Facultad de Ciencias Humanas y Sociales

Grado en Relaciones Internacionales

Trabajo Fin de Grado

El papel de la OTAN en la ciberdefensa europea

¿Cooperación o dependencia de la Unión Europea?

Estudiante: **Patricia Ruiz Ledesma.**

Director/a: Antonio González Terol.

Madrid, junio 2024

Resumen:

La cooperación entre la Organización del Tratado del Atlántico Norte y la Unión Europea es una de las relaciones más importantes para ambas organizaciones y se consideran mutuamente como aliados, por lo que es indiscutible que siguen un proceso similar en cuanto a desarrollo y comparten valores primordiales para el desarrollo de sus actividades. Sin poner en duda esta cooperación, el presente Trabajo de Fin de Grado busca analizar si en materia de ciberdefensa esta relación es de igualdad o si por el contrario la Unión Europea depende de los avances y de las capacidades defensivas de la OTAN. Esta investigación parte del reconocimiento del ciberespacio como un nuevo dominio estratégico, que, junto a los tradicionales, debe ser defendido, convirtiéndose en una prioridad en las estrategias defensivas de todos los países para asegurar la estabilidad y seguridad de sus fronteras y sistemas tecnológicos.

La OTAN, que nace como una alianza militar, presenta un enfoque más defensivo en el ciberespacio, teniendo como base de sus políticas el Artículo 5 de defensa colectiva. Su enfoque militar ha permitido a la Alianza desarrollar unas capacidades ciberdefensivas que se materializan en políticas y organismos. La visión de la OTAN contrasta con el marco normativo que ha diseñado la UE en materia de ciberseguridad. Este enfoque conlleva que la UE carezca de capacidades operativas autónomas que den respuesta a los ciberataques de manera inmediata y centralizada, aunque también cuenten con organismos y políticas especializadas en ciberseguridad. En cambio, presentan un marco de actuación y unas capacidades técnicas que ponen a disposición de los Estados Miembros para que sean ellos los responsables de articular una respuesta efectiva frente a un ciberataque.

Ambas organizaciones reiteran que mantienen una relación de cooperación basada en el intercambio de capacidades y la colaboración a la hora de defender el continente europeo. Lo que busca definir este trabajo de investigación mediante un análisis cualitativo documental es si las capacidades normativas y técnicas de la Unión Europea son suficientes para defender a sus Estados Miembros en caso de sufrir un ciberataque, o si, por el contrario, Europa depende de la respuesta militar y defensiva de la Alianza para proteger sus fronteras y sus sistemas tecnológicos de posibles amenazas.

Palabras clave: ciberespacio, ciberdefensa, diplomacia, seguridad, OTAN, Unión Europea.

Abstract:

Cooperation between the European Union and the North Atlantic Treaty Organization is one of the most important relationships for both organizations and leads to both of them regarding eachb other as allies, making it indisputable to defend that they follow a similar development process and share fundamental values that guide their respective activities. Without questioning this cooperation, the present TFG seeks to analyze wether, in the field of cyber defense, this relationship i son eof equality or wether, on the contrary, the European Union depends on NATO's advancemente and defensive capabilities. This research is based on the recognition of cyberspace as a new strategic domain, which, alongside traditional domains, must be protected, becoming a priority in national defense strategies to ensure the stability and security of borders and technological systems.

NATO, founded as a military alliance, adopts a more defense-oriented approach in cyberspace, building its policies on Article 5 on collective defense. This military focus has enabled the Alliance to develop robust cyber defense capabilities, translated into concrete policies and specialized bodies. NATO's perspective contrasts with the regulatory framework designed by the EU in the area of cybersecurity. This approach implies that the EU lacks autonomous operational capabilities to respond to cyberattacks in a rapid and centralized manner, although they have developed bodies and policies especialized on cybersecurity. Instead, it provides a framework, and technical resources made available to Member States, who remain responsible for articulating an effective response to such threats.

Both organizations repeatedly affirm that they maintain a cooperative relationship based on capacity-sharing and joint efforts to defend the European continent. What this research project seeks to determine, through qualitative and documentary analysis, is whether the European Union's legal and technical capacities are sufficient to protect its Member States in the event of a cyberattack, or whether, instead, Europe relies on the military and defensive response of the Alliance to safeguard its borders and technological systems against potential threats.

Key words: cyber space, cyber defense, diplomacy, security, NATO, European Union.

ÍNDICE

1. INTRODUCCIÓN

1.1 Finalidad

Con este Trabajo de Fin de Grado se pretende analizar en profundidad el papel que desempeñan la OTAN y la UE en el ámbito de la ciberdefensa, y cómo es su relación de cooperación. A través de un enfoque comparativo se busca determinar hasta qué punto la acción ciberdefensiva de la UE puede considerarse autónoma o si, por el contrario, depende estructuralmente de las capacidades, políticas y decisiones de la OTAN. El objetivo es entender las distintas implicaciones que tienen las decisiones de ciberseguridad que la OTAN toma en el espacio euroatlántico y como estas decisiones cambian las nociones de defensa y diplomacia dentro del espacio europeo, hasta el punto de convertir las decisiones europeas en secundarias frente a las de la Alianza.

1.1.2 Motivación

Este TFG surge de un creciente interés por la ciberseguridad y las distintas amenazas que surgen a partir de los desarrollos tecnológico y que desestabilizan la seguridad de la comunidad internacional. Desde pequeña me ha interesado mucho la defensa nacional, las amenazas que ponen en riesgo nuestra seguridad, y sobre todo entenderlas para poder contrarrestarlas haciendo uso de herramientas diplomáticas y de mediación en la medida que sea posible. Mi interés en el ámbito de la ciberseguridad empezó a formarse en marzo de 2024 cuando tuve la suerte de empezar unas prácticas en el departamento de ciberseguridad de una empresa y perdura a día de hoy. Entender como aquello que nos une tanto a las personas, como son las tecnologías, nos puede separar e incluso destruir me abruma, y es lo que hace que mis ganas de seguir ahondando en este tema crezcan día tras día. Entender qué hacen las organizaciones internacionales que nos tienen que defender frente a estas amenazas y como se coordinan me lleva a soñar con formar parte algún día de una de esas organizaciones para poder proteger a mi país.

1.2 Contextualización y relevancia

«Quien controle el ciberespacio ganará las guerras del futuro» (Fuente, 2022). La guerra es el resultado de la unión entre factores estáticos y dinámicos. Los estáticos, como definió Clausewitz, son aquellos que se mantienen siempre igual y no se ven afectados por factores externos, como, por ejemplo, que toda guerra genera una violencia cuya duración es invariable, que no es un fenómeno aislado y que se caracteriza por la incertidumbre. Pero estos factores estáticos conviven con una serie de factores dinámicos

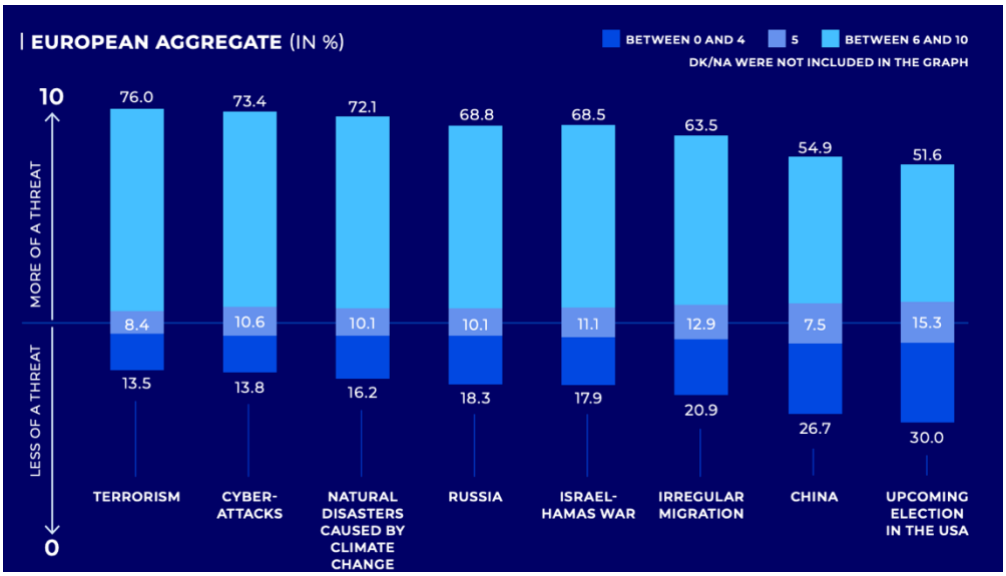
que se ven afectados por los desarrollos tecnológicos que se dan a lo largo de los años y cuyo uso depende de la instrumentalización que cada actor haga de estos desarrollos en base a sus intereses y capacidades. Estos factores dinámicos han ido definiendo diferentes momentos en el "Arte de la Guerra", término que incubó el General Sun Tzu, estableciendo a lo largo de la historia diferentes generaciones de la guerra (Vallejos, 2023).

Hoy en día podemos considerar que ya se han empezado a dar las guerras de quita generación, las cuales destacan por el uso de la fuerza cibernética e informática por parte de los actores para alcanzar sus intereses nacionales o personales, teniendo en mente la ciberguerra como la forma de alcanzar el poder (Lalinde, 2017). Es importante destacar que, mientras que en las primeras generaciones las guerras eran libradas entre estados, las guerras en el ciberespacio se dan a través de amenazas formuladas por diversos actores, estatales y no estatales, debido a la accesibilidad a las tecnologías y el bajo coste de los ataques, a los cuales es muchas veces difícil atribuir un autor debido a la anonimidad que se puede conseguir en Internet. La OTAN defiende que aquellos actores que buscan desestabilizar la Alianza están haciéndolo mediante actividades y campañas cibernéticas maliciosas, instando a los Estados Miembros sobre la importancia de una mayor adaptación y cooperación en este ámbito. Pero, al ser un ámbito emergente y con rápidos avances, las alianzas no deben formarse solo entre países de una misma organización o unión, sino que deben ir más allá, forjando vínculos entre organizaciones para así poder hacer frente a estas amenazas de manera efectiva y contundente.

En noviembre de 2024, la Universidad IE publicó un informe llamado "*Next Generation Security"* cuyo objetivo era entender la visión que la juventud europea tiene sobre el ámbito de la defensa y la seguridad internacional (IE, 2024). En la primera pregunta se les presentaron a los encuestados 8 posibles amenazas para la seguridad europea y les pidieron que diesen su opinión sobre cuáles eran una amenaza real a día de hoy, indicando el 0 que no es una amenaza y el 10 que es una amenaza muy seria. Los ciberataques fueron identificados como la segunda amenaza más real a día de hoy con una puntuación de un 73.4%, solo 2.6 puntos por detrás del terrorismo, la amenaza considerada la más real a día de hoy (IE, 2024). Estos resultados demuestran que los jóvenes son conscientes de que aquellas amenazas emergentes que parecían cosa del futuro se han convertido no solo en una realidad, sino en una prioridad a día de hoy de

cara a la seguridad nacional, convirtiéndose el desarrollo de herramientas ciberdefensivas en una necesidad para asegurar la protección y seguridad de las sociedades.

Gráfica 1: Percepción de amenazas a la seguridad europea entre la juventud, 2024.



Fuente: Next Generation Security, IE University.

1.3 Hipótesis

La cooperación diplomática entre la OTAN y la Unión Europea en materia de ciberdefensa es fundamental para establecer un marco de gobernanza global en ciberseguridad. Las decisiones que toma la Organización del Tratado del Atlántico Norte tienen una gran impacto en la defensa de todos los países del mundo, en especial en la Unión Europea, que, aunque haya avanzado notablemente en el desarrollo de una política común de ciberseguridad, debido a sus limitadas capacidades defensivas, sigue dependiendo de la OTAN para cubrir la dimensión ciberdefensiva y militar que reclaman las amenazas del ciberespacio. Bien es cierto que, mientras la OTAN aporta una filosofía militar a la solución de los problemas, la Unión Europea aporta una seria de herramientas políticas y económicas, creando así vínculos de cooperación entre ambas organizaciones y estableciendo un marco normativo y técnico sólido en el ámbito ciberdefensivo de la Unión Europea.

1.4 Metodología

Para el presente Trabajo de Fin de Grado se ha realizado un análisis cualitativo basado principalmente en el análisis documental, contemplando tanto fuentes primarias como secundarias a lo largo de los años para entender la evolución de la ciberdefensa como concepto y ámbito estratégico en la OTAN y en la UE. Este análisis también ha sido de gran ayuda para conocer las similitudes y diferencias que existen entre ambas organizaciones, las cuales regulan las relaciones entre ambas. Entre las fuentes primarias que se han analizado se encuentran los tratados fundacionales de cada organización, las políticas ciberdefensivas y de ciberseguridad, los conceptos y documentos estratégicos de la Unión Europea, de la Organización del Tratado del Atlántico Norte y de las Naciones Unidas, así como los marcos de cooperación que existen entre ellas.

Por otro lado, también se ha llevado a cabo el análisis de fuentes secundarias entre los que se encuentran los informes del Gobierno de España, artículos académicos y publicaciones en revistas científicas sobre Relaciones Internacionales, seguridad y ciberdefensa. Esta metodología nos ha permitido entender y analizar no solo el contenido normativo y estratégico de cada organización, sino que también el lenguaje que emplea cada organización que establece las prioridades políticas de cada una de ellas, permitiéndonos entender los puntos fuertes de cada organización y aquellos ámbitos en los que necesitan un apoyo externo más significativo.

2. MARCO TEÓRICO

2.1. Conceptos clave

En este apartado se pretenden desarrollar e investigar más a fondo aquellos conceptos que sustentan el marco teórico de este trabajo de investigación. Nos permiten no solo delimitar el objeto de estudio, sino que también facilitan la comprensión de las dinámicas diplomáticas y estratégicas en torno a la cooperación internacional en materia de ciberseguridad y ciberdefensa. En este sentido, se abordarán las nociones de ciberespacio, ciberseguridad, ciberdefensa o ciberdiplomacia, esenciales para entender el desarrollo de las políticas y estrategias en el ámbito de la ciberdefensa internacional, sustentadas por la ciberdiplomacia, la defensa mutua y la gobernanza global, con el objetivo de hacer frente a las amenazas emergentes.

2.1.1 Ciberespacio

Estas amenazas emergentes que desestabilizan el orden internacional se desarrollan en el ciberespacio, una dimensión espacial que combina lo virtual con lo real a través del intercambio de información en grandes volúmenes, implicando una mayor conectividad, pero a su vez una mayor dependencia sobre las transformaciones sociales, económicas y políticas, generando un sistema inestable y con amenazas emergentes no tratadas con anterioridad (Lalinde, 2017). Es por ello por lo que podemos confirmar que la ciberseguridad y la ciberdefensa se desarrollan dentro del ciberespacio al tener como objetivo la defensa de los sistemas, las infraestructuras y los datos que lo conforman.

«El ciberespacio no es un dominio como los demás, pues es terreno de intrínseca asimetría de los bandos en conflicto» (García e Iglesias, 2022). Esto implica que no todos los actores tienen el mismo poder o capacidades en este ámbito, algo que se da en todos los escenarios, lo que es novedoso en el ciberespacio es que los actores que tradicionalmente tenían menos capacidades militares en los conflictos, pueden ser actores de vital importancia en el ciberespacio, por lo que su capacidad de dañar las tecnologías de otros actores puede ser desproporcionada respecto a su tamaño o recursos. En este ámbito, actores no estatales, como pueden ser grupos terroristas, pueden tener acceso al desarrollo o al uso de herramientas digitales de bajo coste, pero con un gran impacto una vez utilizadas. Este cambio en las capacidades de grupos tradicionalmente menos poderosos obliga a que se reformulen las normas y la forma de atajar las amenazas, pues las normas tradicionales pueden no tener los resultados que se esperan de ellas, lo que

dificulta su aplicación en este ámbito.

2.1.2 Ciberseguridad y Ciberdefensa

La ciberseguridad es definida por *Kaspersky*, la empresa de ciberseguridad mundialmente conocida, como la «práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos» (Kaspersky, s.f.). En otras palabras, se puede definir como aquellas herramientas que sirven para proteger los dispositivos electrónicos de cualquier amenaza que ponga en riesgo su funcionamiento y seguridad. Sus funciones se materializan principalmente en la prevención de accesos no autorizados, la detección de vulnerabilidades técnicas, la protección de infraestructuras críticas o en garantizar la continuidad del funcionamiento de estas infraestructuras.

Por otro lado, la ciberdefensa es una de las disciplinas que conforman la ciberseguridad. Es definida como «el conjunto de estrategias implementadas para proteger de forma activa sistemas informáticos, redes, datos y dispositivos contra ataques cibernéticos» (S2GRUPO, 2025). Esta disciplina tiene una función más estratégica cuyo objetivo principal es la defesa de un Estado frente a un ciberataque que surge a partir de una motivación política, militar o geopolítica. En este sentido, podemos ver que las estrategias para las amenazas cibernéticas varían de las estrategias que se utilizaban tradicionalmente para mitigar y reducir los riesgos que los ataques podían causar. Estás estrategias están más orientadas hacia la protección de aquellos sistemas tecnológicos que puedan ser objeto de ataque por parte del adversario para causar el colapso de los sectores económicos, políticos, sociales y de seguridad. Los ejércitos no desempeñan un papel central cuando se dan este tipo de amenazas, pues las forma de contrarrestar estos ataques se centra en el ámbito digital, no tanto en confrontaciones físicas convencionales (Lalinde, 2017). La respuesta que un país tenga frente a un ciberataque no depende en el despliegue militar, sino en su capacidad tecnológica y una exitosa gestión de la información disponible.

2.1.3 Ciberdiplomacia

La diplomacia es definida por la Real Academia Española como: «el conjunto de los procedimientos que regulan las relaciones entre los Estados» (DEL, s.f.). Por lo que, la ciberdiplomacia no son más que aquellos mecanismos que regulan las relaciones entre

los Estados y los actores no estatales en el ciberespacio con el objetivo de preservar la seguridad internacional. Esta disciplina no es solo útil para regularizar las relaciones, sino que es clave también para generar credibilidad (Pardo, s.f.). Como destacó Michael N.Schmitt en su artículo "*The law of cyber warfare:quo vadis?"*: «a medida que los estados se convierten más dependientes en actividades cibernéticas, irán valorando en mayor medida el acceso, y habilidad de explotar, el ciberespacio» (Schmitt, 2014). El objetivo de la ciberdiplomacia en este contexto es convertirse en una herramienta que garantice un uso del ciberespacio equitativo y responsable, no solo para prevenir conflictos, sino también para establecer un marco de gobernanza global al que se adhieran todos los países.

Una gran diferencia entre la diplomacia tradicional y la ciberdiplomacia radica en que, mientras que la diplomacia se suele relacionar con relaciones entre Estados, la ciberdiplomacia incluye también a actores como el sector privado o la sociedad civil, pues el contexto digital ha hecho del ciberespacio un entorno globalizado accesible a todo el mundo, en el que todos pueden ser víctimas y perpetradores de amenazas cibernéticas. Los actores del sector privado son fundamentales como consecuencia de sus capacidades en relación a la infraestructura digital y su poder sobre la opinión pública sobre todo en situaciones de falta de transparencia (Kasper et al, 2021).

La globalización y el uso generalizado de internet han transformado profundamente el panorama de la seguridad internacional. Las nuevas tecnologías traen consigo nuevos desarrollos que pueden convertirse en amenazas para la seguridad de los países cuando no son utilizados con el objetivo para el que fueron creados. Es un ámbito de fácil acceso, lo que hace posible que actores que tradicionalmente no planteaban grandes amenazas para la seguridad de un país se adquieran capacidades ofensivas similares a las de un estado, siendo de vital importancia su inclusión en los diálogos diplomáticos para la creación de unos marcos legales comunes que promuevan la cooperación internacional en el ámbito digital.

2.2 Enfoques teóricos en Relaciones Internacionales

Para poder entender el papel actual de la OTAN y la Unión Europea en el ámbito de la ciberdefensa y la diplomacia, es necesario enmarcar sus acciones a través de unos enfoques teóricos que nos permitan comprender por qué actúan de una manera

determinada ante las amenazas emergente y en qué se basan para tomar decisiones que definirán la estrategia y rumbo de la organización.

2.2.1. *Soft Power*

La Teoría del *Soft Power* fue acuñada por Joseph Nye, quien diferenció entre dos tipos de poder: el *hard power*, que es la habilidad de coaccionar a alguien para que actúe de forma contraria a la que actuarían, a través de amenazas y violencia; y el *soft power*, que definió como la habilidad de conseguir que el resto ansíen los objetivos que tú quieres, no a través de la intimidación sino de la persuasión o la atracción (Gomichon, 2013). Mientras que con el *hard power* te aseguras en gran parte conseguir tus objetivos o por lo menos poner en alerta a la persona hacia la que va dirigida la amenaza, el *soft power* es más complicado de ejecutar y ver sus resultados a corto plazo, pues depende en gran parte en la forma en la que las audiencias reciben el mensaje o la propuesta, siendo crucial la transparencia para ganar la credibilidad necesaria para ganar apoyos (Nye, 2016). Cuando estos apoyos se consiguen, es cierto que son más duraderos que los conseguidos haciendo uso del *hard power*, pues los objetivos, que al principio eran solo de un país o una organización, se transforman en objetivos comunes porque este actor ha conseguido presentar sus valores de una manera en la que el resto de los actores los comparten, sin necesidad de imponérselos, sino ganando credibilidad, lo que hace que todos sientan esos objetivos y futuros resultados como propios.

El desarrollo de la ciberdiplomacia es un claro ejemplo de *soft power*, pues busca la creación de puntos de interés comunes y un espacio de diálogo en el que los países pueden defender sus intereses en el ámbito internacional, pero teniendo a su vez en cuenta las implicaciones que estos pueden tener para el resto de los países. Aunque ambos tipos de poder son necesarios para contrarrestar amenazas como el ciberterrorismo, el *soft power* puede considerarse como más útil en este escenario porque muchas veces la identidad del perpetrador del ataque no se conoce, lo que dificulta la imposición de índole militar, pues no sabes a quién tienen que ir dirigidas, pero siempre suele haber un canal de comunicación por el que los atacantes se comunican con las víctimas para negociar, un canal que bien utilizado, es una herramienta muy poderosa de diplomacia.

2.2.2. Principio de defensa colectiva

El objetivo principal de la comunidad internacional es garantizar la seguridad y la

paz entre los Estados, de manera que se respeten los derechos fundamentales de todas las personas sin discriminación. El uso de fuerza para garantizar esta seguridad está prohibido bajo el Artículo 2.4[1] de la Carta de las Naciones Unidas, aunque hay dos excepciones a este principio, o bien la autorización del Consejo de Seguridad en caso de amenazas que pongan en juego la paz, o la invocación del Artículo 51[2]. Este Artículo estipula que la defensa de un Estado Miembro de las Naciones Unidas que sufre un ataque armado se puede llevar a cabo de manera individual o colectiva (Naciones Unidas, 1945). Este artículo supone un cambio en la visión de la seguridad, que pasa de ser considerada un problema exclusivo de cada Estado, a convertirse en una cuestión de responsabilidad internacional, implicando una puesta en común de los Estados para colectivizar los esfuerzos de defensa y así poder desarrollar respuestas frente a las amenazas emergentes.

Este principio es el que da fundamento jurídico a la creación de organizaciones como la OTAN, la cual incluye en el conocido Tratado de Washington el Artículo 5 este principio de defensa colectiva, defendiendo que: «un ataque armado contra una o más de ellas [Estados Miembros de la Alianza], 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 res-tablecer la seguridad en la zona del Atlántico Norte» (OTAN, 2008). A su vez, la Unión Europea también incluye en su tratado fundacional bajo el ámbito de Política Común de Seguridad y Defensa, la cláusula 7 en el Artículo 42 en el que indica que: «si un Estado miembro es objeto de una agresión armada en su territorio, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el artículo 51 de la Carta de las

[1] Art. 2.4 Carta de las Naciones Unidas: "Para la realización de los Propósitos consignados en el Artículo 1, la Organización y sus Miembros procederán de acuerdo con los siguientes Principios: Para la realización de los Propósitos consignados en el Artículo 1, la Organización y sus Miembros procederán de acuerdo con los siguientes Principios" (Naciones Unidas, 1945).

[2] Art 51 Carta de las Naciones Unidas: "Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un Miembro de las Naciones Unidas, hasta tanto que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales."

Naciones Unidas…ajustándose a los compromisos adquiridos en el marco de la OTAN» (Unión Europea, 2016).

Muy pocos países u organizaciones han invocado el Artículo 51 de la Carta de las Naciones Unidas desde su redacción en el año 1945, pero cabe destacar tanto como la OTAN como la Unión Europea han invocado este principio en un punto de su historia. La OTAN invocó el Artículo 5 que hace referencia a este principio tras los ataques terroristas sobre las Torres Gemelas el 11 de septiembre de 2001 (Riegert, 2022). Por su parte, la Unión Europea lo invocó a través del artículo 42.7 en el año 2015 tras los atentados terroristas en París el 13 de noviembre (Morillas, 2015).

2.2.3 Gobernanza global

La gobernanza global puede definirse como "la suma de muchas formas en que individuos e instituciones, públicas y privadas, manejan sus asuntos en común" (Villamar, 2017). Una de las cualidades de la gobernanza global es que no es estática, ya que debe adaptarse a los intereses y características de cada conflicto o escenario, teniendo en cuenta los objetivos de cada país e intentando llegar a conclusiones colaborativas sin que un solo país sea el que decide sobre el resto en base a sus intereses.

Se puede decir que la gobernanza global en el ciberespacio es intrínseca tras la publicación de las Naciones Unidas en el año 1967 del "Tratado sobre los principios que deben regir las actividades de los Estados en la exploración y utilización del espacio ultraterrestre, incluso la Luna y otros cuerpos terrestres". El Artículo I de este tratado defiende, entre otras ideas, que «El espacio ultraterrestre, incluso la Luna y otros cuerpos celestes, estará abierto para su exploración y utilización a todos los Estados sin discriminación alguna en condiciones de igualdad y en conformidad con el derecho internacional, y habrá libertad de acceso a todas las regiones de los cuerpos celestes», principio apoyado en el Artículo II, el cual estipula que «El espacio ultraterrestre, incluso la Luna y otros cuerpos celestes, no podrá ser objeto de apropiación nacional por reivindicación de soberanía, uso u ocupación, ni de ninguna otra manera» (Naciones Unidas, 2002).

En línea con estos artículos, la gobernanza global se muestra como una herramienta importante para tratar los posibles conflictos que surjan en el ciberespacio, pues como se define en el Tratado de 1967, el ciberespacio es global y no tiene fronteras, ningún estado puede clamarse soberano sobre este ámbito y por ello, se necesitan unas acciones y estrategias comunes entre los Estados, organismos internacionales y actores no estatales, que les permitan gestionar sus relaciones en el ciberespacio de forma pacífica, con el objetivo de establecer unas normas comunes, generando alianzas estratégicas para hacer frente a las crecientes amenazas digitales. Una de las metas de la gobernanza global es que se haga un uso correcto de los desarrollos tecnológicos, los cuales pueden ver transformados los objetivos por los que fueron creados en consecuencia a la ambición de poder y control sobre el ciberespacio.

La gobernanza global ha ido afianzando su importancia estratégica y se ha convertido en una dimensión de vital importancia para la política exterior no solo de los países, sino también de organizaciones internacionales como pueden ser la OTAN o la Unión Europea. Las alianzas internacionales son fundamentales, especialmente para aquellos países cuyas capacidades tecnológicas no están tan desarrolladas, y para el establecimiento de unas normas comunes para asegurar la seguridad de la información y un uso correcto de los desarrollos tecnológicos.

3. LA ESTRATEGIA DE CIBERDEFENSA DE LA OTAN Y SU IMPORTANCIA COMO ACOR DIPLOMÁTICO.

La Organización del Tratado del Atlántico Norte es una alianza política, al promover valores diplomáticos garantizados por el Consejo Atlántico, y militar, ya que fue fundada con la firma del conocido Tratado de Washington el 4 de abril de 1949, como resultado de la aplicación del artículo 51 de la Carta de las Naciones Unidas, el cual reconoce el derecho inherente de los Estados a la legítima defensa colectiva. Lo que al principio era una alianza de 12 Estados, se ha convertido ahora en una organización que ampara y defiende la libertad y la seguridad de 32 Estados Miembros de Norte América y Europa, los cuales afirman su compromiso con la defensa colectiva de los Estados Miembros de la Alianza, contemplada en el Artículo 5 (OTAN, 2022a).

La alianza surge durante el contexto de la Guerra Fría como respuesta a la creciente amenaza comunista de la Unión Soviética tras el fin de la Segunda Guerra Mundial y el miedo de una guerra nuclear, lo que dividió el mundo en dos bloques ideológicos. Después de la caída del Muro de Berlín en 1989 y consecuente desintegración de la Unión Soviética, la Alianza no solo siguió en pie, sino que fue expandiéndose y adaptándose al nuevo contexto internacional. Para adaptar su visión estratégica, la OTAN publica periódicamente los conocidos "Conceptos Estratégicos", en los que definen sus prioridades de seguridad, amenazas principales y medios para hacer frente a estas (Gobierno de España, s.f).

Desde su origen, se estableció como una organización intergubernamental a través de la cual los países miembros gozan de una soberanía e independencia plena, pero sin olvidar su compromiso con la cooperación mutua entre estos estados soberanos, garantizando que todos los miembros se vean apoyados por el resto de los estados a la hora de enfrentar los desafíos de seguridad emergentes (Carmés, 2000). Dentro de la Alianza hay países con más peso en los asuntos internacionales por su papel geopolítico y capacidades, y otros países que se mantienen en una segunda línea, por lo que las decisiones en la OTAN se toman por consenso en el Consejo del Atlántico Norte (OTAN, 2023), asegurando que todos los países tienen la misma capacidad de decisión dentro de la organización y ven sus intereses nacionales salvaguardados, siendo un ejemplo de *soft power*, al invitar a sus miembros a negociar y dialogar en vez de coaccionar.

3.1 La OTAN como actor en ciberdefensa

«El número de ciberataques aumenta cada día, ya sea contra los sistemas de la OTAN o contra los sistemas vitales de nuestros países miembros» (OTAN, 2012). Con esta idea en mente, la Alianza, que tradicionalmente reconocía los dominios terrestre, marítimo y aéreo como sus espacios operacionales clave en su misión defensiva, ha ido incluyendo también en las últimas décadas el ciberespacio, asumiendo el impacto que las amenazas digitales pueden tener sobre la seguridad de un país o región y considerándolo una herramienta de defensa y de disuasión (García e Iglesias, 2022). Aunque hasta unos años más tarde no se desarrollaron medidas operativas concretas, la ciberdefensa se convirtió en un punto más dentro de la agenda estratégica de la alianza tras la Cumbre de Praga en el año 2002, cuando se planteó la necesidad de crear un plan integral para la Alianza en materia de defensa contra los ataques cibernéticos (Fuente, 2022).

En el Artículo 5 del Tratado que fundamenta la creación de esta Organización se estipula que el principio de defensa colectiva podía ser invocado frente a ataques armados dirigidos a algún miembro de la Alianza, pero tras la cumbre de la OTAN en Bruselas en 2021, la Alianza afirmó que, en el caso de darse una amenaza cibernética en uno de los Estados Miembros, la alianza consideraría, teniendo en cuenta las características personales de cada caso, la invocación del Artículo 5, pues su compromiso con la defensa de los países de la alianza pasa también por la ciberseguridad (OTAN, 2024). Esto se dio gracias al reconocimiento del ciberespacio como un dominio operativo en el Compromiso de Ciberseguridad[3], que se publicó en julio de 2016 tras la Cumbre de Varsovia. Que se considere un dominio operativo implica que se vea el ciberespacio como un ámbito más de defensa en el que las capacidades militares de la alianza jueguen un papel fundamental. En este sentido, y dada la creciente interdependencia entre actores internacionales, la OTAN ha intensificado su cooperación con organizaciones como la Unión Europea a la hora de coordinar la respuesta frente a incidentes o el intercambio de inteligencia.

La actuación de la OTAN en materia de ciberdefensa se fundamenta en políticas y escritos, así como en agencias y organismos que ayudan a poner en marcha estos documentos en materia de ciberseguridad. Desde el ataque cibernético en Estonia en

[3] El Compromiso de Ciberdefensa es un documento que responsabiliza a la OTAN a proteger las redes de la alianza, además de establecer mejores prácticas y estándares, aumentando los recursos destinados para este ámbito y la concienciación (Besch, 2018).

2008, la OTAN ha cambiado su visión relativa a la ciberseguridad, desarrollando un planteamiento más estratégico, para hacer frente a las crecientes amenazas, y cada vez menos técnico a través del cual se materializan los objetivos que la Alianza tiene en el ámbito de la ciberdefensa, plasmando el nuevo planteamiento estratégico en la publicación de su primera Política de Defensa Cibernética (Fuentes, 2022). Ejemplo de ello es la adaptación de la Alianza de su visión estratégica tras la aparición del virus Stuxnet, cuando la OTAN aumentó su foco en la ciberdefensa en el Concepto Estratégico de 2010, pues indicaron que estas amenazas era una fuente de desestabilización para la Alianza y por ello debían ser consideradas en su el planteamiento defensivo (Caro, 2011). Los aliados empezaron entonces a ser más conscientes de que su seguridad dependía de cuán bien protegidos estuvieses sus sistemas de información y comunicación y no solamente sus fronteras, las cuales se podían ver mermadas por amenazas tradicionales y tecnológicas.

En los últimos 5 años, los avances estratégicos de la OTAN en ciberdefensa han sido notorios. Tras la Cumbre de la OTAN del año 2021 se publicó la Política integral de Ciberdefensa, la cual reafirma no solo el papel defensivo de la Alianza, sino también su compromiso en la aplicación de todas las medidas necesarias para disuadir y contrarrestar las ciberamenazas, incluyendo la posibilidad de hacerlo mediante respuestas colectivas, invocando el Artículo 5 (OTAN, 2024). El objetivo de esta política es crear normas comunes, pero como defiende Fuentes, sin olvidar que los Estados Miembros tienen la última palabra en cuanto a las acciones ofensivas frente a cualquier ataque, en este caso cibernético[4]. Un año más tarde se publicó el Concepto Estratégico de 2022, un documento de índole política-estratégica que define las prioridades generales de la OTAN para la siguiente década, enfatizando en la necesidad de integrar el ciberespacio en la estrategia general de seguridad de la Alianza, destacando la importancia de la cooperación entre actores estatales y no estatales para hacer frente a las nuevas amenazas y defendiendo, una vez más, la posibilidad de invocar el Artículo 5 (Ministerio de Defensa, 2022). Por otro lado, cabe destacar el desarrollo del mecanismo de la Capacidad Virtual de Apoyo a Incidentes Cibernéticos, integrada por primera vez en la Cumbre de Vilna en 2023 y cuya función es coordinar la asistencia entre aliados en caso de un ciberataque, con el objetivo

[4] Este punto hace referencia al principio de soberanía de cada Estado en el momento de tomar la decisión del nivel de compromiso que está dispuesto a asumir en cada situación. Es similar al envío de tropas en misiones de la OTAN, en las que cada Estado decide de manera voluntaria y basándose en su capacidad técnica.

de minimizar el impacto de las amenazas y preparar a los países para una rápida recuperación de forma homogénea (Illiuta, 2025).

Entre los principales organismos especializados en ciberdefensa de la Alianza destacan tres actores clave, con funciones complementarias. La Autoridad de Gestión de Defensa Cibernética de la OTAN, NCMA, es la encargada de supervisar y coordinar las políticas y estándares de ciberdefensa en el conjunto de la Alianza (Fuentes, 2022). La creación de esta autoridad supone un antes y un después en el enfoque estratégico de la alianza frente a las ciberamenazas, pues establece una figura a la que acudir en caso de sufrir un ciberataque. Por otro lado, la Alianza cuenta con el Centro Cooperativo de Excelencia en Ciberdefensa, CCDCOE**,** con sede en Tallin desde 2008, lo cual es significativo ya que se estableció con Estonia como país anfitrión justo después del ciberataque que sufrieron (Caro, 2011). Este centro no forma parte del mando militar, al no estar bajo el control operativo de organismos como el SHAPE, pero sí está acreditado por la OTAN. Se centra en investigación estratégica, formación, simulacros y análisis jurídico y doctrinal del ciberespacio.

Además de este centro, en el año 2024, la OTAN estableció el Centro Integrado de Ciberdefensa, formado por personal civil y militar, encargado de supervisar y mejorar la ciberseguridad de las operaciones y sistemas de la Alianza, con el objetivo de consolidar y coordinar los esfuerzos de los Miembros y proporcionar a los responsables de la estrategia militar de la OTAN información vital sobre amenazas y vulnerabilidades emergentes. Su actividad la desarrolla gracias a las investigaciones del CCDCOE, utilizando los desarrollos para mejorar sus capacidades (Aicad, 2024). El centro depende de la Agencia de los Servicios de Información y Comunicación, con base en el Cuartel General Supremo de las Potencias Aliadas en Europa (SHAPE). Además de los organismos institucionales, la OTAN reconoce el papel fundamental del sector privado y los centros de investigación en el fortalecimiento de la ciberresiliencia dado a su papel clave en el proceso de innovación tecnológica, en la formación de capacidades y en el diseño de simulacros que ayudan a la planificación estratégica de la alianza (OTAN, 2022b).

Todos los organismos con los que cuentan están bajo las directrices del centro técnico de la Capacidad de Respuesta a Incidentes Informáticos de la OTAN, NCIRC, el cual desarrolla las directrices de seguridad comunes para la alianza con el objetivo de prevenir vulnerabilidades en los sistemas y redes de información. Además de los centros con los que cuentan, la Alianza ha formado el denominado "Equipo de Reacción Rápida" con el objetivo de agilizar la asistencia a los Estados Miembros en caso de necesitar ayuda frente a un ciberataque (OTAN, 2012). En paralelo a su actuación operativa, la Alianza participa activamente en la definición y defensa de normas internacionales sobre el uso legítimo del ciberespacio, siguiendo las directrices de la Organización de las Naciones Unidas.

4. LA ESTRATEGIA DE CIBERDEFENSA DE LA UNIÓN EUROPEA

La Unión Europea como la conocemos hoy en día, fundada bajo el tratado de Maastricht en el año 1993, es la evolución de la Comunidad Económica Europea, fundada en 1958 con el propósito de fomentar la cooperación económica entre Alemania, Bélgica, Italia y Países Bajos. Desde sus inicios, se han ido incorporando nuevos países y su ámbito de actuación ha aumentado, hasta convertirse en una unión económica y política que congrega actualmente a 27 Estados Miembros. Estos países europeos comparten un mercado único que permite la libre circulación de mercancías, servicios, personas y capital dentro de sus fronteras (Comisión Europea, 2022a). Mientras que los ciudadanos están directamente representados por el Parlamento Europeo, el Consejo Europeo y el Consejo de la Unión Europea representan a los países, siguiendo el principio de democracia representativa y con una arquitectura institucional que combina elementos supranacionales e intergubernamentales. Esta estructura de la Unión Europea le permite actuar como un actor decisivo en la esfera internacional a nivel económico, político, diplomático y social.

Dentro de la Unión Europea, las decisiones de seguridad se enmarcan en las responsabilidades del Consejo de la Unión Europea al ser el órgano competente de aplicar el marco de la Política Común de Seguridad y Defensa, establecida por el Tratado de Lisboa de 2007. Para la toma de decisiones se requiere una votación en la que la unanimidad es la única opción para poder implantar una nueva estrategia o decisión. Esto se debe a la naturaleza intergubernamental de la toma de decisiones en materia de seguridad y defensa, por la que la soberanía de todos los estados es respetada en cuanto a su participación y sus capacidades, la cual se ve reflejada en el Artículo 42 del Tratado de la Unión Europea (Unión Europea, 2016).

4.1 La Unión Europea como actor en ciberdefensa

La ciberdefensa se convirtió en un espacio estratégico para la Unión Europea en el año 2013 con la publicación de la Estrategia de Ciberseguridad de la Unión Europea, la cual establece el ciberespacio como un ámbito crítico para la seguridad y el desarrollo económico, con el objetivo de conseguir un ciberespacio abierto, protegido y seguro (Comisión Europea, 2013). El enfoque sobre el ciberespacio de la UE se ha desarrollado más en base a su ámbito normativo que en el defensivo, salvaguardando la aplicación del Derecho Internacional, amparado bajo el marco jurídico internacional de la Carta de las

Naciones Unidas sobre el ciberespacio. La UE ha adoptado una postura a través de la cual promueve el diálogo, pues sostiene que un mejor entendimiento común es la forma de aumentar la ciberresiliencia a nivel mundial (Consejo de la Unión Europea, 2024).

Desde sus inicios en el ámbito de la ciberseguridad en el año 2013, la Unión Europea ha defendido que los principios de defensa de los derechos fundamentales que rigen los ámbitos terrestre, marítimo y aéreo, deben aplicarse también en el ciberespacio, entontando su estrategia desde el punto de vista normativo. Entre estos derechos fundamentales cabe destacar el constante llamamiento a la defesa de la libertad en internet de los ciudadanos de la UE[5]. En su Estrategia de Ciberseguridad cabe destacar también el llamamiento a la necesidad de una cooperación entre el sector público y privado, pudiendo el privado ofrecer tecnologías innovadoras mientras que el sector público es el encargado de articular la estrategia colectiva (Comisión Europea, 2013). En el año 2017, tras el Consejo de Asuntos Generales de noviembre de 2017, los en aquel entonces 28 Estados Miembros, acordaron que la cláusula 42.7 de asistencia mutua de la UE pudiese ser invocada tras un ciberincidente grave (DNS, 2017). Es importante destacar que en las conclusiones se hace hincapié en la responsabilidad principal de cada Estado de mejorar su propia ciberseguridad y garantizar su capacidad de respuesta, siendo la aportación de la UE un valor añadido de cooperación (Consejo de la Unión Europea, 2017).

Años más tarde, en el contexto de la agresión de Rusia a Ucrania, se publicó la Brújula Estratégica para la seguridad y la defensa del año 2022, que establece un plan para reforzar la seguridad y defensa de la UE hasta 2030. En este documento, la UE menciona los ciberataques como uno de los instrumentos utilizado para desestabilizar la Unión y comprometer su seguridad, convirtiéndose el ciberespacio en un ámbito de competencia estratégica (Consejo de la Unión Europea, 2022). Ese mismo año la Comisión Europea publicó la Política de Ciberdefensa, que establece de forma visible las aspiraciones de la UE de asumir mayores responsabilidades y afianzar su soberanía en el ámbito cibernético, lo cual depende de su desarrollo tecnológico, siendo este el primer punto a abordar para conseguir sus objetivos. La Política también resalta la necesidad no solo de contar con capacidades para defenderse y recuperarse de los ciberataques, sino

[5] "Las autoridades de terceros países pueden emplear abusivamente el ciberespacio para ejercer vigilancia y control sobre sus propios ciudadanos. La UE puede contrarrestar esa situación fomentando la libertad en línea y velando por el respeto de los derechos fundamentales en la red". Párrafo incluido en la Estrategia de Ciberseguridad de la Unión Europea 2013 (Comisión Europea, 2013).

también de disuadirlos, prevenirlos y detectarlos (Comisión Europea, 2022,c). Para preparar a los Estados miembros en caso de un ciberataque y mejorar la cooperación entre los sectores público y privado, este documento también contempla el establecimiento de una serie de ejercicios de ciberdefensa de la UE.

En 2023, tras haber actualizado con anterioridad el marco político de ciberdefensa inicial de la Unión, se publicaron las Conclusiones sobre la política de ciberdefensa de la UE, con el objetivo de aumentar la resiliencia de los 27 miembros de la Unión. Esta política se apoya sobre 4 pilares. El primer pilar es la "acción común por una ciberdefensa reforzada", que hace referencia a la necesidad de una cooperación y coordinación por parte de todos los Estados Miembros frente a los ciberataques en relación a la Política Común de Seguridad y Defensa, llamando a una mayor formación y concienciación en el ámbito del ciberespacio. El segundo pilar hace referencia al "afianzamiento del ecosistema de defensa de la UE", por el cual se urge a las entidades militares, la industria de defensa y el sector privado a reforzar sus sistemas tecnológicos a fin de garantizar la seguridad en el ciberespacio de los ámbitos militar y civil sin depender de terceros, ayudando a la UE a convertirse en una organización autónoma a la hora de enfrentar los nuevos retos cibernéticos. Este afianzamiento considera la UE, se debe llevar a cabo armonizando las normativas referentes a las certificaciones y estándares de ciberseguridad. El tercer pilar hace referencia a la "inversión en capacidades de ciberdefensa" como factor de vital importancia para reducir las dependencias estratégicas y mantener una ventaja sobre los adversarios, haciendo hincapié en la necesidad de que sus capacidades esenciales evolucionen al mismo ritmo que los desarrollos tecnológicos. El último pilar está relacionado con "la asociación como forma de afrontar los retos comunes", en el que nombra las relaciones con la OTAN como fundamentales para reforzar la seguridad colectiva a través del diálogo y las consultas relativas al ciberespacio y la seguridad en este.

Entre los organismos que conforman la arquitectura cibernética de la Unión Europea se encuentran diferentes instituciones que están interrelacionadas entre sí y que se complementan en materia de ciberseguridad, con el objetivo de abordar la totalidad del ámbito cibernético. La Agencia de la Unión Europea para la Ciberdefensa, ENISA, garantiza la prevención y resiliencia de los sistemas con el objetivo de avalar la seguridad de los ciudadanos de la UE a través de la colaboración con organizaciones y empresas

intercambiando conocimientos y sensibilización entre otros, desarrollando normas y gestionando las certificaciones (ENISA, s.f.). Por otro lado, la UE cuenta con el CERT-EU, que es el Equipo de Respuesta ante Emergencias Informáticas para las Instituciones, Órganos y Organismos de la Unión Europea. Este organismo actúa como centro de respuesta rápida, siendo el primer respondedor en caso de un ciberataque sobre las Instituciones Europeas, emitiendo alertas tempranas, gestionando incidentes y coordinando la respuesta técnica ante ciberataques, permitiendo a su vez el intercambio de información (CERT-EU, s.f.). La Unión Europea también cuenta con la Agencia Europea de Defensa, EDA, que, aunque no esté orientada únicamente a la ciberdefensa, coordina e impulsa la cooperación militar de los 27 Estados, además de ofrecerles apoyo en el desarrollo de unidades militares especializadas en ciberdefensa. Además, la EDA cuenta con un programa de ejercicios de defensa cibernéticos, los CyDef-X, que se llevan a cabo con el objetivo de concienciar a los Estados Miembros para fortalecer la resiliencia de la UE frente a amenazas cibernéticas. (Sedivy, 2024).

Mientras que la EDA gestiona la parte operacional militar, el SEAE o Servicio Europeo de Acción Exterior, lidera el servicio diplomático de la UE con el objetivo de promover una política exterior más coherente y eficaz fortaleciendo así la influencia de la Unión en el ámbito internacional y desempeñando así un papel clave en la ciberdiplomacia (Unión Europea, s.f.). Por último, cabe destacar el Centro Europeo de Competencia en Ciberseguridad, ECCC, quien lidera la innovación y autonomía tecnológica de la UE en el ciberespacio, coordinándose con los centros nacionales para «construir una comunidad de ciberseguridad sólida» (ECCC, s.f.). Este centro tiene como función principal centralizar la gestión de los fondos europeos destinados al desarrollo de capacidades tecnológicas, coordinando la ciberdefensa y la ciberseguridad civil, actuando como puente entre el ámbito civil y militar y contribuyendo a la reducción de las dependencias tecnológicas estratégicas en terceros países, convirtiéndolo no solo en un centro de coordinación técnica, sino también en una herramienta estratégica para la soberanía digital europea.

5. ANÁLISIS Y DISCUSIÓN

Tras entender el papel que juegan la OTAN y la UE en el ámbito de la ciberdefensa, el marco sobre el cual elaboran su políticas y sus prioridades en el ciberespacio, en este apartado se busca analizar las similitudes y las diferencias de ambas organizaciones en su enfoque sobre la ciberdefensa, así como estudiar los acuerdos de cooperación y las relaciones reales que existe entre la OTAN y la UE para poder definir si se trata de una relación meramente cooperativa o si existe una dependencia de la UE sobre la OTAN en materia de ciberdefensa.

5.1 Similitudes y diferencias

A pesar de que la OTAN y la Unión Europea comparten ideas muy similares sobre cómo afrontar las amenazas en el espacio y fundamentos estratégicos de ciberdefensa, la forma en la que entienden su rol en la esfera internacional y sus capacidades implican que su enfoque a veces sea distinto. El objetivo principal de ambas organizaciones es proteger a sus Estados Miembros, pasando por su defensa en el ciberespacio de acuerdo a las directrices de la Organización de las Naciones Unidas, pero lo hacen desde estructuras, competencias y niveles de ambición diferentes. Este apartado busca entender en qué se diferencian y las implicaciones que esto tiene a la hora de guiar sus acciones defensivas en el ciberespacio.

Entre las similitudes en el enfoque sobre el ciberespacio comparten que ambos reconocen el ciberespacio como un dominio defensivo de vital importancia para la seguridad internacional, a la par que los dominios tradicionales como son la tierra, el mar, el aire y el espacio. Aunque la OTAN lo considere un espacio operativo y la UE un espacio estratégico, tanto como la OTAN como la Unión Europea consideran fundamental la cooperación para enfrentar las amenazas propuestas por este nuevo dominio, tanto entre los miembros de la propia organización, como entre organizaciones, y con el sector privado. Ambas organizaciones internacionales han ido adaptando sus estrategias en ciberdefensa con el paso de los años de manera frecuente, demostrando una gran flexibilidad y adaptabilidad a las amenazas y retos que surgen en el ciberespacio, basándose no solo en la evolución del Derecho Internacional sino también en casos como son el de Estonia o los ciberataques a Ucrania.

La Unión Europea y la OTAN han establecido marcos de cooperación en los que coinciden en varios puntos. El primero es que le dan un papel primordial al sector privado como un aliado de las Organizaciones Internacionales al tener unos recursos tecnológicos que les permiten desarrollar capacidades técnicas a las que estas organizaciones no llegan por motivos de financiación. Además, el sector privado cuenta con infraestructuras técnicas fundamentales que les permiten un exhaustivo estudio del ciberespacio, el cual puede no solo conducir hacia innovaciones normativas y militares, sino que también puede facilitar la detección de amenazas para prevenirlas y tener estrategias preparadas para enfrentarlas. En el caso de la OTAN, la cooperación con el sector privado se materializa, por ejemplo, a través de *Partners Run Locked Shields* 2025[6], en los que participa el sector privado entre otros actores (CCDCOE, 2025). La Unión Europea, lo hace en cambio siguiendo su línea más normativa e incluyendo en documentos como la Política de ciberdefensa de la UE publicada por la Comisión en 2022 la importancia de colaborar y cooperar con el sector privado en materia de ciberdefensa.

En segundo lugar, tanto la OTAN en su Concepto Estratégico del año 2022 como la Unión Europea en la Brújula Estratégica de 2022 mencionan a China y Rusia como países que pueden desestabilizar el orden internacional. Mientras que la OTAN plantea a China como una potencia cuyas «ambiciones y políticas coercitivas desafían nuestros [los de la OTAN] intereses, nuestra seguridad y nuestros valores» (OTAN, 2022b), la Unión Europea lo hace de forma más sutil, indicando que son unos «socios para la cooperación, un competidor económico y un rival sistémico» (Consejo de la Unión Europea, 2022), pero cuyo desarrollo debe estar supervisado para que no desestabilice el orden internacional desafianzando las normas ya establecidas. En el caso de Rusia, ambas organizaciones convergen en que su vulneración repetida del Derecho Internacional, mencionado por la UE, supone una alteración de la seguridad internacional, convirtiéndolo en una de las mayores amenazas de la que deben defender a sus Estados Miembros. El desarrollo de China y las crecientes capacidades y discriminadas agresiones de Rusia han puesto a ambos países en el punto de mira de estas organizaciones y de sus cuerpos defensivos y normativos de ciberseguridad y ciberdefensa.

[6] Los Locked Shields son ejercicios de ciberdefensa que simulan escenarios de ciberataques para preparar, probar y mejorar sus capacidades. En esta fase se involucró al sector privado entre otros y se les integró con organizaciones de defensa para ejemplificar la colaboración público-privada (CCDCOE, s.f.)

La gran diferencia radica en los pilares sobre los cuales se fundamenta cada organización. Por un lado, la OTAN fue creada desde su inicio en el año 1949 como una Alianza defensiva militar transcontinental, lo que implica que sea vista como una potencia militar en el ámbito internacional (Macorra, 2011). Que la Alianza cuente con estructuras como el SHAPE, que coordina las operaciones militares cuando son necesarias, permite a la OTAN tener la posibilidad de ejecutar operaciones militares reales, lo que implica que la disuasión de la Alianza sea resultado de sus capacidades militares. En cambio, la Unión Europea es la evolución de una comunidad económica que surge no en un momento de tensión militar, sino como respuesta al proceso de reconstrucción de una Europa devastada por las Guerras Mundiales, y cuyo objetivo es formar vínculos de unión entre los países del continente para garantizar la paz, proponiendo soluciones coordinadas que favorezcan la cooperación en la región y eviten conflictos. En este sentido, la Unión Europea es considerada una potencial civil que se caracteriza por su capacidad de influencia combinando herramientas normativa, diplomáticas y económicas para responder de manera integrada a las amenazas (Macorra, 2011). Esto implica que la disuasión de la Unión Europea frente a posibles amenazas externas no se basa en la utilización de fuerza militar directa, sino en instrumentos como las sanciones o el compromiso multilateral, añadiendo a su disuasión una connotación normativa basada en el respeto del Derecho Internacional y la defensa de los valores democráticos.

Estas diferencias hacen que los organismos y políticas de cada organización, aunque tengan un objetivo similar, se diferencien en puntos clave a la hora de afrontar la ciberdefensa de sus fronteras. Mientras que los organismos de la OTAN tienen una función operativa que les permite tener una respuesta que se materializa en diferentes acciones a la hora de afrontar un ciberataque, los de la Unión Europea tienen una especialización más técnica que permite elaborar un marco común de gobernanza, lo que permite regular la cooperación entre los Estados Miembros, pero no tienen la capacidad de ejecutar una defensa militar como lo puede hacer la OTAN. Ejemplo de ello es la diferencia entre las capacidades del NCIRC y el CERT-EU, ambos centros de respuesta ante emergencias o incidentes informáticos. Mientras que el NCIRC tiene la capacidad de identificar vulnerabilidades o amenazas y desplegar el Equipo de Reacción Rápida ante un ciberincidente en un Estado Miembro (OTAN, 2012), el CERT-EU realiza el análisis, la prevención y la coordinación de respuestas técnicas, no militares, en caso de que una institución de la Unión Europea sufra un ciberataque. Es decir, este organismo

asesora a las instituciones y les plantea planes de acción o directrices[7], pero no ejecuta las acciones, al contrario que el NCIRC que despliega los Equipos de Reacción Rápida, ejecutando así los planes de acción.

Otra gran diferencia que encontramos dentro de los organismos de ambas organizaciones debido al enfoque militar de la OTAN es que la Alianza cuenta con la Autoridad de Gestión de Defensa Cibernética de la OTAN, NCMA, un órgano militar y operativo centralizado que tiene autoridad para supervisar, coordinar y desarrollar las capacidades de ciberdefensa de la OTAN (Fuentes, 2022). Por el contrario, la Unión Europea no cuenta con ningún organismo que se asemeje a este. Igual que la OTAN cuenta con un organismo que recoge la acción ciberdefensiva, la UE no lo tiene, sino que es la suma de las acciones de diferentes organismos la que hace el papel de la NCMA en el caso de la OTAN. Se puede decir que, dentro de estructura institucional la UE, el organismo con mayor peso en la gestión ciberdefensiva es la Agencia Europea de Defensa, o EDA, la cual, a pesar de no llevar a cabo acciones militares directas sí que coordina el desarrollo de capacidades militares de los 27 Miembros de la UE, con un enfoque más estratégico y normativo. Las funciones que desarrolla la EDA se complementan con otros organismos como puede ser ENISA, que es la autoridad técnica en ciberseguridad de la EU, lo que implica que se ocupe del desarrollo de normas, de asesorar a los Estados Miembros y prepararlos a través de certificaciones de ciberseguridad o analizando las posibles amenazas y consiguiendo una cohesión de ciberseguridad entro de la UE (Tribunal de Cuentas Europeo, 2022). Se puede concluir así que la EDA gestiona la parte militar de la ciberdefensa en la UE mientras que ENISA se ocupa de la parte normativa, no teniendo ninguno de los dos organismos el poder operativo en la defensa de la Unión.

En conclusión, a pesar de tener un objetivo común: la defensa de sus Estados Miembros frente a las amenazas del ciberespacio, la Unión Europea y la OTAN han adoptado diferentes estrategias para hacerlas frente, siendo estas fiel reflejo de sus diferentes naturalezas institucionales y fundacionales. Mientras que la OTAN se guía por una postura defensiva que propone soluciones operativas, basada en capacidades

[7] "Las medidas de ciberseguridad han de especificarse con más detalle en directrices o recomendaciones emitidas por el CERT-EU". Contemplado en el Reglamento 2023/2841 del Parlamento Europeo y del Consejo del 13 de diciembre de 2023.

concretas, despliegue y disuasión colectiva, la Unión Europea tiene un enfoque más normativo para hacer frente a estas amenazas, desarrollando marcos normativos de acción común que inviten a la cooperación pero que dejan en manos de los Países Miembros responsabilidad última de ponerlos en marcha. Esta diferencia estructural se traduce en dos modelos de respuesta que pueden ser complementarios, pero no equivalentes, frente a los desafíos del ciberespacio, lo que llama a la cooperación entre la UE y la OTAN para poder beneficiarse de las fortalezas de la otra organización.

5.2 ¿Cooperación o dependencia?

"La realidad es que la OTAN es un instrumento, mientras que la UE, como Unión supranacional de Estados, es un actor" (Biscop, 2022). Esta frase de Sven Biscop, director de programa de Europa en el Mundo en el Instituto Egmont, en Bélgica, refleja de manera clara la imagen que se tiene de la supuesta cooperación entre la Unión Europea y la OTAN, la cual se asemeja más a una relación de dependencia por parte de la Unión Europea que a una relación entre iguales. Biscop ilustra a la UE como una actor que depende de la forma en la que la OTAN articule su estrategia ciberdefensiva, pues es quién verdaderamente tiene el poder operacional que permite proteger a los Estados Miembros. De los 27 países miembros de la Unión Europea, solo 4 no son miembros de la OTAN. Estos son Austria, Chipe, Irlanda y Malta. Este dato es uno de los indicadores más importantes para entender la razón por la que la UE depende estructuralmente de las capacidades estratégicas de la OTAN, condicionando entre otros la evolución de la ciberdefensa europea.

Tabla 1: Países Miembros de la UE que no son Miembros de la OTAN

PAIS	OTAN	UE
Alemania	x	x
Austria		x
Bélgica	x	x
Bulgaria	x	x
República Checa	x	x
Chipre		x
Croacia	x	x
Dinamarca	x	x
Eslovaquia	x	x
España	x	x
Estonia	x	x
Eslovenia	x	x
Finlandia	x	x
Francia	x	x
Grecia	x	x
Hungría	x	x
Irlanda		x
Italia	x	x
Letonia	x	x
Lituania	x	x
Luxemburgo	x	x
Malta		x
Países Bajos	x	x
Polonia	x	x
Portugal	x	x
Rumanía	x	x
Suecia	x	x

Fuente: creación propia[8]

Tanto la OTAN como la Unión Europea han hecho hincapié en sus diferentes políticas y conceptos estratégicos en que se conciben como socios fundamentales y su cooperación es primordial en materia de ciberdefensa para poder crear una comunidad internacional resiliente frente a las amenazas emergentes. Esta cooperación es posible gracias al reconocimiento de ambas organizaciones del ciberespacio como un ámbito clave para a seguridad colectiva. Las relaciones diplomáticas en materia de ciberseguridad entre ambas partes comenzaron en 2010 cuando empezaron a llevar a cabo consultas entre el personal especializado en ciberdefensa de ambas organizaciones durante reuniones informales, las cuáles se han convertido a día de hoy en una ocurrencia anual (European Union External Action, 2016).

La cooperación técnica en materia ciberseguridad se inició en el año 2016 cuando el Consejo de la UE y la OTAN refrendaron una serie de propuestas de acción comunes entre las que se encuentran algunas contempladas dentro del ámbito de la ciberseguridad. Esta cooperación se materializa a través de diálogos diplomáticos o en el intercambio de

[8] Datos obtenidos del Ministerio de Asuntos Exteriores, Unión Europea y Cooperación del Gobierno de España y del Servicio Público de Empleo Estatal del Gobierno de España.

información en tiempo real entre el NCIRC y el CERT-EU. El objetivo de esta cooperación es desarrollar en ambas organizaciones una capacidad mayor de prevención, detección y respuesta ante ciberataques (Fuentes, 2022).

Como se puede observar, tanto la UE como la OTAN son conscientes de que necesitan ser aliados en materia de ciberdefensa para poder cubrir un rango mayor en el ciberespacio que les permita estar preparados frente a las amenazas emergentes y poder no solo dar una respuesta rápida a estas en caso de materializarse, sino también prepararse para prevenir estas amenazas antes de que se materialicen. Además, su complementariedad, con la OTAN ofreciendo principalmente desarrollos y capacidades en defensa militar, y la UE poniendo a disposición de la Alianza capacidades normativas, diplomáticas y regulatorias, permite que su el papel disuasorio de ambas gane mayor peso a ojos de posibles actores que quieran desestabilizar el espacio euroatlántico. Ambas organizaciones son conscientes de la importancia que tiene la disuasión en el ciberespacio, pues la atribución la autoría del ataque es compleja debido a la anonimidad en la mayoría de los ciberataques, dificultando así la posibilidad de sancionar o exigir responsabilidades, por lo que se debe evitar que el ataque se ejecute en primer lugar.

Aunque en los documentos oficiales de ambas partes se trata la relación entre la OTAN y la UE como una de cooperación, la realdad es que, desde el punto de vista de Europa, esta colaboración es una necesidad estratégica fundamental para garantizar la seguridad de Europa en todos los ámbitos y en concreto en el de la ciberdefensa, ya que la UE carece de mecanismos reales operativos que puedan ofrecer una respuesta defensiva frente a un ataque. En la Brújula Estratégica de 2022 la Unión Europea expresó como el desarrollo europeo en materia de defensa complementa a la OTAN, la cual defienden «sigue siendo el pilar de la defensa colectiva de sus miembros» (Consejo de la Unión Europea, 2022). Aunque dejan entrever que la UE quiere complementar a la OTAN y no depender de ella, también son conscientes del papel principal que juega la OTAN actualmente en el ámbito defensivo, del cual admiten la Unión Europea depende. La propia OTAN, tras la publicación de la Declaración de la Cumbre de Gales, celebrada en el año 2014, se posicionó como el «marco transatlántico para una defensa colectiva y sólida» (OTAN, 2014).

Desde que el ciberespacio se convirtió en un dominio contemplado dentro del Derecho Internacional tras la publicación del "Tratado sobre los principios que deben regir las actividades de los Estados en la exploración y utilización del espacio ultraterrestre, incluso la Luna y otros cuerpos terrestres" en el año 1967 por parte de las Naciones Unidas, la OTAN siempre ha ido un paso por delante que la Unión Europea a la hora de poner en marcha mecanismos y estrategias para defenderlo. En el año 2002, la OTAN ya concebía el ciberespacio como un ámbito a defender y en el que defenderse de amenazas externas (Fuente, 2022). Fue la propia Alianza la que en el año 2013 impulsó la redacción de un documento que analiza cómo el Derecho Internacional se puede aplicar al ámbito del ciberespacio, en especial en relación con las ciberguerras, siendo este el marco dentro del cual se contemplan las acciones ciberdefensivas que están amparadas por la ley. Este documento se conoce como el Manual de Tallín y su redacción fue impulsada por el CCDCOE, y aunque no es un documento oficial, congrega las opiniones de expertos independientes que identifican no solo las normas existentes del derecho internacional que pueden aplicar al ciberespacio, sino también algunas normas que se deberían aplicar a los conflictos del ciberespacio (Ministerio de Defensa, 2013).

Esta dependencia defensiva de la UE se materializa en los respectivos artículos de defensa colectiva. Ambas partes reconocen los ciberataques como una posible agresión que puede conllevar la invocación de estas cláusulas, pero la respuesta y los requisitos que se deben cumplir para invocarlo varían. En el caso del Artículo 5 de la OTAN, principio fundacional de la Alianza, esta cláusula se puede activar en el caso de un ciberataque desde el año 2014 tras la Declaración de la Cumbre de Gales y reafirmado en el Comunicado de la Cumbre de Bruselas de 2021, mientras que en la UE la posibilidad de invoca el artículo 42.7 en caso de un ciberataque se contempla desde el año 2017 (Navarro, 2024).

Mientras que ambas cláusulas están sujetas al marco jurídico establecido con anterioridad en el Artículo 51 de la Carta de las Naciones Unidas y ambos apelan a que cada Estado Miembro preste asistencia en base a sus capacidades, cabe destacar el párrafo final del Artículo 42.7 del tratado de la UE. El párrafo dice lo siguiente: «Los compromisos y la cooperación en este ámbito seguirán ajustándose a los compromisos adquiridos en el marco de la Organización del Tratado del Atlántico Norte, que seguirá

siendo, para los Estados miembros que forman parte de la misma, el fundamento de su defensa colectiva y el organismo de ejecución de ésta». (BOE, 2010). Este párrafo ejemplifica como la Unión Europea depende en materia de defensa de la OTAN, ajustando su actuación al marco y a los intereses de la OTAN. Esta razón viene dada como consecuencia de la capacidad militar defensiva de la OTAN, con la cual la UE no cuenta.

Según el Tribunal de Cuentas, «en general, el nivel de preparación [de la Unión europea] no es proporcional a las amenazas». (Tribunal de cuentas, 2022). Esta afirmación es compartida por países como Suecia o Finlandia, que tras la invasión Rusia de Ucrania han visto sus fronteras más amenazas que nunca, y siendo conscientes de las capacidades defensivas de la OTAN buscan su adhesión para estar cubiertos por la cláusula de defensa colectiva de la Alianza, a pesar de ser ambos miembros de la Unión Europea y estar ya amparados bajo su cláusula de defensa mutua. Al contar la OTAN con capacidades militares, el poder disuasorio de la invocación de esta cláusula es mayor al del poder disuasorio de la Unión Europea, y los países europeos son conscientes de ello, pues la política diplomática y normativa de la UE no les sirve para defenderse frente a grandes actores.

5.3.Caso de estudio: Ucrania

Desde el inicio de la invasión de Ucrania en el año 2022, el conflicto se ha caracterizado, entre otros factores, por el lanzamiento de ciberataques por parte de Rusia sobre las instituciones gubernamentales, las redes energéticas o los sistemas de comunicación de la antigua República Soviética. Aunque Ucrania no sea un Estado Miembro ni de la OTAN ni de la UE, estas organizaciones internacionales juegan un papel fundamental en el conflicto, dando apoyo con sus capacidades tecnológicas para ayudar a Ucrania a hacer frente a los ataques cibernéticos rusos.

Debido a las dimensiones de la guerra, la declaración de cooperación entre la UE-OTAN que se publicó en el año 2022 se diferencia de la de 2018 en varios puntos. Esta declaración reitera una vez más la primacía de la OTAN en materia de defensa y se destaca una vez más el papel fundamental de la defensa colectiva que la Alianza ofrece. En la declaración se indica en varias ocasiones que se espera un desarrollo defensivo de la UE, pero siempre y cuanto este sea complementario al de la OTAN y no suponga una

amenaza para sus capacidades (Colin et al, 2023). En el marco disuasorio del conflicto, como se destaca en un documento publicado por el Real Instituto Elcano, la OTAN ofrece ventajas competitivas en los aspectos operativos y de ejecución directa de acciones disuasorias gracias a sus capacidades defensivas. En cambio, la Unión Europea es de mayor utilidad en las fases de inicio del conflicto gracias a sus competencias en investigación o tecnología (Simón, 2024).

Este argumento apoya una vez más la hipótesis de que las capacidades defensivas de la UE dependen de las de la OTAN, pues en el momento de ejecuta acciones ciberdefensivas la UE carece de instrumentos. Durante la guerra en Ucrania, la Unión Europea ha generado capacidades gracias a sus instrumentos financieros y normativos, pero ha sido la OTAN la que ha liderado las respuestas operativas, como la adhesión de Ucrania al CCDCOE, que permite a Ucrania formarse en materia de ciberdefensa y formar parte de los Locked Shields, siendo esta adhesión una declaración de intenciones de la OTAN a Rusia como arma de disuasión al mostrar su apoyo al país (CCDCOE, 2022). Fue el propio Putin el que en una entrevista declaró que «nos preocupaba la posibilidad de que Ucrania fuera incorporada a la OTAN, ya que representaba una amenaza para nuestra seguridad» (Putin, 2024). Por otro lado, las respuestas europeas se han centrado más en dar un apoyo técnico y económico a Ucrania más que una formación defensiva. Han puesto a su disposición un laboratorio cibernético que permite a Ucrania aumentar sus conocimientos y preparación en materia de ciberdefensa, siendo responsabilidad de Ucrania desarrollar sus capacidades (EEAS, 2022). Una vez más, se ve claramente que la OTAN cuenta con unas capacidades ciberdefensivas con las que puede ayudar a formar a los países para afrontar los ciberataques, mientras que la Unión Europea, al tener unas capacidades más limitadas en ese ámbito se limita a ofrecer apoyo financiero para que sean los países los que desarrollen sus capacidades ciberdefensivas.

6. CONCLUSIONES

La OTAN y la UE surgen desde dos visiones y necesidades estratégicas diferentes que han dirigido a cada organización a desarrollar una serie de capacidades que se adaptan a esta visión, lo que se ha traducido en que cada una cuenta con competencias diferentes en el ciberespacio. La actividad de ambas se rige por la Carta de las Naciones Unidas y sus conclusiones sobre el ciberespacio, creando así un marco de gobernanza global el cuál solo puede ser implementado a base de alianzas. Aunque el marco legislativo sea el mismo, la forma de cada organización de defender sus intereses y el Derecho Internacional es diferente. Esta diferencia nace de los diversos intereses y naturaleza de cada organización. Mientras que la OTAN se fundó como una alianza militar, la Unión Europea nace como foro para fomentar la unión económica de Europa, derivando en una unión política, social y diplomática, lo que conlleva que la Alianza por un lado tenga un papel más operativo y militar, mientras que la UE aporta capacidades tecnológicas y normativas.

El ciberespacio es un terreno operacional y estratégico muy reciente y por ello la comunidad internacional es consciente de la necesidad de colaborar para desarrollar capacidades que puedan proteger los países de las amenazas cibernéticas emergentes. Esta colaboración no debe ser simplemente a nivel estatal, sino que se debe involucrar también a las empresas del sector privado que operan en el ámbito del ciberespacio, pues sus desarrollos tecnológicos e infraestructuras son primordiales para el desarrollo de estrategias robustas en materia de ciberdefensa. A pesar de que la OTAN y la Unión Europea hayan demostrado su ambición por generar vínculos de cooperación en materia de ciberdefensa, tras el análisis realizado en esta investigación se puede afirmar que la Unión Europea depende en gran medida de las capacidades operativas en ciberdefensa de la OTAN. Esto no quiere decir que la UE no tenga capacidades ciberdefensivas ni que no sea un actor importante en la defensa en el ámbito del ciberespacio, sino que su enfoque más normativo y técnico tiene como consecuencia que, a la hora de materializar las estrategias ciberdefensivas, sea la OTAN la que toma las riendas de las operativas. Desde su inicio, la Unión Europea ha ido siguiendo los pasos de la Alianza, que ha tomado en todo momento la iniciativa en los desarrollos y las políticas relativas al ciberespacio.

La guerra en Ucrania ha sido ejemplo de la primacía de la Alianza en el ciberespacio y ha puesto en evidencia que la UE no puede hoy por hoy hacerse cargo de la defensa de sus Estados Miembros ni del continente europeo. Esta conciencia y las crecientes amenazas rusas llevó a países europeos como Finlandia y a Suecia a pedir su ingreso en la OTAN, el cual se formalizó en el año 2024, para estar protegidos bajo el marco de la defensa colectiva de la OTAN contemplada en el Artículo 5 del Tratado de Washington, a pesar de ser miembros de la Unión Europea y estar amparados por la cláusula de defensa mutua de la UE (Domecq, 2022). Cabe destacar que, en el caso de Finlandia, ya existía una cooperación estable en materia de ciberdefensa con la OTAN que se fortaleció en el año 2017, cuando aún no era un Estado Miembro de la Alianza, pero si lo era de la UE, lo que suponía que el país sí que estaba amparado por las estrategias ciberdefensivas europeas (OTAN, 2017).

Mientras que la OTAN desarrolla su papel de liderazgo en la guerra híbrida, la resiliencia y la seguridad energética, la UE sigue trabajando en convertirse en un actor de defensa creíble, lo que demuestra una vez más que, aunque la UE esté poniendo los medios para desarrollar sus capacidades militares aún no ha llegado al punto de ser autosuficiente, lo que implica la necesidad de una cooperación estrecha con la OTAN para cubrir los medios defensivos de los que los países europeos carecen (Colin et al, 2023). Estos resultados hacen que Europa, y en concreto la Unión Europea, sea consciente de la necesidad de desarrollar unas capacidades defensivas que les permitan ser autosuficientes y no depender de la política defensiva de la OTAN, la cual en gran medida se sustenta por las capacidades de Estados Unidos, y para ello deben desarrollar unas capacidades militares con las que no cuentan a día de hoy. La UE deja claro su deseo de una mayor autonomía en sus relaciones con la OTAN en documentos como la Política de Ciberdefensa de la UE del año 2022 y en la Brújula Estratégica del año 2022, en la que recalca que esta mayor autonomía defensiva favorecerá a la seguridad transatlántica, no solo europea, y complementará a las capacidades existentes de la OTAN (Consejo de la Unión Europea 2022).

Esta conciencia sobre la necesidad de una mayor autonomía europea se ha intensificado desde que el presidente del gobierno estadounidense Donal Trump, ha comenzado su segundo mandato y ha puesto en marcha su política "*America First*". Esta política busca priorizar los intereses nacionales de los Estados Unidos, los cuáles Trump defiende se están viendo amenazados por el excesivo gasto e implicación que los Estados

Unidos está teniendo en diferentes organizaciones internacionales, entre las que se encuentra la OTAN, esfuerzos que según el presidente estadounidense no se están viendo igualados por el resto de los Estados Miembros de la alianza. Es por ello por lo que Trump quiere incluir una condición para defender a los países de la Alianza: solo defenderá a aquellos cuyo gasto en defensa sea de al menos el 5% de su PIB (Lyons, 2025). Trump ha cambiado la estrategia de *soft power* que guiaba las decisiones dentro de la Alianza en un ambiente de diálogo y valores compartidos, por el *hard power,* por el que a través de amenazas busca un cambio en los países europeos en materia de defensa.

Estados Unidos se ve con la potestad de lanzar esta amenaza porque es consciente de la dependencia de los Miembros de la Alianza, mayoritariamente europeos, de las capacidades defensivas estadounidenses. 7 miembros de la Unión Europea están aún por debajo del 2% de inversión estipulado por la OTAN y ni si quiera los Estados Unidos tienen una inversión que supere el 4%, solo Polonia supera este valor (Merino, 2025). Es por ello por lo que este gasto en defensa resulta prácticamente inalcanzable para un gran número de países europeos. La inestabilidad de la defensa de la Alianza a consecuencia de las políticas nacionalistas de Donald Trump reafirma dentro de la Unión Europea la necesidad de crear una organización menos dependiente de las capacidades de la OTAN y más autosuficiente en el ámbito defensivo, lo que incluye el desarrollo de capacidades ciberdefensivas autónomas.

En conclusión, aunque la Unión Europea haya desarrollado unas capacidades normativas y técnicas sólidas en materia de ciberdefensa, a través de la creación de marcos regulatorios, la concienciación estratégica y la cooperación con organizaciones internacionales como la OTAN y con el sector privado, su capacidad operativa sigue siendo limitada. Esta limitación a obligado a la UE a apoyarse en la OTAN como principal garante de su defensa en el ciberespacio, dada la infraestructura militar, los mecanismos de respuesta inmediata con los que cuentan y el peso disuasorio de la Alianza. La UE es consciente de que existe una relación de dependencia y de la primacía de la OTAN en defensa colectiva. Es por ello que está trabajando para desarrollar unas capacidades que permitan al continente europeo ser autónomo y poder responsabilizarse de la defensa del continente, siempre de manera complementaria a la OTAN en el marco de la defensa.

7. BIBLIOGRAFÍA

Aicad. (2024). *Centro Integrado de Ciberdefensa: Estrategia de Ciberseguridad para la OTAN*. Aicad Business School. https://www.aicad.es/centro-integrado-de-ciberdefensa

Besch. S. (2018). *El compromiso cibernético de la OTAN*. Encompass. https://encompass-europe.com/comment/natos-cyber-pledge

Biscop. S (2022). *Agenda Exterior: OTAN y autonomía estratégica europea*. Política Exterior. https://www.politicaexterior.com/agenda-exterior-otan-y-autonomia-estrategica-europea/

BOE. (2010). Versión consolidada del Tratado de la Unión Europea. Boletín Oficial del Estado, Gobierno de España. https://www.boe.es/doue/2010/083/Z00013-00046.pdf

Carmés Vázquez. M (2000). *La OTAN: naturaleza, organización y financiación*. Boletin de Información, (266). https://dialnet.unirioja.es/servlet/articulo?codigo=4612272

Caro Bejarano. M. J. (2011). *Nuevo concepto de ciberdefensa de la OTAN*. Ministerio de Defensa, Instituto Español de Estudios Estratégicos, Dirección General de Relaciones Institucionales. https://dialnet.unirioja.es/servlet/articulo?codigo=7271583

CCDCOE. (2022). CCDCOE izó la bandera de Ucrania en solidaridad y apoyo. Centro Cooperativo de Excelencia en Ciberdefensa de la OTAN. https://ccdcoe.org/news/2022/ccdcoe-raised-the-ukrainian-flag-in-solidarity-and-support/

CCDCOE. (2025). El CCDCOE de la OTAN amplía la cooperación en ciberdefensa antes del mayor ejercicio con fuego real del mundo. Centro Cooperativo de Excelencia en Ciberdefensa de la OTAN. https://ccdcoe.org/news/2025/nato-ccdcoe-expands-cyber-defence-cooperation-ahead-of-the-worlds-largest-live-fire-exercise/

CERT-EU. (s.f.). About us. Equipo de Respuesta ante Emergencias Informáticas para las Instituciones, Órganos y Organismos de la Unión Europea: Bruselas. https://cert.europa.eu/about-us

Colin. W et al. (2023). *¿Tiene importancia la nueva Declaración conjunta UE-OTAN?* CSIS: Center for Strategic and International Studies. https://www.csis.org/analysis/does-new-eu-nato-joint-declaration-matter

Comisión Europea. (2022a). *La Unión Europea: ¿qué es y qué hace?* Comisión Europea: Dirección General de Comunicación. Oficina de Publicaciones de la Unión Europea. https://op.europa.eu/en/publication-detail/-/publication/c47b2296-b71a-11ed-

8912-01aa75ed71a1/language-es

Comisión Europea. (2022b). *Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro*. Comisión Europea, Alto representante de la Unión Europea para asuntos exteriores y política de seguridad: Bruselas. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013JC0001

Comisión Europea (2022c). *Política de ciberdefensa de la UE*. Comisión Europea, Alta representante de la Unión Europea para asuntos exteriores y política de seguridad: Bruselas. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022JC0049

Consejo de la Unión Europea. (2017). *Conclusiones del Consejo sobre la Comunicación Conjunta al Parlamento Europeo y al Consejo: Resiliencia, Disuasión y Defensa: construyendo una ciberseguridad sólida para la UE*. Consejo de la Unión Europea: Bruselas. https://www.consilium.europa.eu/media/31666/st14435en17.pdf

Consejo de la Unión Europea. (2022). *Una Brújula Estratégica para la Seguridad y la Defensa: por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e interese y contribuya a la paz y la seguridad internacionales*. Consejo de la Unión Europea: Bruselas. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf

Consejo de la Unión Europea (2024). *Ciberespacio: el Consejo adopta una Declaración sobre un entendimiento común de la aplicación del Derecho internacional en el ciberespacio*. Consejo de la Unión Europea: Bruselas. https://www.consilium.europa.eu/es/press/press-releases/2024/11/18/cyberspace-council-approves-declaration-to-promote-common-understanding-of-application-of-international-law/

Consejo de la Unión Europea. (s.f.). *Cooperación entre la UE y la OTAN*. Consejo de la Unión Europea: Bruselas. https://www.consilium.europa.eu/es/policies/eu-nato-cooperation/

Diccionario de la lengua española (s.f). *Diplomacia*. DEL, Real Academia Española, Asociación de Academias de la Lengua Española. https://dle.rae.es/diplomacia

DNS (2017). *La UE reforzará la ciberseguridad*. Departamento Nacional de Seguridad, Gobierno de España. https://www.dsn.gob.es/index.php/es/es/actualidad/sala-prensa/ue-reforzar%C3%A1-ciberseguridad

Domec. J. (2022). *Agenda Exterior: OTAN y autonomía estratégica europea*. Política Exterior. https://www.politicaexterior.com/agenda-exterior-otan-y-autonomia-

estrategica-europea/

ENISA (s.f). *Who we are*. European Union Agency for Cybersecurity: Atenas. https://www.enisa.europa.eu/about-enisa/who-we-are

EEAS. (2016). *EU and NATO increase information sharing on cyber incidents*. European Union External Action: The Diplomatic Service of the European, Union: Bruxelles. https://www.eeas.europa.eu/node/5253_en

EEAS. (2022), Ukraine: EU sets up a cyber lab for the Ukranian Armed Forces. European Union External Action: The Diplomatic Service of the European, Union: Bruxelles. https://www.eeas.europa.eu/eeas/ukraine-eu-sets-cyber-lab-ukrainian-armed-forces_en

Fuente Cobo. I. (2022). *La OTAN y el ciberespacio: un nuevo dominio para las operaciones*. Revista del Ejército de Tierra español, 972, abril 2022. https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/LaOTAN_ciberespacio.pdf

Gobierno de España. (s.f.). *¿Qué es la alianza atlántica, qué es la OTAN?* Gobierno de España: Ministerio de Asuntos Exteriores, Unión Europea y Cooperación. https://www.exteriores.gob.es/RepresentacionesPermanentes/otan/es/Organismo/Paginas/Que-es.aspx

García. R; Iglesias. L. (2022). *La ciberdefensa en el ámbito de la OTAN.* Academia de las Artes y las Ciencias Militares. https://www.acami.es/wp-content/uploads/2022/05/Ciberdefensa-ambito-OTAN-web.pdf

Gomichon, M. (2013). *Joseph Nye on Soft Power*. E-INTERNATIONAL RELATIONS. https://www.e-ir.info/2013/03/08/joseph-nye-on-soft-power/

IE. (2024). *NEXT GENERATION SECURITY: A study on how young Europeans perceive the defense sector*. IE University: center for the governance of change. https://static.ie.edu/CGC/Next%20Generation%20Security%20Report.pdf?_gl=1*k6ed5z*_gcl_au*MjEyMjkzNzIxMS4xNzQ5OTcyMDIx*_ga*MTUyODMwODE0NS4xNzQ5OTcyMDIx*_ga_Y7HB3S34Y5*czE3NDk5NzIwMjMkbzEkZzEkdDE3NDk5NzIwNTIkajMxJGwwJGgw*_fplc*blAwSGR6N1JxdkFKaXNIVHpBY2FkeHNwSjJBcEgyMjUxakd3d2wxb093OTVBYmZTSFVwOEVGc1dmNFlCR3pFYyUyRm50aEolMkZldEQzbWdjJTJGbnF5REhORXg3NUI4NDFkaHFyalNqRjhDZU85RHdVMUE4aXh6U1BQSTNybUVJdnFRJTNEJTNE

Illiuta. B. (2025). *La OTAN realiza un ejercicio para practicar la coordinación de apoyo frente a ciberataques de los países miembro*. El Radar. https://www.elradar.es/la-

otan-realiza-un-ejercicio-para-practicar-la-coordinacion-de-apoyo-frente-a-ciberataques-de-los-paises-miembro/

Kaspersky. (s.f.). *¿Qué es la ciberseguridad?* Kaspersky. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kasper, A., Osula, A. M., & Molnár, A. (2021). Ciberseguridad y ciberdiplomacia de la UE. IDP, 34, 1-15. https://raco.cat/index.php/IDP/article/view/n34-kasper/487930

Lyons. E. (2025). *Trump cuestiona la voluntad de los aliados de la OTAN de defenderse colectivamente mientras pone en duda el compromiso de Estados Unidos con el tratado*. CBS News. https://www.cbsnews.com/news/trump-nato-article-5-collective-defense-europe-doubt-us-treaty-commitment/

Macorra García. A. (2011). *OTAN-Unión Europea ¿qué relación existen realmente? Análisis del enfoque de fuerzas de reacción rápida*. Dialnet: Boletín de Información, ISSN 0213-6884, N. 320, 2011, pags 33-50. https://dialnet.unirioja.es/servlet/articulo?codigo=3850925

Merino. A. (2025). *El gasto en defensa de los países de la OTAN*. El Orden Mundial. https://elordenmundial.com/mapas-y-graficos/gasto-defensa-paises-otan/

Ministerio de Defensa. (2013). *Publicación del Manual de Tallín sobre "Ley Internacional en la Ciberguerra"*. Ministerio de Defensa, Gobierno de España. https://www.tecnologiaeinnovacion.defensa.gob.es/es-es/Contenido/Paginas/detallenoticia.aspx?noticiaID=59

Ministerio de Defensa (2022). *Nuevo Concepto Estratégico de la OTAN*. Ministerio de Defensa, Gobierno de España: Madrid. https://www.defensa.gob.es/Galerias/main/nuevo_concepto_estrat_gico_de_la_otan.pdf

Morillas. P. (2015). *El 42.7: Cobertura Europea para la defensa francesa*. CIDOB. https://www.cidob.org/sites/default/files/2024-09/366_OPINION_POL%20MORILLAS_CAST.pdf

Naciones Unidas (1945). *Carta de las Naciones Unidas*. Organización de las Naciones Unidas. https://www.un.org/es/about-us/un-charter

Naciones Unidas. (2002). *Tratados y principios de las Naciones Unidas sobre el espacio ultraterrestre*. Naciones Unidas: Nueva York. https://www.unoosa.org/pdf/publications/STSPACE11S.pdf

Navarro. P. (2024). A Comparative Study of Article 5 of the NATO and Article 42(7) Of the Treaty on The European Union: Its Scope and Limits. Finabel. https://finabel.org/wp-content/uploads/2024/02/61.A-comparative-study-of-article-4.pdf

Nye. J. (2016). *Soft Power: The Means to Success in World Politics. Chapter 4: Wielding Soft Power*. Belfer Center for Science and International Affairs: Harvard Kennedy School. https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/joe_nye_wielding_soft_power.pdf

Osorio Lalinde, A., Lorduy López, G., Amaya Henao, L. M., & Arenas Méndez, T. (2017). *Ciberseguridad y ciberdefensa: pilares fundamentales de la seguridad y defensa nacional*. Revista De Las Fuerzas Armadas, (241), 6–14. https://doi.org/10.25062/0120-0631.823

OTAN. (2008). *Tratado del Atlántico Norte*. Organización del Tratado del Atlántico Norte. https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=es

OTAN. (2012). *Equipo de Reacción Rápida de la OTAN para combatir ciberataques*. Organización del Tratado del Atlántico Norte. https://www.nato.int/cps/en/natolive/news_85161.htm

OTAN. (2014). *Declaración de la Cumbre de Gales*. Organización del Tratado del Atlántico Norte. https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease

OTAN. (2016). *Compromiso de ciberdefensa*. Organización del Tratado del Atlántico Norte. https://www.nato.int/cps/en/natohq/official_texts_133177.htm#:~:text=In%20recognition%20of%20the%20new,on%20land%20and%20at%20sea.

OTAN. (2017). *La OTAN y Finlandia intensifican su cooperación en ciberdefensa*. Organización del Tratado del Atlántico Norte. https://www.nato.int/cps/en/natohq/news_141464.htm

OTAN. (2022a). *Founding treaty*. Organización del Tratado del Atlántico Norte. https://www.nato.int/cps/en/natohq/topics_67656.htm

OTAN. (2022b). *Concepto Estratégico de la OTAN 2022*. Organización del Tratado del Atlántico Norte. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

OTAN. (2023). *Toma de decisiones por consenso en la OTAN*. Organización del Tratado del Atlántico Norte. https://www.nato.int/cps/en/natohq/topics_49178.htm

OTAN. (2024). *Ciberdefensa*. Organización del Tratado del Atlántico Norte. https://www.nato.int/cps/en/natohq/topics_78170.htm#:~:text=NATO's%20policy%20o

n%20cyber%20defence&text=Allies%20reaffirmed%20NATO's%20defensive%20mandate%20and%20committed%20to%20employing%20the,including%20by%20considering%20collective%20responses.

Pardo, G. (s.f.). *¿Qué es la ciberdiplomacia?* Instituto Mediterráneo de Estudios de Protocolo. https://www.protocoloimep.com/diplomacia-publica/que-es-la-ciberdiplomacia/

Putin. V. (2024). *Respuestas a las preguntas del periodista Pavel Zarubin*. Presidente de Rusia. http://en.kremlin.ru/events/president/news/73457

Rieger, B. (2022). *El Artículo 5, la cláusula de asistencia mutua de la OTAN*. DW. https://www.dw.com/es/qu%C3%A9-dice-el-art%C3%ADculo-5-la-cl%C3%A1usula-de-asistencia-mutua-del-tratado-de-la-otan-y-en-qu%C3%A9-se-diferencia-del-art%C3%ADculo-4/a-63782748

S2GRUPO. (2025). Ciberdefensa y ciberseguridad: la gestión de la seguridad de la información. S2GRUPO. https://s2grupo.es/ciberdefensa-y-ciberseguridad-la-gestion-de-la-seguridad-de-la-informacion/

Schmitt, M.N (2014). The law of cyberwarfare: quo vadis? Stanford Law School. https://law.stanford.edu/wp-content/uploads/2018/03/schmitt.pdf

Sedivy. J. (2024) EDA Annual Repport 2024. European Defence Agency: Brussels. https://eda.europa.eu/docs/default-source/brochures/eda---annual-report-2024---webdfcdc23fa4d264cfa776ff000087ef0f.pdf

Simón. L. (2024), Una reflexión sobre las relaciones OTAN-EU en tiempos de guerra. Real Instituto Elcano. https://media.realinstitutoelcano.org/wp-content/uploads/2024/05/ari71-2024-simon-relaciones-otan-ue-en-tiempos-de-guerra.pdf

Tribunal de Cuentas Europeo (2022). *Ciberseguridad de las instituciones, órganos y organismos de la UE*. Tribunal de Cuentas Europeo. https://www.eca.europa.eu/Lists/ECADocuments/SR22_05/SR_cybersecurity-EU-institutions_ES.pdf

Unión Europea. (2016). *Tratado de la Unión Europea*. Unión Europea. https://eur-lex.europa.eu/eli/treaty/teu_2016/art_42/oj

Unión Europea (s.f.). *Servicio Europeo de Acción Exterior (SEAE).* Unión Europea: Bruselas. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-external-action-service-eeas_es

UNOOSA. (s.f). *Historia*. Oficina de las Naciones Unidas para Asuntos del Espacio

Ultraterrestre. https://www.unoosa.org/oosa/en/aboutus/history/index.html

Vallejo, G.D. (2023). *Las generaciones de la guerra y la modificación de la doctrina de base: Reversión del "Arte de la Guerra"*. Instituto Internacional de Estudios en Seguridad Global. https://ciia-historia-militar.iniseg.es/administracion/public/uploads/adjuntos/las-generaciones-de-la-guerra-y-la-modificacion-de-la-doctrina-de-base-reversion-del-arte-de-la-guerra.pdf%22Arte%20de%20la%20Guerra

Villamar. Z.N (2017). *Gobernanza Global y (su propio) desarrollo*. Revista de Relaciones Internacionales de la UNAM, (127). https://www.revistas.unam.mx/index.php/rri/article/view/61149

ANEXO I: Declaración de Uso de Herramientas de IA Generativa en Trabajos Fin de Grado

Por la presente, yo, Patricia Ruiz Ledesma, estudiante de Relaciones Internacionales de la Universidad Pontificia Comillas al presentar mi Trabajo Fin de Grado titulado " El papel de la OTAN en la ciberdefensa europea: ¿Cooperación o dependencia de la Unión Europea?", declaro que he utilizado la herramienta de IA Generativa ChatGPT u otras similares de IAG de código sólo en el contexto de las actividades descritas a continuación:

1. **Sintetizador y divulgador de libros complicados**: Para resumir y comprender literatura compleja.

2. **Traductor**: Para traducir textos de un lenguaje a otro.

Afirmo que toda la información y contenido presentados en este trabajo son producto de mi investigación y esfuerzo individual, excepto donde se ha indicado lo contrario y se han dado los créditos correspondientes (he incluido las referencias adecuadas en el TFG y he explicitado para qué se ha usado ChatGPT u otras herramientas similares). Soy consciente de las implicaciones académicas y éticas de presentar un trabajo no original y acepto las consecuencias de cualquier violación a esta declaración.

Fecha: 16 / 6 / 2025

Firma: Patricia Ruiz Ledesma