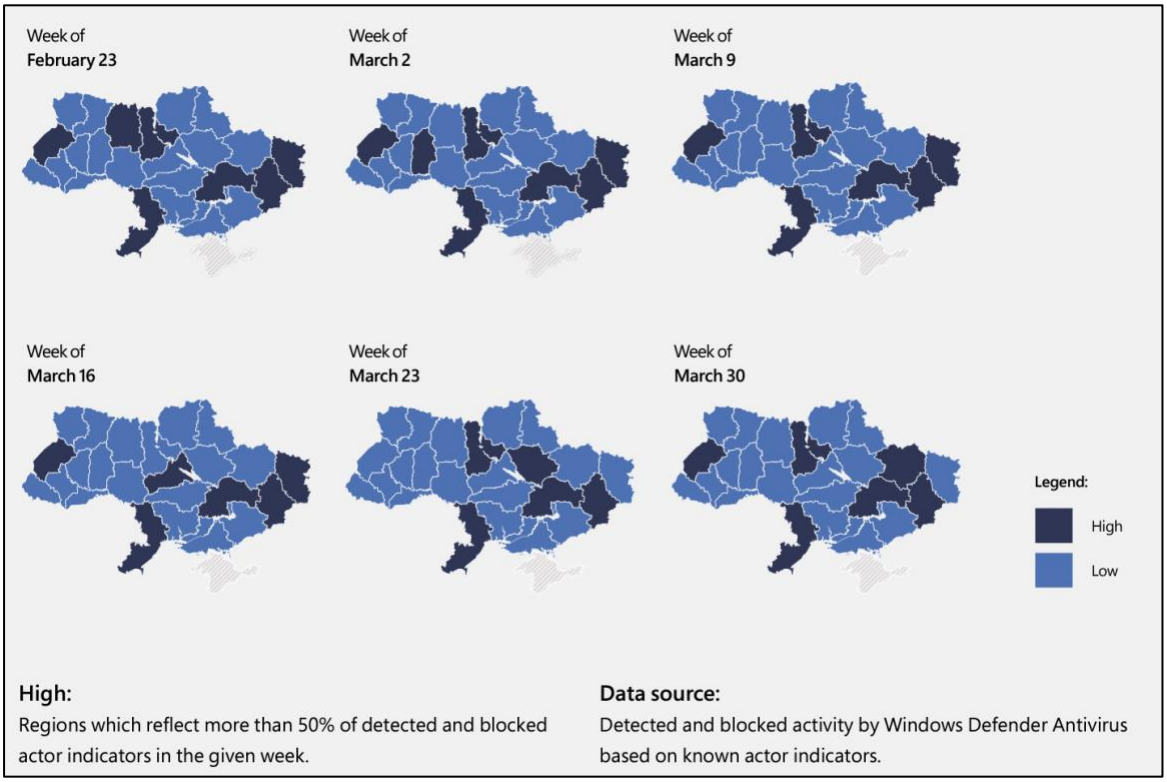
de piratas informáticos ruso conocido como *Sandworm*" al igual que el ataque cibernético de 2015. (Zinets, 2016)

Si bien, el conflicto llegó al punto álgido en febrero de 2022, desde 2021, los ciberataques a infraestructura crítica ucraniana estaban en el mapa. El informe de la Unidad de Seguridad Digital de Microsoft del 27 de abril de 2022 señala que, en 2021, actores rusos como NOBELIUM y DEV-0257 (también conocido como *Ghostwriter*) realizaron campañas de *phishing*. Además, señaló que "sus actividades parecían estar dirigidas a asegurar el acceso persistente para la recopilación de inteligencia estratégica y de campo de batalla o para facilitar futuros ataques destructivos en Ucrania durante un conflicto militar." (Microsoft, 2022, p.5)

La experiencia ucraniana frente a los ciberataques genera necesidades que ponen a prueba su resiliencia ante los embates rusos, bajo esta premisa, el 17 de febrero de 2022, el ministro Mykhailo Fedorov junto con el Parlamento tomaron "medidas para modificar su ley de protección de datos para permitir que los datos del gobierno se trasladen de los servidores locales existentes a la nube pública" (*Microsoft On the Issues*, 2022, p. 5), por lo que esta capacidad para evacuar los datos críticos da cuenta de la existencia de nuevas formas de ejercer la defensa en tiempos de guerra, ya que las comunicaciones y operaciones digitales a través de la red son esenciales.

El informe de Microsoft de 2022, indica "que al menos seis actores estado-nación alineados con Rusia lanzaron más de 237 operaciones contra Ucrania, que estuvieron acompañadas de actividades de espionaje e inteligencia que afectan a otros estados miembros de la OTAN, además de alguna actividad de desinformación" (Microsoft Prensa, 2022), en la imagen 5 se identifican las zonas geográficas con mayor actividad cibernética maliciosa, en el que se observa que va de la mano con los ataques armados en aire y tierra dirigidos a las provincias de Donetsk y Lugansk, es decir, existe una correlación entre el entorno físico y virtual de las operaciones rusas en el terreno ucraniano.

Imagen 5. Actividad cibernética maliciosa semanal en Ucrania (2022)



Fuente: Microsoft Prensa, (2022) *Microsoft publica un informe sobre los destructivos y persistentes ciberataques de Rusia a Ucrania*, Centro de noticias, https://news.microsoft.com/es-es/2022/04/28/microsoft-publica-un-informe-sobre-los-destructivos-y-persistentes-ciberataques-de-rusia-a-ucrania/

Para contrarrestar los embates a redes informáticas ucranianas, “cuando los primeros misiles impactaron en Ucrania, expertos civiles de la industria de ciberseguridad del país se acercaron al gobierno para ofrecer ayuda” (Delcker, 2022), auspiciado por el empresario Yegor Aushev en coordinación con el ministro de Transformación Digital en Ucrania Mykhailo Federov, en febrero de 2022 se creó *IT Army Of Ukraine*, conformado por voluntarios especialistas en tecnologías de la información que buscan atacar servicios de información rusos. Este ejército cibernético “trabaja en colaboración con funcionarios del Ministerio de Defensa de Ucrania para atacar la infraestructura y los sitios web rusos” (*Council on Foreign Relations*, 2023b) que se organizan a través de la aplicación de mensajería *Telegram*.

En la página oficial de *IT Army of Ukraine* es de acceso público, en *itarmy.com.ua* se encuentra disponible información de los requerimientos técnicos para unirse al ejército y ejecutar ataques DDoS contra servidores rusos cuya misión es:

> Ayudar a Ucrania a ganar al paralizar las economías agresoras, bloquear servicios financieros, de infraestructura y gubernamentales vitales, y agotar a los principales contribuyentes. También detenemos la propaganda hostil de los medios y difundimos la verdad sobre la guerra. Queremos que cada residente de los países agresores se sienta y se canse de la agresión de su país. (*It Army of Ukraine,* 2023)

En el informe de junio de 2022 del *Center for Security Studies* (CSS) ETH Zürich, Stefan Soesanto señala que su estructura se basa en:

> 1) Un llamado a la acción global continuo que moviliza a cualquiera que esté dispuesto a participar en ataques DDoS coordinados contra objetivos de infraestructura rusos designados, principalmente civiles.
> 2) Un equipo interno probablemente compuesto por personal de inteligencia y defensa ucraniano que ha estado experimentando y realizando operaciones cibernéticas cada vez más complejas contra objetivos rusos específicos. (Soesanto, 2022, p. 4)

Por su parte, *IT Army of Ukraine* posee legitimidad ante la comunidad internacional, y proviene desde el mismo Estado en colaboración con el sector privado, con miembros civiles y militares. En ese mismo sentido, en el Foro Europeo de Ciberseguridad CYBERSEC 2022 en Katowice, Polonia, el Ejército y el ministro Mykhailo Federov fueron premiados “por su heroica resistencia a la agresión rusa y por la protección de las fronteras digitales del mundo democrático.” (Guachi, 2022) El ejército cibernético que emergió tras la invasión de Rusia a Ucrania posee cualidades que distan de una forma convencional de conflicto, fuera de los márgenes tradicionales de las fuerzas armadas. Sin embargo, en este contexto, la atribución, una de las características más complejas con respecto a los ciberataques, sigue siendo problemática.

3.2.2 Rusia

La intervención militar de Rusia en Ucrania, denominada por ese gobierno como “operación militar especial”, anunciada por el presidente ruso Vladimir Putin, se ha manifestado en distintos frentes, desde las batallas en tierra con un gran número de efectivos militares,

pasando por el espectro político y económico, hasta el espacio cibernético. Se presume que varios años atrás, el gobierno ruso se sirvió de tácticas que combinan ataques convencionales y ciberataques, ejemplo de ello están aquellos perpetrados a Georgia en 2008 y Crimea en 2014, sin embargo, derivado de la naturaleza estos ataques y del ciberespacio, la atribución no se dio de forma oficial.

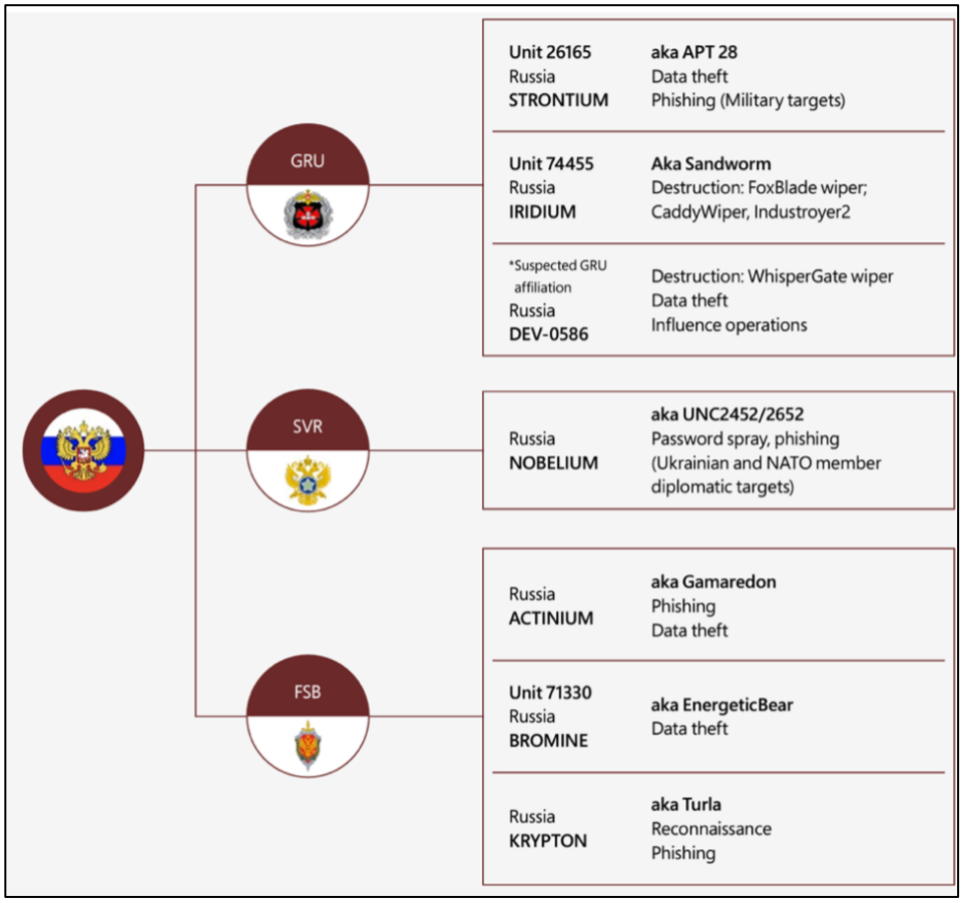
Uno de los grupos rusos a los que se atribuyen gran cantidad de ciberataques es IRIDIUM, también conocido como *Sandworm,* mismo que la NSA acusó en 2020 de un ataque global, también, se le relaciona con ataques a la red eléctrica de Ucrania en 2015 y a los ataques perpetrados a Georgia en 2008. Las acciones de este grupo están atribuidas a la Agencia de Inteligencia Militar (GRU) de Rusia "este actor de amenazas se dirige a los sistemas de control industrial utilizando una herramienta llamada *Black Energy*, asociada con la generación de electricidad y energía con fines de espionaje, denegación de servicio y destrucción de datos." (*Council on Foreign Relations,* 2023)

Derivado de la gran cantidad de ciberataques de *Sandworm* hacia Ucrania y otros países el Centro de Derechos Humanos de UC Berkeley envió una serie de recomendaciones a la Corte Penal internacional (CPI) en la Haya en donde "insta a la CPI a considerar enjuiciamientos por crímenes de guerra de piratas informáticos rusos por sus ataques cibernéticos en Ucrania" (Greenberg, 2022) señalando específicamente a *Sandworm* como principal responsable de los apagones de 2015 y 2016. Esta medida podría ser un precedente en la forma en la que se aborda el tema en las Relaciones Internacionales y otras disciplinas, además abre la posibilidad a la extensión de las leyes que rigen los conflictos y la guerra.

Ahora bien, a pesar de que las capacidades rusas para irrumpir en infraestructura crítica ucraniana han sido probadas de manera intermitente en diversos momentos del conflicto, incluso desde 2014, estas no son utilizadas para definir el curso del conflicto, lo que podría representar:

- Una estrategia rusa para desgastar a Ucrania y sus aliados
- La carencia de un aparato cibernético con la capacidad necesaria para irrumpir e interrumpir el funcionamiento en la infraestructura ucraniana.

Imagen 6. Principales actores rusos responsables de las amenazas cibernéticas a Ucrania y sus principales operaciones.



Fuente: Microsoft Prensa, (2022*) Microsoft publica un informe sobre los destructivos y persistentes ciberataques de Rusia a Ucrania*, Centro de noticias, https://news.microsoft.com/es-es/2022/04/28/microsoft-publica-un-informe-sobre-los-destructivos-y-persistentes-ciberataques-de-rusia-a-ucrania/

El informe especial de Microsoft, *An overview of Russia's cyberattack activity in Ukraine* de abril de 2022, ofrece un esquema que identifica los principales actores de origen estatal ruso que están vinculados a ciberataques perpetrados al país lidereado por Volodimir Zelensky. Por su parte, el presidente ruso, Vladimir Putin ha optado por otras vías de ataque, lo cual atiende a la posibilidad de que la dimensión de los ciberataques podría generar que el conflicto escale afectando no solo a Ucrania, sino a otros países aliados miembros de la OTAN, lo cual, dependiendo de su impacto, traería como consecuencia la invocación del artículo 5° del Tratado de Washington.

El 24 de febrero, un ciberataque dirigido a la red satelital KA-SAT (Group, 2023) afectó a miles de personas ubicadas en Ucrania, mimo que coincide con la fecha de la invasión, de

modo que la estrategia rusa incluyó ataques en tierra y en el ciberespacio, sin embargo, la experiencia de Estonia y Georgia permitió que fueran desplegado un equipo de respuesta rápido para evitar consecuencias que tuvieran gran impacto.

Empero, el alcance de la participación de los miembros se ha visto limitado por el Derecho Internacional, sin embargo, hay una evidente línea difusa cuando de ciberataques se trata. El 20 de mayo de 2022, el presidente ruso se reunió con su Consejo de Seguridad en donde afirmó que:

> el número de ciberataques contra la infraestructura rusa de la información ha crecido durante todos los últimos años, […] pero con el inicio del operativo especial militar en Donbass, en Ucrania, los desafíos en este ámbito se hicieron más agudos y serios, más amplios. De hecho, se ha desatado una agresión verdadera contra Rusia, una guerra en la esfera de la información" (RT, 2022)

A pesar de que varios países de la Alianza Atlántica condenaron la intervención rusa, enviado apoyo financiero, militar y humanitario; las bajas, el territorio ocupado y los enfrentamientos continúan sobre la nación ucraniana. En ese sentido, el conflicto se aborda desde varios frentes por parte de países e instituciones como la OTAN, que va desde sanciones económicas, cierre de fronteras a políticos rusos, hasta aquellas medidas implementadas en ámbito cibernético en donde "*YouTube* bloqueó los medios estatales rusos. *Facebook* también bloqueó las ediciones oficiales rusas de RT y *Sputnik* en la Unión Europea" (Bravo, 2023). Las limitaciones y bloqueos dan cuenta del papel tan relevante que tienen estas plataformas que Rusia y Ucrania utilizan para hacer propaganda de su ideología e intereses en el conflicto.

En el informe *A year of Russian hybrid warfare in Ukraine* de marzo de 2023, Microsoft señala que, desde enero, la actividad de *IRIDIUM* "parece estar preparándose para una nueva campaña destructiva, como su ola de implementaciones de *malware Foxblade* y *Caddywiper* contra el gobierno ucraniano y las organizaciones de medios en los primeros días de la guerra" (*Microsoft Threat Intelligence,* 2023), en donde los principales objetivos hacia los que serían dirigidos los ataques son de índole gubernamental, en donde se verían comprometida infraestructura civil y militar.

En suma, la estrategia rusa frente al conflicto presenta desde un ámbito multidominio, tocando diferentes frentes como el geopolítico, energético, hasta el cibernético. Por su

parte, la comunidad internacional tiene la necesidad de prospectar nuevos escenarios en donde la posibilidad de enfrentarse a una ciberguerra no se descarta. Los esfuerzos por generar mejores capacidades y marcos de acción son cada vez más especializados, ya que el conflicto entre Rusia y Ucrania hace uso del ciberespacio como un campo de batalla con el mismo nivel de importancia que el aire, la tierra, el mar y el espacio.

3.3 Perspectivas frente al conflicto

Desde su creación, la OTAN es la organización más especializada en materia de seguridad y defensa, por las operaciones realiza y por la amplia capacidad de acción que posee. Su papel en la escena internacional es parteaguas para el avance en materia cibernética. La ciberdefensa es uno de los temas en donde la Organización está comprometida, no solo en el ámbito político, sino también en el contexto militar.

La multiplicidad de organismos y capacidades, desde las económicas, políticas y jurídicas hasta las militares y tecnológicas, son determinantes cuando se analiza lo que Nye llama ciberpoder (Nye, 2010). A su vez, el conflicto entre Rusia y Ucrania que escaló en una invasión el 24 de febrero de 2022 da cuenta de la importancia de salvaguardar las redes e infraestructuras informáticas como parte esencial en un escenario de guerra.

En ese mismo sentido, la intervención militar por las fuerzas armadas rusas sobre territorio ucraniano tuvo efectos contraproducentes para la Federación Rusa, ya que esto “llevó a la OTAN a desplegar más soldados y armas en los territorios de sus miembros en Europa del Este y persuadió a Suecia y Finlandia a abandonar su neutralidad y solicitar su ingreso en la OTAN” (Arhirova, 2023). Por lo tanto, la participación de la OTAN en el conflicto persiste con ayuda financiera, militar y humanitaria que los países miembros le brindan a Ucrania continuará, incluido su respaldo a *IT Army Of Ukraine*.

El conflicto entre Rusia y Ucrania da cuenta de que la hibridez es una constante en el devenir de los enfrentamientos futuros, ya que los ataques tradicionales con equipo militar convencional no son suficientes para desarmar a un país. “Los conflictos en el espacio cibernético son asimétricos, multidimensionales, disruptivos y continuos.” (Saavedra y Parraguez, 2018, p. 74) pueden darse incluso en tiempos de paz, llevando a las víctimas a un desgaste constante en el que los daños siempre generan costos elevados, empero,

estos pueden disminuir si se cuenta con un sistema de ciberdefensa y ciberseguridad apropiados, actualizados y eficaces.

La transversalidad de los ciberataques y sus consecuencias en Ucrania genera la necesidad de impulsar al sector público y privado y a la sociedad, ya que el desconocimiento es uno de los factores que genera ventaja con respecto a los efectos de los ataques cibernéticos. Países como “Irán, Israel, China, Rusia, Reino Unido o Estados Unidos poseen capacidades porque han invertido y promovido la agenda de ciberseguridad civil y militar” (Calderín y Jiménez, 2016), lo cual los posiciona como referentes en la materia, a su vez, la OTAN a nivel regional cuenta con una gran cantidad de herramientas para enfrentarse a las amenazas en el ciberespacio, sin embargo, esto genera nuevos conflictos con características que requieren de cooperación y un alto nivel de comunicación, pues los efectos de los ciberataques, como se evidenció con los casos de Estonia, Georgia, Estados Unidos y Ucrania, son imprevisibles.

El impacto de los ciberataques es cada vez más directo en el quehacer y cotidianeidad de las personas, de modo que la cooperación con organizaciones como la OTAN, debe ser complementaria más no sustitutiva, ya que los valores e intereses de los países podrían no tener el mismo orden de prioridad para la Alianza, dejando así en una posición de desventaja a los países que se enfrentan a amenazas no convencionales en su espacio cibernético. La dependencia tecnológica y voluntad de los países con mayor desarrollo tecnológico genera asimetrías en los conflictos; países que poseen infraestructura tecnológica vulnerable y/o insuficiente para contrarrestar los ciberataques, los vuelve un blanco fácil para quienes buscan atentar contra su seguridad en el ciberespacio.

Conclusiones

El ciberespacio, trasciende fronteras, generando nuevas formas de interacción entre los diversos actores que confluyen en este. Las atribuciones del espacio cibernético como dominio operativo lo diferencian de otros, como la tierra, el aire, el mar y el espacio, ya que fue creado de forma artificial, por lo que día con día sus características son innovadoras y requieren de perspectivas amplías para abordarlo desde el sector público y privado. De este modo, los debates entorno al ciberespacio y su integración a las agendas nacionales e internacional, está en constante evolución, en donde el desarrollo de capacidades de ciberdefensa y ciberseguridad necesitan de la sinergia entre el ámbito público y privado, así como de la esfera nacional e internacional.

Como se señala en el primer capítulo, las definiciones en torno a la materia son importantes, ya que estas restringen o permiten desarrollar herramientas que aborden lo que este dominio necesita, ya que lo que ocurre en el ciberespacio tiene impacto virtual y material. La multidimensionalidad de la ciberseguridad y la ciberdefensa “impacta los diversos niveles de la seguridad (personal, pública, nacional e internacional); pone en el centro del debate la tensión entre soberanía y transnacionalización, así como las dinámicas entre la cooperación” (Lozano y Rodríguez, p. 84), ejemplo de lo anterior son los eventos como el de Estonia en 2007 y los ciberataques en el marco del conflicto entre Rusia y Ucrania, que demuestran que los ataques cibernéticos requieren una respuesta en varios sentidos, desde el legal y jurisdiccional, hasta el militar y gubernamental.

Por otro lado, la carencia de un marco jurídico que facilite atribución de los ciberataques, genera dificultades para capturar a los atacantes debido a la falta de certidumbre legal o voluntad de los gobiernos de donde podría provenir el ciberataque, ya que los ataques no son perpetrados solamente por usuarios o grupos organizados de forma aislada, sino que en varios casos existe la sospecha que los atacantes están aliados con gobiernos que los proveen de información y recursos económicos, como en el caso de los ciberataques Estonia en 2007, aunque no fue comprobado, “se presume que pudo contar con la participación del gobierno ruso debido a las circunstancias que rodearon el evento” (IEEE, 2010, p. 178).

La cooperación que se necesita para lograr que la ciberseguridad y ciberdefensa estén garantizadas, requiere de una amplia colaboración en diversos temas, además de la necesidad de compartir información, la comunicación entre instituciones, gobiernos y empresas es esencial. Por consiguiente, el compromiso y voluntad política son elementos que van de la mano de la celebración de acuerdos o creación de órganos encargados de garantizar la seguridad en el ciberespacio. Sin embargo, dicha cooperación se vuelve compleja cuando se habla de la soberanía nacional de las entidades involucradas en el ciberespacio, que no conoce de fronteras pero que para algunas naciones puede verse como una debilidad, de modo que ello complica la atribución a los responsables de los ataques.

El capítulo dos, destaca que existe una correlación entre los artículos 4°, 5° y 6° del Tratado de Washington y que a pesar de que no contempla explícitamente la posibilidad de incluir a los ciberataques como elementos que pueden ser objeto de defensa colectiva, es probable que se integren, pues el tratado no es restrictivo frente a los cambios, evoluciones y transformaciones en el devenir de los años. Esa característica fortalece a la Alianza Atlántica y a sus miembros, puesto que esta apertura le permite a la Organización responder a los retos y desafíos del contexto internacional. A raíz de la evolución constante de las amenazas, el ciberespacio requiere de estrategias y herramientas que nutran las acciones de la OTAN en sinergia con los esfuerzos de los países miembros para poder enfrentarlas si llegaran a escalar al nivel de un ataque armado que traería como consecuencia la invocación del artículo 5°.

A través de la incorporación al análisis de la TCSR, se logra identificar a la ciberseguridad y ciberdefensa como parte de la seguridad nacional y por ende internacional. Ya que los miembros de la OTAN identifican los ataques cibernéticos como amenazas que pueden desestabilizar a una sociedad y por lo tanto al Estado. De manera que, a partir de 2016, cuando la Alianza reconoció al ciberespacio como dominio de operaciones militares, reforzó su integración a la agenda de seguridad y defensa, por lo que los miembros y la Organización en conjunto, incorporaron políticas y estrategias en favor de la seguridad cibernética, por lo que el proceso de integración se consolida, sobre todo en un contexto en el que las amenazas híbridas son parte un conflicto vigente entre Rusia y Ucrania.

Ahora bien, los ciberataques representan una amenaza a la seguridad nacional de los Estados, sin embargo, como en el caso de Estonia, también son una oportunidad para generar nuevos y mejores instrumentos que respondan a estas amenazas, ya que, a partir de este evento, la OTAN y sus miembros trabajaron en la consolidación y creación de capacidades para enfrentarse a las amenazas cibernéticas.

La forma en la que la OTAN se enfrenta a las crecientes ciberamenazas es parteaguas para la comunidad internacional, porque tiene un papel determinante en la materia por su avance en la integración del ciberespacio como ámbito de operaciones militares, por la creación de estructuras en favor de la ciberdefensa y la ciberseguridad, y por el reconocimiento de amenazas en el entorno cibernético, de tal forma incide a nivel regional e internacional.

Por su parte, en el capítulo tres, se abordó la integración del espacio cibernético a la OTAN como un ámbito de operaciones en el que los ciberataques son parte de los conflictos internacionales. La identificación de las amenazas en el ciberespacio y su inclusión en la agenda de seguridad de la OTAN le permite continúe vigente, sumado a la posibilidad de crear instrumentos que sumen a su estrategia de seguridad y defensa. Además de la ayuda financiera, militar y humanitaria que los miembros de la Alianza proveen a Ucrania, el reconocimiento internacional del ejército cibernético *IT Army of Ukraine*, sienta precedente, a pesar de que se encuentran fuera de los márgenes del Derecho Internacional que rige los conflictos.

Asimismo, se identificaron diversos esfuerzos de cooperación referentes al ciberespacio en la relación OTAN-Ucrania, lo que se suma como referente en la comprobación de la hipótesis de esta investigación. De manera que las respuestas de la OTAN en el marco del conflicto se han dado en el área política y técnica, tales como:

- La Representación de la OTAN en Ucrania
- El Paquete de Asistencia Integral
- *NATO-Ukraine Platform on Countering Hybrid Warfare*
- *Resilience Advisory Support Team*
- El Programa Nacional Anual
- *Tallinn Mechanism to Coordinate Civilian Cyber Assistance to Ukraine*
- *Virtual Cyber Incident Support Capability*
- El Consejo OTAN-Ucrania

De modo que los instrumentos citados dan cuenta del papel que tiene la OTAN en el conflicto dado que este tiene impacto en la seguridad regional. Además, a pesar de la confrontación bélica, la Alianza se ha fortalecido, consolidando el proceso de adhesión de Finlandia y avanzando con la aprobación unánime de la integración de Suecia, sumando así hasta ahora 31 países miembros.

En suma, a lo largo de tres capítulos, la hipótesis de investigación “la OTAN considera al ciberespacio como un dominio de operaciones militares y su defensa está integrada en su concepto estratégico de 2022. Esto coloca a la organización como referente para la comunidad internacional en cuanto al desarrollo de capacidades para afrontar los desafíos y amenazas en esta área al tiempo que abre el debate sobre los alcances de la defensa colectiva en este dominio” se comprueba. Si bien, el Concepto Estratégico de 2010 ya contemplaba los ataques cibernéticos dentro de las amenazas a la seguridad, el Concepto Estratégico de 2022, reconoce al ciberespacio como un escenario que al ser propenso a ciberataques deber contar con las capacidades suficientes para enfrentarse al uso malintencionado de las tecnologías.

Aunado a lo anterior, los Informes Anuales de 2020 y 2021, allanaron el camino hacia el reconocimiento del ciberespacio como un dominio en el que “las operaciones híbridas contra los aliados podrían alcanzar el nivel de ataque armado y llevar al Consejo del Atlántico Norte a invocar el Artículo 5 del Tratado del Atlántico Norte” (NATO, 2022b), por lo que los alcances de la defensa colectiva de la OTAN podrían aplicarse a este, de manera que la Conferencia anual de Ciberdefensa, celebrada por primera vez en noviembre de 2023 no solo confirma la posición de la Alianza como referente en la materia, sino que también consolida sus intereses políticos y militares en el entorno cibernético en la región.

Con la firma del Acuerdo Técnico de Adhesión de Ucrania al Centro de Excelencia de Ciberdefensa Cooperativa (CCDCOE) de la OTAN (SSSCIPU, 2023) en enero de 2023, fortalece los vínculos entre los miembros y aliados. Además, esta alianza, amplía el conocimiento de la Organización frente a los ciberataques, ya que la experiencia ucraniana ante los embates rusos en el ciberespacio suma nuevas perspectivas para los ejercicios cibernéticos del Centro, en donde el conflicto ha demostrado la sofisticación de los ataques cibernéticos, mismos que la OTAN está tomando en cuenta para el desarrollo de ejercicios y capacidades que respondan al contexto.

No cabe duda de lo importante que es desarrollar estrategias de ciberdefensa lo que entre otros elementos incluye la cooperación a través del intercambio de información de vulnerabilidades, alertas, amenazas y ataques. La mejora de las capacidades de contrainteligencia, la seguridad de productos y tecnologías, la concientización y formación de ciudadanos y servidores públicos en ciberseguridad, dan mayor certeza y efectividad a la hora de responder para que los daños sean menores.

A su vez, las brechas materiales se han trasladado al espacio digital, ante ese panorama la creación de instrumentos en favor de la cooperación, innovación, desarrollo tecnológico y de cibercapacidades, en alianza con el sector público y privado se requiere para enfrentar los riesgos y amenazas. La articulación de normas que sumen a la precisión conceptual de los ciberdelitos también es importante para delimitar y definir el alcance de los instrumentos en el ciberespacio y evitar su uso indiscriminado en favor de intereses geopolíticos, económicos y/o militares.

Establecer principios comunes de actuación, líneas de acción y, por consiguiente, la creación de estructuras de decisión y coordinación y canales adecuados para los flujos de información respondan a las amenazas en el ciberespacio con el menor número de consecuencias es un proceso que está en desarrollo. Los esfuerzos requieren de cooperación, compromiso profundo y voluntad política para lograr avanzar de forma concreta y eficaz y favorecer así el mantenimiento de la paz y seguridad internacionales.

Finalmente, los intereses políticos y militares de la OTAN se encaminan hacia la búsqueda de una respuesta rápida y eficaz para la protección del ciberespacio mediante: la capacitación de personal para responder ante los ataques, la creación de organismos especializados en ciberseguridad y el impulso de acuerdos de cooperación entre las entidades públicas y gubernamentales favoreciendo la cooperación en favor de la ciberseguridad y la ciberdefensa; así como el resguardo de sus redes informáticas desarrollando constantemente capacidades estratégicas e instrumentos legales que favorezcan el ámbito de aplicación.

Referencias

ACNUR (2023) Emergencia en Ucrania, https://www.acnur.org/emergencias/emergencia-en-ucrania

Agency, N. (2023). TRIDENT JAGUAR 2018 tests NATO's readiness, https://www.ncia.nato.int/about-us/newsroom/trident-jaguar-2018-tests-natos-readiness.html

Air Force (22 de octubre de 2022) AFTC kicks off new digital engineering, https://www.af.mil/News/Article-Display/Article/3175078/aftc-kicks-off-new-digital-engineering-efforts/

Ambrós, Isidre (2011) China- anuncia la creación de un ejército azul para la ciberguerra. Corresponsal en Pekín, Portal de noticias, Off News, http://offnews.info/verArticulo.php?contenidoID=31344

Arroyo Belmonte, Rocío. (2021-presente) ¿La geocultura de la digitalización? Bróker Internacional [Podcast]. Spotify. https://open.spotify.com/episode/00x9o2J1YfhHL99ImzZqio

Asamblea General (2010) Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones el contexto de la seguridad internacional A/65/201. [Archivo PDF] https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/65/201&Lang=S

_____ (2011) Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional A/RES/66/24. [Archivo PDF] https://daccess-ods.un.org/access.nsf/Get?OpenAgent&DS=A/65/201&Lang=S

Awan, Imran (2017) Cyber-Extremism: the power of social media, Springer Link, https://doi.org/10.1007/s12115-017-0114-0

Banco Mundial (2020) Acceso a la electricidad (% de población) – United States https://datos.bancomundial.org/indicator/EG.ELC.ACCS.ZS?end=2020&locations=US&start=2020&view=map

_____ (2022) Personas que usan Internet (% de la población) Estonia, https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?locations=EE

_____ (2023) Gasto militar PIB – Russian Federation, 1 de abril de 2023 https://datos.bancomundial.org/indicator/MS.MIL.XPND.GD.ZS?locations=RU

BBC New Mundo (2021) EE. UU. declara estado de emergencia tras un ciberataque a la mayor red de oleoductos del país, https://www.bbc.com/mundo/noticias-internacional-57033536

Borbúa, V., Herrera, R., & Reyes, R. (2017) Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. URVIO, *Revista*

Latinoamericana De Estudios De Seguridad, 31-45, https://www.redalyc.org/journal/5526/552656641013/html/#redalyc_552656641013_ref41

Borja, Adsuara (2019) Juegos de guerra digitales, Cuadernos de Pensamiento Político, No. 63 FAES, Fundación para el Análisis y los Estudios Sociales, https://www.jstor.org/stable/10.2307/26741139

Bravo, Jorge (2023) Un año después: Rusia-Ucrania y la tecnología, El Economista, https://www.eleconomista.com.mx/opinion/Un-ano-despues-Rusia-Ucrania-y-la-tecnologia-20230317-0009.html

Burt, Tom (2022) The hybrid war in Ukraine, Microsoft, 27 de abril de 2022., https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

Burtseva, Larisa, Valentyn Tyrsa, y Flores R., Brenda L. (2015) Norbert Wiener: padre de la cibernética. Revista UABC. 4 (54), 44-53. https://issuu.com/revistauabc/docs/ru54

Buzan, Barry Ole Wæver & Japp de Wilde, Regions and Powers. The structure of International Security, Cambridge Studies in International Relations, Londres, 2003

Calderín F. Juanfer y Jiménez Juanfer y María, María (7 de julio de 2016), Estados Unidos, Rusia o China presentan ventajas para el cibercrimen, Observatorio Internacional de Estudios de Terrorismo. Recuperado el 22 de noviembre de 2021 de https://observatorioterrorismo.com/entrevistas/estados-unidos-rusia-o-china-presentan-ventajas-para-el-cibercrimen/

Caro Bejarano, María José (2012) Ciberdefensa. Equipos de respuesta inmediata de la OTAN, Documento de opinión, Instituto Español de Estudios Estratégicos, https://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI16-2012_NatoRapidReactionTeam_MJCaro.pdf

Check Point Software Technologies (2023) Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most, https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

Chi, M. (2017). Big data in national security. Australian Strategic Policy Institute. http://www.jstor.org/stable/resrep04118

CISA, Cybersecurity & Infrastructure Security Agency (2023) Critical Infrastructure Sectors, https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors

Cisco (10 de abril de 2022) ¿Qué es la ciberseguridad?, https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

Council on Foreign Relations, (2015) Compromise of a power grid in eastern Ukraine, diciembre de 2015, https://www.cfr.org/cyber-operations/compromise-power-grid-eastern-ukraine

_____ (2023) Connect the Dots on State-Sponsored Cyber Incidents – Sandworm, https://www.cfr.org/cyber-operations/sandworm

_____ b (2023) Connect the Dots on State-Sponsored Cyber Incidents - Ukrainian IT Army, https://www.cfr.org/cyber-operations/ukrainian-it-army

Code of Conduct Distributed in the United Nations – What's New?, https://ccdcoe.org/incyder-articles/an-updated-draft-of-the-code-of-conduct-distributed-in-the-united-nations-whats-new/

Comisión Europea, (17 de septiembre de 2021) La protección de datos en la Unión Europea https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_es

Consejo Europeo-Consejo de la Unión Europea (2021) Ciberseguridad: el Consejo adopta unas Conclusiones sobre la Estrategia de Ciberseguridad de la UE, https://www.consilium.europa.eu/es/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy

_____ (2022) Ciberseguridad: cómo combate la UE las amenazas cibernéticas. https://www.consilium.europa.eu/es/policies/cybersecurity

Consejo de la Unión Europea (2022b) Consejo adopta una ayuda de 18 000 millones de euros a Ucrania, https://www.consilium.europa.eu/es/press/press-releases/2022/12/10/council-adopts-18-billion-assistance-to-ukraine/

Cooperative Cyber Defence Centre of Excellence (14 de abril de 2022) Exercises. https://ccdcoe.org/exercises/

_____ (5 de marzo de 2022) The Tallinn Manual. https://ccdcoe.org/research/tallinn-manual/

DataReportal (21 de octubre de 2022) Digital Around the World. https://datareportal.com/global-digital-overview

Deutsche Welle (2014) Crimea: el 95,5% de sufragantes votó a favor de anexión a Rusia, https://www.dw.com/es/crimea-el-955-de-sufragantes-vot%C3%B3-a-favor-de-anexi%C3%B3n-a-rusia/a-17500362

Del Arenal, C. (1989). La teoría de las relaciones internacionales hoy: debates y paradigmas. Estudios Internacionales, 22(86), 153–182, http://www.jstor.org/stable/41391301

Delcker, Janosch, (2022) Inside Ukraine's cyber guerrilla army, Deutsche Welle, https://www.dw.com/en/ukraines-it-army-who-are-the-cyber-guerrillas-hacking-russia/a-61247527

Departament of Defense, (3 de marzo de 2022) National Military Strategy for Cyberspace Operations (NMS-CO) 2006. [Archivo PDF] https://www.hsdl.org/?view&did=35693

Departamento de Seguridad Nacional. (1º de noviembre de 2021) La OTAN y la UE aumentan la cooperación en ciberseguridad. Gabinete de la presidencia del gobierno. https://www.dsn.gob.es/es/actualidad/sala-prensa/otan-ue-aumentan-cooperaci%C3%B3n-ciberseguridad

Diario Oficial de la Unión Europea (2019) Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo. [Archivo PDF] https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=PLe

Duster, Chandelis, (7 de junio de 2022) Secretaría de Energía dice que los adversarios tienen la capacidad de cerrar la red eléctrica de Estados Unidos https://cnnespanol.cnn.com/2021/06/07/secretaria-energia-granholm-ciberataques-trax/

Energy.gov (17 de enero de 2023) *Cybersecurity*, https://www.energy.gov/cybersecurity

Espona, José Rafael (2018) Guerra híbrida y capacidades estratégicas de la OTAN: aportaciones de Lituania, Letonia y Estonia. Documento Opinión, Instituto Español de Estudios Estratégicos. [Archivo PDF] https://www.ieee.es/Galerias/fichero/docs_opinion/2018/DIEEEO55-2018_GuerraHibrida_OTAN_Lit-Est-Let_RafaelJEspona.pdf

European Union Agency for Cybersecurity (2022) Acerca de la ENISA- Agencia de la Unión Europea para la Ciberseguridad. https://www.enisa.europa.eu/about-enisa/about/es

Exercise Trident Juncture 2018 (2023) Trident Juncture 2018, https://www.nato.int/cps/en/natohq/157833.htm

Fojón, Enrique (3 de febrero de 2014) La OTAN y la ciberdefensa, Real Instituto Elcano, https://www.realinstitutoelcano.org/la-otan-y-la-ciberdefensa/

_____ & Sanz Villalva Ángel F. (2010) Ciberseguridad en España, una propuesta para su gestión, Real Instituto Elcano, https://www.realinstitutoelcano.org/analisis/ciberseguridad-en-espana-una-propuesta-para-su-gestion-ari/

France diplomacy, Ministère de l'Europe et des Affaires étrangères, (5 de enero de 2021) https://www.diplomatie.gouv.fr/en/french-foreign-policy/united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism/article/paris-call-for-trust-and-security-in-cyberspace

Fuente Cobo, Ignacio (2022) La OTAN y el ciberespacio: un nuevo dominio para las operaciones, Revista Ejército, N° 972, https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/LaOTAN_ciberespacio.pdf

Gibney, Elizabeth (2022) Where is Russia’s cyberwar? Researchers decipher its strategy, Nature. 17 de marzo de 2022. Disponible en: https://www.nature.com/articles/d41586-022-00753-9

Greenberg, Andy (2022). The Case for War Crimes Charges Against Russia's Sandworm Hackers, https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/

Group, G. (2023), Viasat explica el ciberataque del cual fue víctima en Europa al iniciarse la guerra en Ucrania, https://www.satelital-movil.com/2022/04/viasat-explica-el-ciberataque-del-cual.html

Guachi, M. (2022), Ucrania recibió 2 premios CYBERSEC, Root Nation, https://root-nation.com/es/noticias-es/es-ucrania-premios-cybersec/

Gutiérrez, Angélica (2012) Como el terrorismo islámico usa internet, Quadernos de criminología: revista de criminología y ciencias forenses, https://dialnet.unirioja.es/descarga/articulo/4111887.pdf

Hanssen L. y H. Nissenbaum (2009) Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly.

Henderson, Christian (2015) The United Nations and the regulation of cyber-security, Edward Elgar Publishing.

Hernández, Jaime J. (2015) Ciberguerra, las batallas del siglo XXI, https://www.eluniversal.com.mx/articulo/mundo/2015/08/16/ciberguerra-las-batallas-del-siglo-xxi

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, http://www.jstor.org/stable/26463926

Instituto Español de Estudios Estratégicos (2011) Cuadernos de estrategia 149. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio. https://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2011/Cuaderno_149.html

_____ (2012) Documento informativo. Ciberdefensa equipos de respuesta inmediata de la OTAN. https://www.ieee.es/publicaciones-new/documentos-informativos/2012/DIEEEI16-2012.html

International Telecommunication Union (16 de abril de 2022) Global Cybersecurity Agenda. https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

_____ (2020) Global Cybersecurity Index. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

INTERPOL (2020) Panorama mundial de la ciberamenaza relacionada con la Covid-19, https://www.interpol.int/es/content/download/15217/file/20COM0312-Cyberthreats-Campain_ProjectSheet%20-%20SP%20-2020-05.pdf

_____ (2020b) Ciberdelincuencia: efectos de la Covid-19, https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf?inLanguage=esl-ES

IT Army of Ukraine (2023) Home, https://itarmy.com.ua/?lang=en

Junta Interamericana de Defensa (2020) Guía de ciberdefensa. Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar, Gobierno de Canadá, https://www.jid.org/wp-content/uploads/2022/01/Ciberdefensa10.pdf

Jorge, Ricart Raquel (2022) Ucrania en busca de refugio digital, Real Instituto Elcano, Royal Institute, 4 de marzo de 2022 https://www.realinstitutoelcano.org/comentarios/ucrania-en-busca-de-refugio-digital/

Kaspersky (10 de abril de 2022) ¿Qué es la ciberseguridad? https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kemp, Simon (2021) 6 in 10 people around the world now use the internet. Data reportal. 14 de abril de 2022. https://datareportal.com/reports/6-in-10-people-around-the-world-now-use-the-internet

_____ (2023) Digital 2023: The United States of America, 9 de febrero de 2023, https://datareportal.com/reports/digital-2023-united-states-of-america

Kurczyn P., Sánchez A. y Mendizábal G. (2019) Industria 4.0 trabajo y seguridad social (núm. 872), Instituto de Investigaciones Jurídicas, https://archivos.juridicas.unam.mx/www/bjv/libros/12/5645/20.pdf

Lee, Dave (2014) La confrontación cibernética entre Rusia y Ucrania, BBC News Mundo, https://www.bbc.com/mundo/noticias/2014/03/140306_tecnologia_guerra_cibernetica_rusia_ucrania_aa

Lorents Peter & Ottis Rain (2010) Cyberspace: definition and implications. Proceedings of the 5th International Conference on Information Warfare and Security, https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/

López de Anda, María Magdalena (2011). Epistemologías del ciberespacio, Virtualis, No. 4, Julio-diciembre, 67-92, https://www.revistavirtualis.mx/index.php/virtualis/article/view/44

Lozano Vázquez A. y Rodríguez Sumano A. (2020) Seguridad y asuntos internacionales, Anthropos, diciembre 258, 76-88, https://www.academia.edu/51435168/Revista_Anthropos_258_Versi%C3%B3n_Digital_Lozano_Rodr%C3%ADguez_Eds_Enero_Marzo_2021_2_1_

Mando Conjunto del ciberespacio (MCCE) – EMAD, (2022) https://emad.defensa.gob.es/unidades/mcce/

Marrone, A. y Sabatino, E. (2021). Cyber Defence in NATO Countries: Comparing Models. Istituto Affari Internazionali (IAI). http://www.jstor.org/stable/resrep28807

Martínez, S. (2022). La OTAN aumentará los efectivos de la fuerza de respuesta rápida a 300.000, https://www.elperiodico.com/es/internacional/20220627/otan-aumentara-efectivos-fuerza-respuesta-stoltenberg-13946722

McKenna Katelyn Y. A. y Bargh, John A. (1998) Coming out in the age of the Internet: Identity "demarginalization" through virtual group participation. Journal of Personality Social Psychology. Vol. 75(3), 681-694, http://doi.apa.org/getdoi.cfm?doi=10.1037/0022-3514.75.3.681

Mcguinness, Demien (2017) Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país BBC News Mundo, https://www.bbc.com/mundo/noticias-39800133

Mele, Stefano (2019) La Strategia Della Nato In Ambito Cyber - Europa Atlantica. Europa Atlantica. https://europaatlantica.it/firewall/2019/06/la-strategia-della-nato-in-ambito-cyber/

Microsoft (11 de abril de 2022) ¿Qué es la ciberseguridad? https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390

Microsoft Prensa (2022), Microsoft publica un informe sobre los destructivos y persistentes ciberataques de Rusia a Ucrania, Centro de noticias, https://news.microsoft.com/es-es/2022/04/28/microsoft-publica-un-informe-sobre-los-destructivos-y-persistentes-ciberataques-de-rusia-a-ucrania/

Microsoft Threat Intelligence, (2023) A year of Russian hybrid warfare in Ukraine, 15 de marzo de 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW10mGC

Ministerio de Defensa del Reino de España (2011) Nuevo Concepto de Ciberdefensa de la OTAN, Documento Informativo del IEEE 09/2011 [Archivo PDF] https://www.ieee.es/Galerias/fichero/docs_informativos/2011/DIEEEI09-2011ConceptoCiberdefensaOTAN.pdf

_____ (2018) Concepto de ciberdefensa, resumen ejecutivo, Centro Conjunto de Desarrollo de Conceptos (CESEDEN), https://emad.defensa.gob.es/Galerias/CCDC/files/Concepto_CIBERDEFENSA_Resumen_Ejecutivo.pdf

_____ (2022) Ciberamenazas y tendencias Edición 2022, Gobierno de España, https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-ciberamenazas-y-tendencias-edicion-2022-1/file.html

Morán Blanco, Sagrario (2017) La ciberseguridad y el uso de las tecnologías de la información y la comunicación (tic) por el terrorismo. Revista Española de Derecho Internacional. Vol. 69, No. 2, Julio-diciembre, pp. 195-222. https://www.jstor.org/stable/10.2307/26187882

Naciones Unidas (12 de abril de 2022) Los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional.

https://www.un.org/disarmament/es/los-avances-en-la-informatizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/

National Cyber Security Centre (2018) Russian military 'almost certainly' responsible for destructive 2017 cyber attack, https://www.ncsc.gov.uk/news/russian-military-almost-certainly-responsible-destructive-2017-cyber-attack

NATO's ACT (2022) Exercise Cyber Coalition 2022 Concludes in Estonia, https://act.nato.int/articles/exercise-cyber-coalition-2022-concludes-estonia

NATO Modelling & Simulation Centre of Excellence, 2022), *Just finished the CWIX 2022, NATO exercise at the NATO Modelling Simulation Centre of Excellence*, https://www.mscoe.org/just-finished-the-cwix-2022-nato-exercise-at-the-nato-modelling-simulation-centre-of-excellence

NCI Agency (2023) NCI Agency particpates in NATO's largest and most complex computer-based excercise, https://www.ncia.nato.int/about-us/newsroom/nci-agency-participates-in-natos-largest-and-most-complex-computerbased-exercise.html

News, R., & News, R. (2022). La geopolítica detrás del Concepto Estratégico de la OTAN, https://www.lisanews.org/geopolitica/la-geopolitica-detras-del-concepto-estrategico-de-la-otan/

Nordstern (8 de octubre de 2022) Infografía: puntos críticos de Ciberseguridad 2020, https://www.nordsterntech.com/post/puntos-cr%C3%ADticos-de-ciberseguridad-en-2020

North Atlantic Treaty Organization (2012) Strategic Concept 2010. 6 de marzo de 2022. https://www.nato.int/cps/en/natohq/topics_82705.htm

North Atlantic Treaty Organization (2016) Cyber Defense Pledge. 6 de marzo de 2022. https://www.nato.int/cps/en/natohq/official_texts_133177.htm

North Atlantic Treaty Organization (2018) Tratado del Atlántico Norte. 13 de abril de 2022 https://www.nato.int/cps/en/natohq/official_texts_17120.htm?selectedLocale=es

North Atlantic Treaty Organization (2019) Nato will defend itself. 6 de marzo de 2022. https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

_____ (2019b) Remarks by NATO Secretary General Jens Stoltenberg at the Cyber Defence Pledge Conference, London. 5 de marzo de 2022. https://www.nato.int/cps/en/natohq/opinions_166039.htm

North Atlantic Treaty Organization (2020) NATO readies for cyber threath, 16 de noviembre, 25 de marzo de 2023, https://www.nato.int/cps/en/natohq/news_179481.htm?selectedLocale=en

_____ (2020b) The Secretary's General Annual Report 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/sgar20-en.pdf#page=25

North Atlantic Treaty Organization (2021) Brussels Summit Communiqué. 14 de abril de 2022. https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en

_____ (2021b, 19 de julio) Statement, [Comunicado de prensa], 25 de marzo de 2023, https://www.nato.int/cps/en/natohq/news_185863.htm

_____ (2021c) The Secretary's General Annual Report 2021, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/3/pdf/sgar21-en.pdf

North Atlantic Treaty Organization (2022) NATO 2022, Strategic Concept, https://www.nato.int/cps/en/natohq/topics_210907.htm

_____ (2022b) NATO 2022, Strategic Concepts, https://www.nato.int/cps/en/natohq/topics_56626.htm

_____ (2022c) The Secretary's General Annual Report 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/sgar22-en.pdf

North Atlantic Treaty Organization (2023, 4 de abril) Press Statement, [Comunicado de prensa], https://www.nato.int/cps/en/natohq/opinions_213464.htm

_____ (2023b, 11 julio) Vilnius Summit Communiqué, https://www.nato.int/cps/en/natohq/official_texts_217320.htm

_____ (2023c, 28 de julio) Relations with Ukraine, https://www.nato.int/cps/en/natohq/topics_37750.htm

_____ (2023d, 9 de noviembre), Secretary General: Through NATO, we can build a secure cyberspace for all, https://www.nato.int/cps/en/natohq/news_219850.htm?selectedLocale=en

_____ (2023e, 12 de diciembre) Exercise Crossed Swords Tests Allied Cyber Operations, https://www.act.nato.int/article/exercise-crossed-swords-tests-allied-cyber-operations/

Nye, Jr. Joseph (2010) Cyber Power. Defense Technical Information Center https://apps.dtic.mil/sti/citations/ADA522626

Office of Cybersecurity, Energy Security, and Emergency Responce, (2023) *Colonial Pipeline Cyber Incident*, https://www.energy.gov/ceser/colonial-pipeline-cyber-incident

Office of Counter-Terrorism (11 de abril de 2022) Cybersecurity. https://www.un.org/counterterrorism/cybersecurity

Office for Disarmament Affairs (12 de abril de 2022) About us, https://www.un.org/disarmament/about/

Ortega, Morán Arturo (2005) *Ciberespacio,* Centro Virtual Cervantes, https://cvc.cervantes.es/el_rinconete/anteriores/febrero_05/14022005_01.htm

Ostorm Elinor (2002) Reformulating the commons, *Ambiente & Sociedade*, Número 10, 5-25 https://doi.org/10.1590/S1414-753X2002000100002

Paris Call (5 de enero de 2022) The supporters, https://pariscall.international/en/supporters

Parlamento Europeo (2023) Una solución a largo plazo para las necesidades de financiación de Ucrania, https://www.europarl.europa.eu/news/es/press-room/20231013IPR07125/una-solucion-a-largo-plazo-para-las-necesidades-de-financiacion-de-ucrania

Perry B. John. (1996). Declaración de independencia del Ciberespacio [Archivo PDF] http://www.uhu.es/ramon.correa/nn_tt_edusocial/documentos/docs/declaracion_independencia.pdf

Poveda Criado, Miguel Ángel, & Torrente Barredo, Begoña (2016). Redes sociales y ciberterrorismo. Las TIC como herramienta terrorista, https://www.redalyc.org/articulo.oa?id=31048481030

Quintana, Yolanda (2018) Ciberseguridad, una cuestión de Estados, Estudios de Política Exterior S. A., https://www.jstor.org/stable/10.2307/27045819

República Popular China (2015} Document: China's Military Strategy, USNI News, https://news,usni.org/2015/05/26/document-chinas-military-strategy#SGA

RT en español (2022) Putin: "Se ha desatado una guerra contra Rusia en el ciberespacio", https://actualidad.rt.com/actualidad/430385-putin-desatarse-guerra-rusia-ciberespacio

Saavedra, B. y Parraguez, L. (2018) La Ciberseguridad: análisis político y estratégico, Revista De Las Fuerzas Armadas, https://doi.org/10.25062/0120-0631.801

Segura Serrano, Antonio (2017) Ciberseguridad y Derecho Internacional. Revista Española de Derecho Internacional, Vol. 69, No. 2, Julio-diciembre, pp. 291-300. https://www.jstor.org/stable/10.2307/26187886

Sevillano, Fernando (2021) Ciberdefensa: el papel de los directivos ante un ciberataque. WTW, Willis Towers Watson Update. https://willistowerswatsonupdate.es/ciberseguridad/las-consecuencias-de-la-innaccion-ante-un-ciberataque/

Smith, B. (2022). Defending Ukraine: Early Lessons from the Cyber War - Microsoft On the Issues https://aka.ms/June22SpecialReport

Soesanto Stefan (2022) IT Army of Ukraine: Structure, Tasking, and Ecosystem, Taylos Grossman, Center for Security Studies (CSS) ETH Zürich, https://css.ethz.ch/en/publications/risk-and-resilience-reports/details.html?id=/t/h/e/i/the_it_army_of_ukraine

Sonia (2015). Ejército azul cibernético del Ejército Popular de Liberación de China, http://spanish.china.org.cn/specials/txt/2015-07/28/content_36165122.htm)

SSSCIPU (2023) Ukraine has signed an agreement on accession to the NATO Cooperative Cyber Defence Centre of Excellence, https://cip.gov.ua/en/news/ukrayina-pidpisala-ugodu-pro-priyednannya-do-ob-yednanogo-centru-peredovikh-tekhnologii-z-kiberoboroni-nato

Statista (2023) Ayuda enviada a Ucrania durante la guerra ruso-ucraniana a enero de 2023 por país y tipo, https://es.statista.com/estadisticas/1294251/guerra-rusia-ucrania-tipo-ayuda-militar-enviada-a-ucrania-por-cada-pais-en-2022/

Stone, Marianne (2009) Security according to Buzan: a Comprehensive Security Analysis. [Archivo PDF] http://geest.msh-paris.fr/IMG/pdf/Security_for_Buzan.mp3.pdf

The Economist, (2010) The threat from the Internet, cyberwar, https://www.economist.com/leaders/2010/07/01/cyberwar

Torres Soriano, Manuel R. (2018) El dilema de interpretación en el ciberespacio, Instituto de Estudios Estratégicos, https://dialnet.unirioja.es/servlet/articulo?codigo=6467940

Tallin Manual 2.0 on the International Law Applicable to Cyber Operations (2017) Cambridge University Press.

Unión Internacional de Telecomunicaciones (2010) Ciberseguridad. [Archivo PDF] https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

_____ (2023) La población mundial sin conexión sigue disminuyendo hasta los 2 600 millones de personas en 2023, https://www.itu.int/es/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx#:~:text=La%20reducci%C3%B3n%20desde%20los%202,5%20400%20millones%20de%20personas.

U. S. Army Cyber Command, (14 de septiembre de 2022) https://www.arcyber.army.mil/

U. S. Department of State (2023) Formalization of the Tallinn Mechanism to Coordinate Civilian Cyber Assitance to Ukraine, https://www.state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/

U. S. Goverment Accountability Office (2021) *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (infographic),* https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic

Wegenner, Henning (2014) La ciberseguridad en la Unión Europea, documento de opinión, Instituto Español de Estudios Estratégicos, https://dialnet.unirioja.es/servlet/articulo?codigo=7651416

Wilson, Clay (2007) Botnets, cybercrime, and cyberterrorism: vulnerabilities and policy issues for Congress, Congressional Research Service.

Wolter, Detlev, (2013) The UN Takes a Big Step Forward on Cybersecurity, Arms Control Today, https://www.armscontrol.org/act/2013-09/un-takes-big-step-forward-cybersecurity#source

World Economic Forum (2021) Informe de Riesgos globales de 2021. [Archivo PDF] https://www.zurich.com.mx/-/media/project/zwp/mexico/docs/grr2021-executive_summary_spanish.pdf

_____ (2022) Inteligencia Estratégica, https://intelligence.weforum.org/topics/a1Gb0000000pTDXEA2/key-issues/a1Gb00000015QsVEAU

Zinets, Natalia (2016) Ukraine hit by 6,500 hack attacks, sees Russian “cyberwar”, Reuters, 29 de diciembre de 2016. Disponible en: https://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC