**FACULTAD DE DERECHO**
**UNIVERSIDAD DE LEÓN**
**CURSO 2022 / 2023.**

# LA CIBERDEFENSA EN LA UNIÓN EUROPEA.

# THE CYBERDEFENSE IN THE EUROPEAN UNION.

## MÁSTER EN DERECHO DE LA CIBERSEGURIDAD Y ENTORNO DIGITAL

AUTOR: D. JAVIER MARTÍN GÓMEZ.

TUTORA: DRA. MARÍA DE LAS MERCEDES FUERTES LÓPEZ.

# ÍNDICE

**ABREVIATURAS Y ACRÓNIMOS.**

| | |
|---|---|
| **AED** | Agencia Europea de Defensa. |
| **BITDE** | Base industrial y tecnológica de la defensa europea |
| **CCDCOE** | Centro de Excelencia para la Ciberdefensa Cooperativa. |
| **CERT** | Equipo de Respuesta para Emergencias Informáticas. |
| **CERT UE** | Equipo de respuesta a emergencias informáticas para las instituciones europeas y organismos de la UE. |
| **CIDCC** | Centro de Coordinación del ámbito del Ciberespacio y de la Información. |
| **COS** | Centros de Operativos de Seguridad. |
| **CSIRT** | Equipos de Respuesta a Incidentes de Seguridad Informática. |
| **CTISP** | Respuestas a Ciberamenazas e Incidentes de Ciberseguridad. |
| **CyCLONe** | Red de Organizaciones de Enlace de Crisis Cibernéticas de la UE. |
| **DIANA** | Acelerador de Innovación de Defensa del Atlántico Norte. |
| **ECSF** | Marco Europeo de Habilidades en Ciberseguridad. |
| **EDSIS** | Sistema Europeo de Información sobre Normalización de la Defensa. |
| **EDSTAR** | Sistema Europeo de Referencia de Estándares de Defensa. |
| **EEMM** | Estados Miembros. |
| **EES** | Estrategia Europea de Seguridad. |
| **EESD** | Escuela Europea de Seguridad y Defensa. |
| **ENISA** | Agencia de la Unión Europea para la Ciberseguridad. |
| **EU INTCEN** | Centro de Inteligencia y de Situación de la UE. |
| **FED** | Fondo Europeo de Defensa. |
| **HEIDI** | Centro para la Innovación de Defensa de la UE. |
| **NCIRC** | Capacidad de Respuesta a Incidentes Informáticos de la OTAN |
| **ONU** | Organización de las Naciones Unidas. |
| **OSCE** | Organización para la Seguridad y la Cooperación en Europa |

| | |
|---|---|
| **OTAN** | Organización del Tratado del Atlántico Norte. |
| **PCSD** | Política Común de Seguridad y Defensa. |
| **PESD** | Política Exterior de Seguridad y Defensa. |
| **SEAE** | Servicio Europeo de Acción Exterior. |
| **TFUE** | Tratado de Funcionamiento de la Unión Europea. |
| **TIC** | Tecnologías de la Información y las Comunicaciones. |
| **TUE** | Tratado de la Unión Europea. |
| **UE** | Unión Europea. |
| **UE CAIH** | Centro de la Unión Europea para el mundo académico y la innovación en el ámbito del ciberespacio. |

**RESUMEN.**

Debido un aumento exponencial de ciberataques y ciberamenazas en los últimos años en el entorno de la UE, es indispensable contar con una ciberdefensa puntura, es decir, que cuente con las herramientas e instrumentos de última generación para así ofrecer un ciberespacio seguro tanto a sus ciudadanos, instituciones y empresas. Asimismo, resulta imprescindible una cooperación no solamente entre los propios EEMM sino también con socios externos, que a priori cuenten con valores e intereses similares con la UE.

Sin embargo, para alcanzar los objetivos marcados por la UE, no solamente sería necesarios instrumentos o profesionales técnicos, sino también unos mecanismos jurídicos que nos permitan actuar en caso de que la ciberdefensa de la UE se vea comprometida o llegue a ser atacada como es la cláusula de solidaridad y cláusula de defensa mutua

**Palabras clave:** ciberataque, ciberamenaza, ciberdefensa, ciberespacio, cooperación, cláusula de solidaridad y cláusula de defensa mutua.

**ABSTRACT**

Due to an exponential increase in cyber-attacks and cyber-threats in recent years in the EU environment, it is essential to have a timely cyber-defense, one that has the latest generation of tools and instruments to offer a secure cyberspace to its citizens, institutions and companies. Cooperation is also essential not only between the Member States themselves but also with external partners, which a priori have similar values and interests to the EU.

However, to achieve the objectives, set by the EU, not only technical instruments or professionals are needed, but also legal mechanisms that allow us to act in the event

that the EU's cyber defense is compromised or attacked, such as the solidarity clause and the mutual defense clause.

**Keywords:** cyber-attack, cyber-threat, cyber-defense, cyberspace, cooperation, solidarity clause and mutual defense clause.

**OBJETO DEL TRABAJO.**

El objeto principal del trabajo es buscar la forma de acercar la ciberdefensa al mundo jurídico, concretamente al entorno de la Unión Europea. Para lograr este objetivo ha sido necesario establecer tres peldaños, sin olvidar el punto introductorio.

Al principio se realiza una andadura por los diferentes dominios de combate hasta llegar al ciberespacio, escenario en el que son protagonistas la ciberseguridad y ciberdefensa, en la que se establece el ejemplo de la fortaleza, por el cual se observa a través un caso práctico las diferencias existentes entre estas dos disciplinas y en la que se da una definición de esta última, atendiendo a los diferentes documentos elaborados por los expertos.

En el primer punto, se hace un recorrido cronológico de los diferentes antecedentes que se han ido dando a lo largo de los años hasta conformar la política de ciberdefensa que se tiene la UE en la actualidad y de los instrumentos que posee. Asimismo, también se ha explicado con algo más de profundidad aquellos elementos jurídicos verdaderamente relevantes para la ciberdefensa como son: la estrategia de ciberseguridad de 2013, la política de ciberdefensa de 2014, la comunicación sobre la resiliencia, disuasión y defensa para fortalecer la ciberseguridad de la UE, la cooperación estructurada permanente y finalmente actualización de la política de ciberdefensa en 2018.

En segundo lugar, me inmiscuyo directamente en la política de ciberdefensa vigente hoy en día, la de noviembre de 2022, considerando este punto como el elemento central del trabajo, en el que se recorre de una forma precisa cada uno de los pilares que la conforman y aportando a su vez posibles instrumentos que podrían entrar en juego en un futuro, para así mejorar la aplicación de dicha política y hacer frente de una forma más adecuada y eficaz a los ciberataques y ciberamenzas de los enemigos.

Y en último lugar, me adentro en los principales mecanismos que posee la Unión Europea, cláusula de solidaridad y cláusula de defensa, en caso de que reciba un ciberataque. Pues bien, además de analizar cada uno de estos mecanismos también se determina cuando es conveniente aplicar uno u otro, indicándose cuáles son sus diferencias y comparándolo con otra herramienta como es el art. 5 del Tratado de Washington.

**METODOLOGÍA.**

En la elaboración del presente trabajo se expone como se estructura la actual política de ciberdefensa de la Unión Europea y los diferentes instrumentos y herramientas que tiene para defenderse de actores externos. En este sentido, se ha seguido una estructura metodológica organizada de manera que sea más fácil la compresión de dicha investigación.

Primeramente, es necesario retroceder al punto de partida, es decir, a la elección del tema. Pues bien, esta cuestión puede resultar un gran desafío para un estudiante que tenga que hacer por primera vez un trabajo de estas características, no siendo este mi caso, ya que en el Trabajo Final de Grado que elaboré, en cierta medida, tiene relación con el asunto a tratar, como es la política antiterrorista en la Unión Europea.

En este contexto, no me resultó muy complicado la elección del tema, ya que a través una investigación previa por mi parte y atendiendo a las clases dadas por profesionales externos a la Universidad de León en las que mencionaron este tema y su importancia, pues reafirmaron aún más mi idea de realizar mi trabajo sobre este asunto.

Una vez que tenía la certeza que iba a realizar el trabajo sobre este tema, se lo comenté a mi tutora, Dra. Mercedes Fuertes, que no solamente le pareció muy interesante, sino que también me motivó a ello y me suministró una gran cantidad de información sobre el tema, la cual ha sido imprescindible para realizar el trabajo.

Por último, con la ayuda de mi tutora comencé a recopilar información de diversas fuentes, sobre todo, portales webs, artículos de revistas especializadas y manuales teóricos elaborados por expertos en ciberdefensa en el ámbito jurídico. Asimismo, ha sido necesario acudir una copiosa legislación comunitaria conformado por el derecho originario y el derecho derivado.

**INTRODUCCIÓN.**

Tradicionalmente la tierra y el agua han sido los dos campos de batalla en los que empezó a combatir el ser humano y a lo largo de los siglos sus tácticas, técnicas y procedimientos han ido evolucionando.

En el S. XX aparece un nuevo campo de batalla, el aire, el cual ha tenido un gran empuje a finales del siglo pasado y lo que llevamos de éste. Se consideró que la comunicación satelital se convirtió en nuevo escenario, el cual las naciones explotan para la extensión del mando, control y la vigilancia de las capacidades de inteligencia del enemigo.

Tras la Cumbre de la OTAN de Varsovia de 2016, los Jefes de Estado y de Gobierno de las naciones de la OTAN consideran y reconocen el ciberespacio como un quinto escenario, pues las operaciones militares que se realizan en el ciberespacio son transversales al resto de los dominios de tierra, mar, aire y espacio, ya que las acciones llevadas a cabo en este dominio repercuten directamente en los sistemas que operan en estos dominios[1].

El grado de dependencia de la sociedad europea respecto de las Tecnologías de la Informaciones y Comunicaciones (en adelante TIC) y el ciberespacio cada día crece más, por lo que resulta necesario conocer sus amenazas y darles una respuesta adecuada.

En este sentido, el ciberespacio se ha convertido en un escenario idóneo para llevar cabo ciberamenazas y ciberataques debido a una serie de características que presenta, entre ellas: carece de fronteras; hay una infinidad de actores (ciberespias, ciberdelincuentes, ciberterroristas, hacktivistas, script kiddies, etc.); el entrono legal es muy complejo, a pesar de que hay determinados aspectos que se está intentando regular,

[1] DEPARTAMENTO DE SEGURIDAD NACIONAL. *Acuerdo Cyber Pledge de la OTAN* [en línea]. Fecha de consulta: 19 de junio de 2023. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/acuerdo-cyber-pledge-otan

pero para ello es necesario no solamente la voluntad de las naciones, organizaciones supranacionales, como la UE, sino un compromiso mundial: y por último, no solamente afecta a un ámbito en concreto sino, que atañe a diversos ámbitos, desde compañías energéticas, pasando por la sanidad, educación o justicia, por ende ataca al corazón las naciones, o en este caso de la UE, que no es otro que los ciudadanos.

En este contexto, las operaciones que se llevan a cabo en el ciberespacio son las siguientes: seguridad cis, operaciones defensivas, operaciones de respuesta defensiva, operaciones de vigilancia y reconocimiento y las operaciones defensivas[2].

La seguridad cis es equivalente a la ciberseguridad, ahora bien, cabría hacerse varias preguntas ¿quién se encargaría del bastionado de la red? En este caso la autoridad operativa del sistema apoyándose en sus administradores, que llevarían a cabo una serie de acciones preventivas de protección y de recuperación en el caso de que se cayeran las redes. Además, efectuaría una ardua labor como la prevención, análisis de riesgo, parcheo de vulnerabilidades, limitación de privilegios, políticas de seguridad, segmentación de redes, y, por último, tener una política de backups para restaurar los sistemas que han sido dañados.

En este punto, cabría traer a colación el termino operaciones defensivas, que es el conjunto de medidas y acciones encaminadas a detectar, identificar, interceptar, rechazar y neutralizar todo tipo de ataques o intento de penetración en el área de operaciones de ciberdefensa. Se llevaría una serie de medidas de respuesta interna para evitar que el enemigo no pueda entrar y realizar cualquier tipo de ataque o daño, siendo algunas de estas medidas las siguientes: monitorización, gestión de incidentes, y desde un punto de vista de respuesta se tendría: la infiltración, perturbación, denegación de servicios del

[2] CENTRO CRIOPOLÓGICO NACIONAL. *Planeamiento de Operaciones en el Ciberespacio I (Capitán de Corbeta Santos Sande, MCCD)* [video]. Fecha de consulta: 19 de junio de 2023. Disponible en: https://www.youtube.com/watch?v=zFWr7p09AMs

enemigo para que no pueda seguir actuando. Asimismo, hay que destacar que la capacidad de respuesta ante ese ataque tiene que ser legítima, proporcional y legal.

A continuación, es necesario realizar una breve diferencia entre ciberdefensa y ciberseguridad. En este caso, la Comisión Europea declaró *"la falta de definición de la frontera entre ciberdefensa y ciberseguridad"*[3]. En este sentido, la ciberdefensa ha sido definida por el Parlamento Europeo como el análisis de amenazas y estrategias para proteger a los ciudadanos, instituciones y gobiernos de las amenazas dirigidos contra ellos[4]. Siguiendo con este breve análisis, se ha determinado que la ciberdefensa es un concepto mucho más amplio que el de ciberseguridad, a pesar de que este último también incluya la seguridad de la información y de las telecomunicaciones, la tecnología operativa y las plataformas de las tecnologías de la información necesarias para los activos digitales[5].

Para finalizar este punto y que sea mucho más clara la diferenciación entre la ciberseguridad y ciberdefensa es necesario traer a colación el esquema de fortaleza[6]. La creación de una fortaleza es responsabilidad de la ciberseguridad, que tendrá que crear muros más altos y anchos, beneficiando así el bastionado de la red para evitar o disuadir al enemigo, pero cuando el enemigo empieza a atacar ¿quién lucha contra el enemigo? pues bien, aquí es donde entra en juego la ciberdefensa.

En este escenario habría diferentes actores, por un lado, los vigías, que se encargarían de monitorizar y de ver lo que hay alrededor, a continuación, las catapultas y las defensas que mantendrían la distancia con el enemigo, como pueden ser los firewalls, por otro lado,

[3] Comunicación Conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE. Bruselas 13 de noviembre de 2017, JOIN (2017) 450 final, pp.19. Fecha de consulta: 19 de junio de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017JC0450&from=es

[4] PARLAMENTO EUROPEO. *Cyber: How big is the threat?* [en línea]. Fecha de consulta: 19 de junio de 2023. Disponible en: https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

[5] PARLAMENTO EUROPEO. Cyber: How big is the threat? *..., op. cit.,* pp. 1.

[6] CENTRO CRIOPOLÓGICO NACIONAL. *Planeamiento de Operaciones en el Ciberespacio I ..., op. cit.*

los IDS e IPS, que se encargarían del control de acceso, es decir, identificarían al enemigo para que no entre dentro de la fortaleza, es decir, de la red, después, la infantería, que sería el antivirus, se encargaría de luchar contra el enemigo, y por último, se tendría al SIEM, el comandante de la guardia, que estudia el campo de batalla y ve cómo va evolucionando.

## 1. EL PASADO DE LA CIBERDEFENSA DE LA UE.

### 1.1. Antecedentes.

En 2003 se aprobó la Estrategia Europea de Seguridad (en adelante EES), siendo un acontecimiento de referencia en la se exponen los desafíos, amenazas y objetivos a los que estaba expuesta Europa debido al protagonismo alcanzado por agentes no estatales. En concreto, las principales amenazas que destaca esta estrategia son: el terrorismo internacional, la proliferación de armas de destrucción masiva, los conflictos regionales, la descomposición del Estado y la delincuencia organizada.

En 2004, un año más tarde, el Reglamento 460/2004[7] crea la Agencia de la UE para la ciberseguridad (en adelante ENISA) con el objetivo de afianzar el sector de las redes y sistemas de información tras los numerosos perjuicios económicos derivados de fallos de seguridad, convirtiéndose la ciberseguridad en un asunto transcendental en el paradigma europeo. Además, es importante destacar que estimuló la creación del Programa Europeo de Protección de Infraestructuras Críticas en 2007[8], que para la ciberdefensa es un ámbito fundamental.

La EES presentaba una serie carencias formales y conceptuales, que iban desde la falta de elementos imprescindibles que aportaban tanto el Tratado de Lisboa como la

[7] Reglamento (CE) n° 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información. Diario Oficial de la Unión Europea L 77, 13.03.2004, 99, pp. 1-11. Fecha de consulta: 24 de mayo de 2023. Disponible en: http://data.europa.eu/eli/reg/2004/460/oj

[8] MACHIN OSÉS, Nieva y GAZAPO LAPAYESE, Manuel. La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI*. 2016, n.º 42, pp. 47-68.

Política Común de Seguridad y Defensa (en adelante PCSD), de los cuales se derivan los posibles ataques cibernéticos que se puedan dar[9].

Frente a las diversas carencias que se hallaron, lo más lógico hubiera sido sustituir o realizar una nueva estrategia, pero en su defecto se aprobó en 2008 el Informe sobre la aplicación de la EES[10] que, a pesar de mejorar la aplicación de dicha estrategia con la contribución de diferentes propuestas para incrementar la eficacia de la política europea de defensa y la cooperación entre las instituciones de la Organizaciones de Naciones Unidas (en adelante ONU) y la UE, solo sirvió para prorrogar la vigencia de la Estrategia de 2003, quedando totalmente obsoleta, de manera que era conveniente adoptar una nueva estrategia[11].

Dos años más tarde, en 2010, bajo la presidencia española se adoptó la Estrategia de Seguridad Interior[12] que fue aprobada los días 25 y 26 de marzo por el Consejo Europeo. Esta nueva estrategia señala las principales amenazas a las que tiene que hacer frente la UE, que se ven fortalecidas por las condiciones que genera la sociedad globalizada, siendo un claro ejemplo de ello la cuestión de la ciberseguridad, en la que se incluye la ciberdelincuencia como una amenaza para los sistemas de información y un reto para las autoridades policiales.

Asimismo, en 2010, la Comisión Europea lanzó la Estrategia Europa 2020[13], cuya finalidad era afrontar los retos económicos de la próxima década. Entre las siete

[9] RUBIO DAMIÁN, Francisco. Necesidad de una nueva estrategia europea de seguridad. *Revista Ejército.* 2012, n.º 860, pp. 6-10.
[10] Informe sobre la aplicación de la Estrategia Europea de Seguridad. Ofrecer seguridad en un mundo de evolución. Bruselas, 11 de diciembre de 2008, S407/08. Fecha de consulta: 24 de mayo de 2023. Disponible en: https://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/ES/reports/104637.pdf
[11] RUBIO DAMIÁN, Francisco. Necesidad de una…, *op. cit.*, pp. 9-10.
[12] Comunicación de la Comisión al Parlamento Europeo y al Consejo. La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura. Bruselas, 22 de noviembre de 2010, COM(2010) 673 final. Fecha de consulta: 24 de mayo de 2023. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:ES:pdf
[13] Comunicación de la Comisión. Europa 2020. Una estrategia para un crecimiento inteligente, sostenible e integrado. Bruselas, 3 de marzo de 2020, COM(2010) 2020 final. Fecha de consulta: 24 de mayo de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52010DC2020

propuestas que se encontraban en dicha estrategia destacó la Agenda Digital para Europa[14] que tenía como objetivo incrementar al máximo la capacidad de las TIC en el ámbito económico y social, y como no podía ser de otra manera se vaticinaba la creación de un equipo de respuesta a emergencias informáticas para las instituciones europeas y organismos de la UE (en adelante CERT UE) para que se diese una coordinación con equipos similares en los Estados Miembros (en adelante EEMM)[15].

### 1.2.Estrategia de ciberseguridad de la UE de 2013.

En años anteriores a 2013 ya eran conocidas tanto las vulnerabilidades que presentaban ciertos dispositivos (Internet de las cosas) como los daños que podrían producir el uso de la inteligencia artificial en caso de que cayeran en malas manos[16]. En este sentido, para enfrentarse a la gran problemática del incremento de los ciberataques, se aprobó el 7 de febrero de 2013 la Estrategia de Ciberseguridad Europea con el objetivo de alcanzar un ciberespacio abierto, protegido y seguro, siendo este el documento donde se ubica el origen de la ciberdefensa en la UE[17].

Presenta una serie de prioridades y medidas estratégicas para afrontar los problemas que se derivan de la inseguridad en el ciberespacio:[18] lograr la ciberresiliencia,

---

[14] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las regiones. Agenda Digital para Europa. Bruselas, 19 de mayo de 2010, COM(2010)245 final. Fecha de consulta 24 de mayo de 2023. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:es:PDF

[15] Comunicación COM(2010) 245 final, Acción clave 6: *"Presentará en 2010 medidas encaminadas a conseguir una política de seguridad de las redes y de la información reforzada y de alto nivel, incluyendo iniciativas legislativas tales como una Agencia Europea de Seguridad de las Redes y de la Información (ENISA) renovada y medidas que permitan reaccionar con más rapidez en caso de ciberataque, incluyendo un CERT para las instituciones de la UE".*

[16] ALONSO LECUIT, Javier. Evolución de la agenda de ciberseguridad de la Unión Europea. *Real Instituto Elcano.* 2018, n.º 121.

[17] PIERNAS LÓPEZ, Juan Jorge. Ciberdiplomacia y ciberdefensa en la Unión Europea. Cizur Menor (Navarra): Aranzadi, 2020, pp. 143.

[18] Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio, abierto protegido y seguro. Bruselas, 7 de febrero de 2013, JOIN(2013) 1 final, pp. 5. Fecha de consulta: 24 de mayo de 2023. Disponible en: https://data.consilium.europa.eu/doc/document/ST%206225%202013%20INIT/es/pdf

reducir de forma radical la ciberdelincuencia, desarrollo de estrategias y capacidades de ciberdefensa vinculadas a la PCSD, desarrollar los recursos industriales y tecnológicos de ciberseguridad, y, por último, establecer una política internacional coherente en el ciberespacio.

En este sentido, para desarrollar una serie de capacidades adecuadas en ciberdefensa debería llevarse a cabo tanto un aumento en la resiliencia de los sistemas de comunicación e información, como un desarrollo en la detección, respuesta y recuperación en caso de un posible ciberataque[19].

Se aprecia un especial interés por parte de la Alta Representante en una serie de actividades claves en los que los EEMM y la Agencia Europea de Defensa (en adelante AED) podrán colaborar entre ellos.[20]. Se debe promover el desarrollo y las capacidades de ciberdefensa en cada uno de sus ámbitos como la tecnología, personal, la formación o la infraestructura. Igualmente, se debe fomentar la coordinación entre el sector civil y el sector militar con el objetivo fundamental de intercambiar información, intercambio de buenas prácticas, evaluación de riesgo, respuesta a incidentes y concienciación. Además, se señala que se elaborará una política de ciberdefensa de la UE. Y, por último, se llevarán a cabo una serie de diálogos con organizaciones internacionales, entre ellos la Organización del Tratado del Atlántico Norte (en adelante OTAN), con el objetivo de aumentar las capacidades de ciberseguridad, la coordinación y evitar la duplicación de esfuerzos.

Finalmente, a juicio de PIERNAS LOPEZ, los objetivos de esta estrategia eran poco precisos porque en vez de ir dirigidos a desarrollar una verdadera política de ciberdefensa para la UE y los EEMM, parece que solo conduce a complementar los esfuerzos de los EEMM y a mantener diálogos con socios internacionales.[21]

[19] Comunicación JOIN(2013) 1 final, pp. 12.
[20] Comunicación JOIN(2013) 1 final, pp. 12-13.
[21] PIERNAS LÓPEZ, Juan Jorge. Ciberdiplomacia y ciberdefensa*…, op. cit.,* pp. 144.

### 1.3. Marco político de ciberdefensa de la UE de 2014.

Siguiendo la Estrategia de Ciberseguridad de 2013[22] y las Conclusiones sobre la PCSD de diciembre de 2013, se establece que para que la UE y sus EEMM puedan reaccionar a los desafíos de una forma coherente era necesario llevar a cabo un marco político de ciberdefensa para el año 2014[23]. De igual forma, el Consejo Europeo se comprometió a elaborar un plan de trabajo y una serie de proyectos para perfeccionar la cooperación civil-militar y la protección de los recursos en las misiones y las operaciones de la UE[24].

Esta política fue adoptada, finalmente, por el Consejo el 18 de noviembre de 2014, en la que se refleja como el ciberespacio al igual que cualquier otro ámbito de la actividad militar (tierra, agua, aire y espacio) se requieren unas capacidades sólidas, para así apoyar las estructuras, misiones y operaciones de la PCSD[25]. En este documento, además, de establecerse los ámbitos prioritarios de actuación de la PCSD, también aclara las funciones de cada uno de ellos.

Este Marco tiene la misión de propulsar las capacidades de ciberdefensa relacionadas con la PSCD por parte de los EEMM y de mejorar la protección de las redes de comunicación de la PCSD utilizadas por las entidades de la UE. Se debe tener en cuenta que el ciberespacio es un ámbito que está en constante evolución por lo que resulta fundamental fomentar la cooperación entre el sector civil y el militar a la hora de desarrollar capacidades útiles para cada uno de estos sectores, y por supuesto, poniendo

[22] Comunicación (2013) 1 final, pp. 13: *"Elaborar un marco político de ciberdefensa de la UE para proteger las redes dentro de las misiones y operaciones de la PCSD [...]"*

[23] Conclusiones del Consejo Europeo 19 y 20 de diciembre de 2013. Bruselas, 20 de diciembre de 2013, EUCO 217/13, pp. 4. Fecha de consulta: 25 de mayo de 2023. Disponible en: https://data.consilium.europa.eu/doc/document/ST-217-2013-INIT/es/pdf

[24] Conclusiones EUCO 217/13, pp. 6. Véase Resolución del Parlamento Europeo, de 21 de mayo de 2015, sobre la aplicación de la política común de seguridad y defensa. Diario Oficial de la Unión Europea L 178 de 2.7.2019, pp. 1-115. Fecha de consulta: 26 de mayo de 2023. Disponible en: http://data.europa.eu/eli/reg/2019/1111/oj

[25] Marco político de ciberdefensa de la UE. Bruselas, 18 de noviembre de 2014, 15585/14, pp. 2. Fecha de consulta: 25 de mayo de 2023. Disponible en: https://data.consilium.europa.eu/doc/document/ST-15585-2014-INIT/es/pdf.

de relieve la importancia de la industria de defensa europea con base industrial y tecnológica (en adelante BITDE), que tendrá un gran peso en este caso.

Sin duda, no se podía olvidar dos aspectos fundamentales como son la formación y la cooperación con socios internacionales. Respecto a la formación, no solamente se llevarán a cabo intercambios entre EEMM entre sí, sino también entre instituciones de la UE, socios internacionales y, evidentemente, habría una participación del sector privado. Y en cuanto a la cooperación, es totalmente imprescindible incrementar la cooperación con los socios internacionales, particularmente con la OTAN, y deberá extenderse una mayor colaboración con otros socios como la Organización para la Seguridad y la Cooperación en Europa (en adelante OSCE) y la ONU.

En este documento en el que se incluyen más de cuarenta medias, se ha destacar aquellas que están directamente relacionadas con los CERTs, como, por ejemplo, la intención de mejorar la cooperación entre los CERTs militares de los EEMM de forma voluntaria, para mejorar la prevención y la gestión de incidentes, o reforzar la cooperación entre el CERT UE y los organismos de ciberdefensa pertinentes de la UE y la Capacidad de Respuesta a Incidentes Informáticos de la OTAN (en adelante NCIRC)[26].

Y, por último, pero no menos importante, señala que en caso de producirse una crisis cibernética podrá acudirse a los mecanismos que se ubica en el art. 222 del Tratado de Funcionamiento de la Unión Europea (en adelante TFUE), es decir, a la cláusula de solidaridad, y, por otro lado, se podrá aplicar la cláusula de defensa mutua del art. 42. 7 del Tratado de la Unión Europea (en adelante TUE)[27].

[26] TRINBERG, Lorena. *EU Cyber Defence Policy Framework Presents More Than 40 Action Measures* [en línea]. Fecha de consulta: 26 de mayo de 2023. Disponible en: https://ccdcoe.org/incyder-articles/eu-cyber-defence-policy-framework-presents-more-than-40-action-measures/

[27] Conclusiones EUCO 217/13, pp. 6.

### 1.4. Comunicación conjunta al Parlamento Europeo y al Consejo. Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE.

PIERNAS LÓPEZ señala que la política de ciberdefensa se vio claramente beneficiada tras el fortalecimiento que se experimentó en ciberseguridad tras la presentación de esta comunicación en septiembre de 2017[28].

En la introducción de este documento se observa cómo, debido al aumento de dispositivos a la red se ha ido adquiriendo una especial importancia para evitar que el campo del ciberespacio se convierta en un campo de batalla a la hora de propagar noticias falsas, campañas de desinformación o incluso que se lleven a cabo ciberataques contra infraestructuras vitales[29].

Al igual que, en el campo de la ciberseguridad es indispensable la cooperación entre el sector civil y militar en la ciberdefensa, lo que sería primordial llevar a cabo una colaboración entre los EEMM, concretamente para el intercambio de información, investigación y desarrollo de estrategias comunes, y por supuesto, llevar a cabo actividades de formación, ejercicios y pruebas conjuntas, por lo que será fundamental que coopere ENISA y el Centro Europeo de Competencia e Investigación en Ciberseguridad[30].

Debido a la importancia que tiene la defensa cibernética es necesario contribuir con investigación, por eso alguna de estas tecnologías como los sistemas de cifrado basados en tecnologías cuánticas, sistemas biométricos o la detección avanzada de amenaza persistente podrían financiarse a través del Fondo Europeo de Defensa (en adelante FED)[31].

[28] PIERNAS LÓPEZ, Juan Jorge. Ciberdiplomacia y ciberdefensa*..., op. cit.,* pp. 146.
[29] Comunicación JOIN(2017)450 final, pp. 2-3.
[30] Comunicación JOIN(2017)450 final, pp. 11.
[31] Comunicación JOIN(2017)450 final, pp. 11.

Es importante mencionar que los EEMM con capacidades en ciberseguridad más avanzada, con el apoyo del Alto Representante, la Comisión y la AED, podrán incluir la ciberdefensa en el marco de una "cooperación estructurada permanente" (en adelante CEP), lo que significó un punto de inflexión para poder conseguir una autonomía estratégica de la UE[32].

Por último, como viene siendo habitual en años anteriores a 2017, se remarca la necesidad de estrechar lazos de cooperación con la OTAN en diversas materias como fomentar la interoperabilidad mediante normas coherentes de defensa cibernética y llevar a cabo ejercicios y formación entre ambas organizaciones[33].

### 1.5. Cooperación estructurada permanente.

El Tratado de Lisboa implicó una gran evolución en el proceso de integración europea y tuvo una gran transcendencia sobre todo en la política europea de defensa[34], de tal manera, en diciembre de 2017, la Decisión (PESC) 2017/2315[35] establece la CEP, que según el art. 42.6 del TUE se define como un instrumento de cooperación en materia de defensa, por el cual, los EEMM que cumplan los criterios más elevados de capacidades militares podrán avanzar de una forma más rápida y estrecha en el desarrollo de dichas capacidades[36].

En relación con este asunto, el Protocolo n.º 10[37] ofrece más características sobre la CEP y parece ser que el objetivo es mejorar las capacidades militares para proporcionar

[32] Comunicación JOIN(2017)450 final, pp. 19.
[33] Comunicación JOIN(2017)450 final, pp. 22.
[34] CÓZAR MURILLO, Beatriz. La cooperación estructurada permanente: ¿El impulso definitivo que necesita la política común de seguridad y defensa? *Boletín IEEE.* 2017, n.º 8, pp. 5.
[35] Decisión (PESC) 2017/2315 del Consejo, de 11 de diciembre de 2017, por la que se establece una cooperación estructurada permanente y se fija la lista de los Estados miembros participantes. Boletín Oficial de la Unión Europea L 331, 14.12.2017, pp. 57–77. Fecha de consulta: 31 de mayo de 2023. Disponible en: http://data.europa.eu/eli/dec/2017/2315/oj
[36] CÓZAR MURILLO, Beatriz. La cooperación estructurada permanente…, *op. cit.,* pp. 6
[37] Protocolo (n° 10) sobre la cooperación estructurada permanente establecida por el artículo 42 del Tratado de la Unión Europea. Boletín Oficial de la Unión Europea C 326 de 26.10.2012, p. 275-277. Fecha de consulta: 31 de mayo de 2023. Disponible en: http://data.europa.eu/eli/treaty/teu_2012/pro_10/oj

fuerzas más operativas[38] y fortalecer las capacidades en materia de ciberespacio[39]. Esta CEP estará abierta a todos los EEMM, en la medida que se cumplan los dos requisitos que marca el art. 1 de dicho protocolo, por un lado, que desarrollen capacidades de defensa por medio de sus contribuciones nacionales y que en caso de que fuese necesario las desarrollen en programas de la AED, y, por otro lado, que como muy tarde en 2010, los EEMM tengan la capacidad de aportar unidades de combate y elementos de apoyo, como el transporte y la logística, tal y como determina en el art. 43 del TUE.

Siguiendo este protocolo, los EEMM se comprometen a cumplir las condiciones acordadas en materia de seguridad y de defensa asumiendo una serie de compromisos en los ámbitos que señalan en su art. 2 b), en el que se dispone que los EEMM tendrán que llevar a cabo una armonización de las capacidades militares para no caer en la duplicación de esfuerzos, siendo totalmente necesario aumentar la cooperación en materia de ciberdefensa[40].

En consecuencia, para garantizar la coherencia de la ejecución de los proyectos de CEP, el Consejo adoptó la Decisión (PESC) 2018/340, de 6 de marzo de 2018[41], en la que se estableció inicialmente una lista de diecisiete proyectos a desarrollar, entre los que se encontraban dos, relacionados directamente con la ciberdefensa como son la Plataforma de Intercambio de Información sobre Respuestas a Ciberamenazas e Incidentes de Ciberseguridad (en adelante CTISP) y los Equipos de Respuesta Telemática

[38]CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL. La cooperación estructurada permanente en el marco de la Unión Europea. Documentos de seguridad y defensa 42, pp.43. Fecha de consulta: 1 de junio de 2023. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF81.pdf

[39] OFICINA DE PUBLICACIONES DE LA UNIÓN EUROPEA. *Cooperación estructurada permanente en materia defensa y seguridad* [en línea]. Fecha de consulta: 1 de junio de 2023. Disponible en: https://publications.europa.eu/resource/cellar/354b8739-f4aa-11e8-9982-01aa75ed71a1.0003.02/DOC_1

[40] OFICINA DE PUBLICACIONES DE LA UNIÓN EUROPEA. *Cooperación …, op. cit.*

[41] Decisión (PESC) 2018/340 del Consejo, de 6 de marzo de 2018, por la que se establece la lista de proyectos que deben desarrollarse en el marco de la Cooperación Estructurada Permanente (CEP). Diario Oficial de la Unión Europea L 65, 8.3.2018, pp. 24–27. Fecha de consulta: 1 de junio de 2023. Disponible en: http://data.europa.eu/eli/dec/2018/340/oj

Rápida y de Asistencia Mutua en el ámbito de la Ciberseguridad (en adelante CCRT), ambos situados en el número 12 y 13 de esta decisión.

Posteriormente, el 12 de noviembre de 2019 se adoptó la Decisión (PESC) 2019/1909[42], tras la aprobación de las recomendaciones establecidas en el dictamen militar del Comité Militar de la Unión Europea sobre las recomendaciones de la Alta Representante[43], por lo cual, se procede a modificar y actualizar la Decisión 2018/340, en la que se incorporado dos proyectos nuevos vinculados a la ciberdefensa como es el Centro de la Unión Europea para el mundo académico y la innovación en el ámbito del ciberespacio ( en adelante UE CAIH), situado en el número 36, y por otro lado, el Centro de Coordinación del ámbito del Ciberespacio y de la Información (en adelante CIDCC), ubicado en el número 43.

### 1.6. Marco político de ciberdefensa de la UE (actualización 2018).

El incremento del papel de la ciberdefensa de la UE como así se demuestra en el Plan de Desarrollo de Capacidades de 2018, en el que se habilitó un conjunto de capacidades para operaciones cibernéticas como la cibercooperación, la investigación y la ciberinformación[44], no fue suficiente como así se evidencia en la Resolución emitida por el Parlamento Europeo el 13 de junio de 2018, ya que en el considerando F aparece reflejado que los servicios de inteligencia extranjeros se aprovechan de las vulnerabilidades que presentas las redes y los sistemas de información europeos [45]. Ante

[42] Decisión (PESC) 2019/1909 del Consejo de 12 de noviembre de 2019 por la que se modifica y actualiza la Decisión (PESC) 2018/340 por la que se establece la lista de proyectos que deben desarrollarse en el marco de la Cooperación Estructurada Permanente. Diario Oficial de la Unión Europea L 293 de 14.11.2019, pp. 113-118. Fecha de consulta: 5 de junio de 2023. Disponible en: http://data.europa.eu/eli/dec/2019/1909/oj

[43] Decisión (PESC) 2019/1909, considerando 10.

[44] AGENCIA EUROPEA DE DEFENSA. Fact sheet: *Capability Development Plan* [en línea]. Fecha de consulta: 1 de junio de 2023. Disponible en: https://eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0f

[45] Resolución del Parlamento Europeo, de 13 de junio de 2018, sobre ciberdefensa (2018/2004(INI)). Diario Oficial de la Unión Europea C 28 de 27.1.2020, pp. 57-70. Fecha de consulta: 1 de junio de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52018IP0258&qid=1685638347275

esta situación, el Parlamento Europeo pide a la Comisión que se actualice el marco de ciberdefensa de la UE[46], de este modo, unos meses más tarde, exactamente el 19 de noviembre de 2018 se adoptó el Marco político de ciberdefensa de la UE.

A pesar de que, en los anteriores documentos, ya mencionados, apuntaban a que el ciberespacio era un ámbito de actuación, en este marco se resaltaba aún más esta condición, como se demuestra en su alcance y objetivo al exponer que el ciberespacio lo equipara con los otros dominios físicos (tierra, mar, aire y espacio)[47]. En relación con esto, GUTIERREZ ESPADA define el ciberespacio no como un espacio físico sino como *"una realidad virtual de la que forman parte los ordenadores, servidores y redes del mundo"*[48].

El marco actualizado establece seis objetivos prioritarios, en el que se incluyen una serie de acciones a desarrollar en cada uno de estos ámbitos. Estas prioridades son las siguientes: apoyar el desarrollo de las capacidades y ciberdefensa de los EEMM, mejorar la protección de los sistemas de comunicación e información de la PCSD utilizados por las entidades de la UE, fomentar la cooperación civil-militar, investigación y tecnología, mejorar las posibilidades de educación, formación y ejercicios, y, por último, incrementar la cooperación con los socios internacionales.

Asimismo, al igual que, en el marco político de ciberdefensa de 2014, la política de ciberdefensa de 2018 alude que en casos de cibercrisis se podría haber acudido a los mecanismos de gestión crisis, que no son otros que los artículos 222 del TFUE y 47.2 del TUE.

[46] Resolución 2018/2044(INI), párrafo 64.
[47] Resolución 2018/2044 (INI), pp. 2
[48] GUTIERREZ ESPADA, Cesáreo. La ciberguerra y el Derecho internacional. En MARTÍNEZ PÉREZ, Enrique. *Las amenazas a la seguridad internacional hoy.* Valencia: Tirant lo Blanch, 2017, pp. 206.

## 2. EL PRESENTE DE LA CIBERDEFENSA DE LA UE.

La COVID-19 obligó a acelerar los procesos de digitalización para dar soluciones a muchos de los retos a los que se enfrenta la UE como la innovación, el cambio climático, la creación de empleo o la propia educación. Ahora bien, todo proceso conlleva una serie de consecuencias y en este caso según los datos de ENISA aumentaron los ciberataques entre 2020 y 2021.

El COVID-19 unido a la agresión de Rusia a Ucrania han puesto en jaque a la UE por lo que la Comisión y el Alto Representante presentaron el 10 de noviembre de 2022 una Comunicación conjunta sobre la política de ciberdefensa y un Plan de Acción sobre Movilidad Militar 2.0 dando lugar a la actual política de ciberdefensa[49].

Por medio de estas políticas se aumentarán las capacidades en ciberdefensa y se reforzará la coordinación y la cooperación entre las comunidades cibernéticas militares y civiles, mejorando así la gestión eficiente de las crisis cibernéticas en la comunidad, reduciendo sus dependencias estratégicas en tecnologías críticas. Además, se estimularán la formación, atracción y retención de los cibertalententos y se intensificará la cooperación con los socios del sector.

Dicho documento se organiza entorno a cuatro pilares. En primer lugar, la UE reforzará sus mecanismos de coordinación entre los actores nacionales y en materia de ciberdefensa para afianzar el intercambio de información y la cooperación entre las comunidades militares y civiles. En segundo lugar, el ecosistema de defensa, es decir, es necesario seguir trabajando en la normalización y certificación para asegurar tanto el ámbito militar como el civil. En tercer lugar, las capacidades de ciberdefensa, en la que los EEMM deben aumentar significativamente las inversiones de forma colaborativa utilizando las plataformas de cooperación y los mecanismos de financiación disponibles

[49] Comunicación Conjunta al Parlamento y al Consejo. Política de ciberdefensa de la UE. Bruselas, 8 de febrero de 2013, JOIN(2022) 49 final. Fecha de consulta: 6 de marzo de 2023. Disponible en: https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf

a nivel de la UE. Y en último lugar, afrontar los retos comunes, creando o retomando diálogos con países socios en materia de ciberdefensa[50].

### 2.1. Reforzar la ciberdefensa.

La UE fomenta y mejorará los mecanismos de coordinación y cooperación entre los diferentes actores nacionales y de la UE, apoyando aún más si cabe la PSCD. No obstante, es imprescindible la cooperación entre los sectores público y privado, principalmente, en cuanto a compartir información e intercambio de buenas prácticas. En este sentido, es primordial crear un entorno seguro para el intercambio de información entre los EEMM, ya que la descoordinación deriva en fragmentación y en duplicación de esfuerzos, por lo que se recomienda la creación de una Unidad Cibernética Conjunta[51] para garantizar una red de información rápida y segura, que se pondrá en funcionamiento antes del junio de 2023.

#### 2.1.1. Cooperación en la comunidad de defensa en la UE.

En la actual política de ciberdefensa se fija el objetivo de crear el Centro de Coordinación de Ciberdefensa de la UE (en adelante EUCDCC) convirtiéndose en el núcleo para recopilar, analizar, evaluar y distribuir información con el fin de llevar a cabo misiones y operaciones relacionada con la PSDC en el marco de ciberdefensa, convirtiéndose en un soporte con el propósito de un mejor conocimiento en materia de defensa. Este centro se basará en el proyecto de CEP sobre el CIDCC, ya mencionado anteriormente, que será considerado como un centro militar en el que los estados participantes contribuyen con personal nacional. Se establecerán unas relaciones entre EUCDCC, el Centro de Inteligencia y de Situación de la UE (en adelante EU INTCEN)

[50] COMISIÓN EUROPEA. *Preguntas y respuestas: La política de ciberdefensa de la UE* [en línea], Fecha de consulta: 6 de marzo de 2023. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/qanda_22_6643

[51] Recomendación (UE) 2021/1086 de la Comisión de 23 de junio de 2021 sobre la creación de una Unidad Conjunta Cibernética. Diario Oficial de la Unión Europea L 237, 5.7.2021, pp. 1–15. Fecha de consulta: 7 de marzo de 2023. Disponible en: http://data.europa.eu/eli/reco/2021/1086/oj

y con la inteligencia del Estado. No obstante, cada uno de estos Estados decide de forma independiente para que amenaza, incidente y operación contribuyen con medios o información.

Debido a la importancia del desarrollo de las nuevas tecnologías y lo importante que es mantenerse actualizado en el sector de defensa, en mayo de 2021 se inició el trabajo para la creación de Centro para la Innovación de Defensa de la UE (en adelante HEIDI), cuando el Consejo de Asuntos Exteriores solicitó que se reforzara las funciones de la AED. En este sentido, el 17 de mayo de 2022, los Ministros de Defensa de la UE aprobaron la creación de HEIDI, siendo una plataforma que posibilita una mayor cooperación entre los EEMM en materia de defensa[52].

El detonante para la creación de una red CERTs militares fueron los ejercicios cibernéticos celebrados en 2021 y 2022[53]. No obstante, en el Marco de Políticas de Ciberdefensa de 2014 ya se señalaba la falta de una red de CERTs militares (en adelante MilCert), mientras que la Estrategia de Ciberseguridad de la UE solicitó la elaboración de una red de este tipo, pero siempre apoyándose en los esfuerzos de la AED. En este sentido, para mejorar la cooperación militar, AED creará MilCert con el objetivo de crear una comunidad de confianza para aumentar la captación, la interconexión y la implementación de las lecciones aprendidas, dando así una respuesta más eficaz a las posibles amenazas que podrían afectar a la defensa de la UE. Con la creación de esta red se pretende, además de extender el intercambio de información de los CERTs entre sí, que se lleven a cabo operaciones no solamente de carácter defensivo, sino también ofensivo.

[52] AGENCIA EUROPEA DE DEFENSA. Fact sheet: *Hub for Defence Innovation (HEIDI)* [en línea]. Fecha de consulta: 6 de marzo de 2023. Disponible en: https://eda.europa.eu/docs/default-source/brochures/hedi-factsheet-(final).pdf

[53] AGENCIA EUROPEA DE DEFENSA. *Second EDA Live Cyber Exercise for Military CERTs Concluded* [en línea]. Fecha de consulta: 6 de marzo de 2023. Disponible en: https://eda.europa.eu/news-and-events/news/2022/01/26/second-eda-live-cyber-exercise-for-military-certs-concluded

En los próximos años, tanto la AED como los EEMM elaborarán una infraestructura que abrirán la puerta para favorecer el intercambio de información entre esta red MilCert. Por otro lado, se realizará una vez al año un ejercicio para simular un escenario de "fuego real" que permita probar nuevos mecanismos de respuesta, así como estudiar una mejor respuesta ante situaciones de emergencia.

Simultáneamente, para seguir afianzando el intercambio de información con el objetivo de establecer una estrategia fidedigna en el ámbito de las operaciones militares se fortalecerá la Conferencia de Cibercomandantes de la UE. Esta institución se creó a partir de las reuniones de los cibercomandos europeos (CyberCo) celebradas durante los meses de enero y junio de 2022. En este foro participará tanto la AED, que es la que encabezará dicho ente, como el Estado Mayor de la UE reuniéndose dos veces al año para debatir sobre cuestiones de la actualidad, creando así unos diálogos de forma más permanente.

### 2.1.2. Cooperación civil-militar en la UE.

La red de CERTs militares, para la mejora del intercambio de información no solamente colabora con la comunidad de defensa sino también con la comunidad civil. En este sentido, atendiendo a la nueva política de ciberdefensa, cuando la red de CERTs militares alcance tal grado de experiencia, la AED apoyará a los EEMM para establecer la posibilidad de cooperación con los Equipos de Respuesta a Incidentes de Seguridad Informática (en adelante CSIRT), que congregará tanto a los CSIRT nacionales como al CERT UE, pudiendo colaborar con el sector privado.

La conferencia de cibercomandantes podría cooperar con la Red de Organizaciones de Enlace de Crisis Cibernéticas de la UE (en adelante CyCLONe), que surgió tras la segunda edición de los ejercicios BlueOlex, mejorando los mecanismos de

colaboración ante una crisis de ciberseguridad a gran escala en Europa[54]. Asimismo, la conferencia de cibercomandantes contribuye con Blueprint de la Comisión Europea[55] para dar una respuesta rápida en caso de incidente transfronterizo.

El Centro de Coordinación de Ciberdefensa de la UE, ya mencionado, podría colaborar con la Unidad Cibernética Conjunta o Grupo Operativo sobre Crisis Cibernéticas como así lo denomina el propia Política de Ciberdefensa de 2022, compuesto por la Comisión, Servicio Europeo de Acción Exterior (en adelante SEAE), ENISA, CERT UE, Europol, red CSIRT y CyCLONE que tendrán como objetivo *"coordinar los esfuerzos de la UE con vistas a la prevención, detección, desaliento, disuasión, mitigación y respuesta a los incidentes y crisis de ciberseguridad"*[56].

Es necesario destacar el proyecto que se señala en el propio marco de política de ciberdefensa de 2022, Cyber Ranges Federation[57], por el cual se permite agrupar las capacidades de los ejércitos cibernéticos con fines de investigación. Asimismo, también se resalta Ciber Phalanx[58], una combinación entre ejercicios y cursos sobre amenazas cibernéticas e hibridas en el proceso de planificación de operaciones tanto a nivel estratégico como operativo. Concretamente, en el Ciber Phalanx 2021[59] organizado por AED y Portugal en el que participaron ciento treinta planificadores de operaciones y quince EEMM de la AED, así como instituciones de la UE, socios y la OTAN, se señaló

[54] DEPARTAMENTO DE SEGURIDAD NACIONAL. *Unión Europea-Ciberseguridad* [en línea]. Fecha de consulta: 7 de marzo de 2023. Disponible en: https://www.dsn.gob.es/en/actualidad/seguridad-nacional-ultima-hora/uni%C3%B3n-europea-%E2%80%93-ciberseguridad-15

[55] Recomendación (UE) 2017/1584 de la Comisión de 13 de septiembre de 2017 sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala. Diario Oficial de la Unión Europea L 239, 19.9.2017, pp. 36–58. Disponible en: http://data.europa.eu/eli/reco/2017/1584/oj

[56] Recomendación (UE) 2021/1086 de la Comisión de 23 de junio de 2021 sobre la creación de una Unidad Conjunta Cibernética.

[57] PESCO PROJECTS. *Cyber Ranges Federation* [en línea]. Fecha de consulta: 8 de marzo de 2023. Disponible en: https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/

[58] AGENCIA EUROPEA DE DEFENSA. Fact Sheet: *Cyber Phalanx* [en línea]. Fecha de consulta: 1 de marzo de 2023. Disponible en: https://eda.europa.eu/docs/default-source/eda-factsheets/cyph-fact-sheet_v04.pdf

[59] AGENCIA EUROPEA DE DEFENSA. *CYBER PHALANX: EDA's dedicated cyber training for Operation Planners wraps in Portugal* [en línea]. Fecha de consulta: 8 de marzo de 2023. Disponible en: https://eda.europa.eu/news-and-events/news/2021/10/05/EDA-cyber-phalanx-wraps-in-portugal

la importancia de interrelación entre distintos expertos en ciberdefensa y los planificadores de operaciones.

En estos últimos años está cobrando una gran relevancia los equipos de seguridad de las organizaciones, denominada Centros de Operativos de Seguridad (en adelante COS). La comunidad de ciberdefensa podría aprovecharse de las capacidades civiles reforzando así las capacidades de detención y respuesta a través de la elaboración de los COS de infraestructuras civiles de la UE. Esta red COS estará formada por múltiples centros plurinacionales pudiendo aprobar la participación de entes de defensa y estableciendo herramientas de intercambio de información con los responsables militares y con el Centro de Coordinación de Ciberdefensa de la UE. Además, estos COS plurinacionales, a su vez se congregan en varios COS nacionales que contarán con la ayuda del Programa Europa Digital[60].

Finalmente, el I+D es la herramienta más importante para llegar a tener un excelente sistema de ciberdefensa. En este sentido, se puede pedir tanto a la UE como a los EEMM que disminuyan los trámites burocráticos, permitiendo a las empresas llevar a cabo resultados innovadores. Asimismo, se debe favorecer no solo la colaboración con empresas sino también con universidades, siendo estas grandes entidades de innovación, con la finalidad de reducir la dependencia de productos de terceros países para crear una mayor autonomía, pero para que sea posible será imprescindible la contribución del FED.

### 2.2.Asegurar el ecosistema de defensa.

Hasta los programas más simples pueden ser utilizados para llevar a cabo ciberataques, poniendo en jaque a empresas, gobiernos y por supuesto al área de defensa.

[60] Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo de 29 de abril de 2021 por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240. Diario Oficial de la Unión Europea L 166, 11.5.2021, pp. 1–34. Fecha de consulta: 8 de marzo de 2023. Disponible en: http://data.europa.eu/eli/reg/2021/694/oj

De ahí que cobre una gran importancia la normalización y certificación tanto en el terreno civil como militar.

En este ámbito, los EEMM elaboran sus propias normas de seguridad sin tener en cuenta la conexión con el sector privado, a pesar de la existencia de los productos de doble uso, siendo así un aspecto negativo a la hora de llevar a cabo misiones de la PCSD.

### 2.2.1. Certificación.

Actualmente, no existe una normativa común aplicable tanto al sector de la defensa, más concretamente a la ciberdefensa. Sin embargo, en un principio, hace varios años atrás, en diversos preceptos aparecía cierta colaboración entre ambos sectores, pero no tuvo mucho éxito, ya había ciertos EEMM que no estaban por la labor de que el sector de defensa y el privado colaborasen por miedo a que los sistemas de defensan se vieran comprometidos, y obligaron a que se eliminara todo lo relacionado con defensa, siendo el principal impedimento la gobernanza de los EEMM. De este modo, no parece que sea pueda hacer mucho más hasta que los EEMM entienden que la única forma de seguir progresando es a través de la cooperación y colaboración.

No obstante, el día 18 de abril de 2023, propuso una modificación en el Reglamento sobre la Ciberseguridad[61] para adquirir en un futuro una serie de certificaciones para servicios especialmente críticos que sean prestados por proveedores, con el objetivo de dar respuesta a incidentes de seguridad o que se den las auditorias de seguridad necesarias para así prevenir, detectar o dar respuesta a los ciberataques[62].

[61] Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013 («Reglamento sobre la Ciberseguridad») (Texto pertinente a efectos del EEE). Diaripo Oficial de la Unión Europea L 151, 7.6.2019, pp. 15–69. Fecha de consulta: 19 de mayo de 2023. Disponible en: http://data.europa.eu/eli/reg/2019/881/oj

[62] Proposal for a regulation of the European Parliament and of the council amending Regulation (EU) 2019/881 as regards managed security services. COM(2023) 208 final. Fecha de consulta: 19 de mayo.

Bajo mi humilde opinión, al igual que se ha avanzado hacia un sistema de certificación de ciberseguridad a escala de la UE, también se puede avanzar en el ámbito de la ciberdefensa, creando un "marco único de certificación en la UE" permitiendo certificar sistemas, procesos y productos principalmente militares. Sabiendo, que el ámbito de ciberdefensa es bastante delicado se pondrán una serie de requisitos a las empresas para que puedan participar en este ámbito. Siendo el objetivo principal incrementar la ciberdefensa de la UE emitiendo certificados que podrán ser reconocidos en toda la UE.

### 2.2.2. Normalización.

Según al art. 2 del Reglamento (UE) 1025/2012 del Parlamento Europeo y del Consejo, de 25 de octubre de 2012, sobre la normalización europea y aplicándolo al contexto de ciberdefensa, se puede definir como la unificación de procesos, desarrollos y diseños de materiales y equipos utilizados por las Fuerzas Armadas para la defensa en el ciberespacio.

Debido a la importancia de la normalización en este entorno, la AED lanzó en 2007 el Sistema Europeo de Información sobre Normalización de la Defensa (en adelante EDSIS) con el objetivo de promover una mayor normalización de los equipos de defensa, permitiendo tanto a los EEMM de la propia agencia como a la industria, participar en el proceso de normalización de defensa[63]. Posteriormente, en 2012 se desarrolló el Sistema Europeo de Referencia de Normas de Defensa (en adelante EDSTAR), que comprende

Disponible en: https://digital-strategy.ec.europa.eu/es/library/proposed-regulation-managed-security-services-amendment
Véase también FUNDACIÓN GALICIA EUROPEA. *Ciberdefensa: hacia unas capacidades más sólidas de la UE en pro de una cooperación operativa eficaz, la solidaridad y la resiliencia* [en línea]. Fecha de consulta: 19 de mayo de 2023. Disponible en: https://fundaciongaliciaeuropa.eu/es/ciberdefensa-cara-a-unhas-capacidades-mais-solidas-da-ue-en-prol-dunha-cooperacion-operativa-eficaz-a-solidariedade-e-a-resiliencia/

[63] AGENCIA EUROPEA DE DEFENSA. *European defence standardisation* [en línea]. Fecha de consulta: 16 de marzo de 2023. Disponible en: https://eda.europa.eu/what-we-do/all-activities/activities-search/materiel-standardisation

estándares de "mejores prácticas" seleccionados tanto por organizaciones gubernamentales como por la industria[64].

En la Política de Ciberdefensa de 2022 se pueden ver destellos de lo que podría llegar a ser una colaboración entre el sector civil y militar, a través de la propuesta de Ley de Ciberresiliencia[65] que comprenderá, siempre que se pueda, normas de ciberseguridad tanto para productos civiles como militares. Esto se ve reforzado por el Plan de acción sobre las sinergias entre la industria civil, de defensa y espacial[66], por el cual se promoverá el uso de tanto de normas civiles como de defensa, con la posibilidad de creación de nuevas normas.

### 2.2.3. Ciberresiliencia en el ecosistema de defensa.

Resulta preciso insistir que, en un mundo globalizado, los ciberincidentes están a la orden del día, siendo la ciberresiliencia un aspecto fundamental en el ecosistema de defensa. Conviene manifestar los ciberataques pueden afectar a las infraestructuras militares de los EEMM, infraestructuras críticas, misiones y operaciones de la PCSD, industria de la defensa y centros de investigación como así indica la Política de ciberdefensa de 2022. En este escenario se opera con información especialmente sensible por lo que precisa inversión para reforzar las estructuras militares.

Las infraestructuras críticas, desde hace varios años, son objetos de ciberataques, como se dio en el pasado en Estonia, y como se da prácticamente a diario en Ucrania. Por eso, la UE fomenta seguir aumentando la protección de las infraestructuras, como señala

[64] AGENCIA EUROPEA DE DEFENSA. *European Defence Standards Reference System (EDSTAR)* [en línea]. Fecha de consulta: 16 de marzo de 2023. Disponible en: https://edstar.eda.europa.eu/

[65] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020. COM/2022/454 final. Fecha de consulta: 16 de marzo de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52022PC0454

[66] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico Social Europeo y al Comité de las Regiones. Plan de acción sobre las sinergias entre las industrias civil, de la defensa y espacial. COM/2021/70 final. Fecha de consulta: 23 de marzo de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52021DC0070&from=ES

la última política de ciberdefensa. Debido a esto se enfocará, sobre todo en mejorar la seguridad de las telecomunicaciones, transporte, energía y espacio[67].

Antes de lanzar la Política de Ciberdefensa de 2022, se puso de manifiesto la importancia de las infraestructuras físicas y digitales, pero tras los lamentables hechos de la Guerra de Ucrania y el sabotaje a Nord Stream se articuló la propuesta de Recomendación del Consejo que tiene *"por objeto por objeto intensificar el apoyo de la UE para mejorar la resiliencia de las infraestructuras críticas, y garantizar una coordinación a escala de la Unión en lo que a preparación y respuesta se refiere."*[68]

Además, se pone de relieve la importancia que ha cobrado las infraestructuras marítimas, que verán reforzadas su ciberseguridad como así se refleja en el plan de acción de la UE para digitalizar el sistema eléctrico[69]. En este ámbito cobra un especial interés los cables submarinos, que son el principal instrumento en el que se apoyan el resto de las infraestructuras, sin olvidar que por ellos circula una gran cantidad información a través del globo terráqueo. De esta forma, se tienen los servidores y espacios donde se almacena la información ya que en la actualidad todavía es necesario espacios físicos para acumular datos.

En relación con el párrafo anterior, la AED organizó la primera reunión de expertos sobre "Protección de infraestructuras marítimas críticas" en la que se reunieron alrededor de 170 expertos, en la que trataron los problemas existentes en esta materia: defensa, diplomacia, seguridad marítima, ciberseguridad y autonomía estratégica, para

[67] Conclusiones del Consejo sobre la elaboración de la posición de la Unión Europea en materia cibernética. Fecha de consulta: 18 de marzo de 2023. Disponible en: https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/es/pdf

[68] Propuesta de Recomendación del Consejo sobre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras crítica. COM/2022/551 final. Fecha de consulta: 22 de marzo de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022DC0551&from=ES

[69] Comunicación de la Comisión, al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Digitalizar el sistema eléctrico: plan de acción de la UE. COM/2022/552 final. Fecha de consulta: 23 de marzo de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022DC0552&from=ES

combatir el terrorismo, la piratería o los ciberataques, por lo cual sería necesario llevar a cabo una cooperación entre actores públicos, privados y militares[70].

Asimismo, las infraestructuras espaciales reciben una especial atención, y a aún más después del ciberataque realizado a la red satelital KA-SAT (satélite que ofrece conexión a Internet a Europa y parte de Oriente Medio), por parte de Rusia, poniendo en peligro tanto a los sistemas de defensa, a la sociedad, como a la economía. No obstante, la Brújula Estratégica, tras este ciberataque, señaló que se elevará el nivel de ciberresiliencia en este tipo de infraestructuras.

Finalmente, desde hace unos años, se ha intentado socavar las infraestructuras críticas de la UE, por lo que la Comisión, en el 2020, se planteó realizar una mejora considerable en materia de resiliencia sobre tales infraestructuras y seguridad de las redes y los sistemas de información, por lo que se elaboraron dos directivas, que hoy en día se encuentran en vigor, como son la Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión y la Directiva (UE) 2022/2557 relativa a la resiliencia de las entidades críticas[71].

### 2.3. Inversión en ciberdefensa.

Las inversiones en ciberdefensa en la UE han aumentado exponencialmente de forma paralela a como lo han hecho los ciberataques, sobre todo hoy en día, con la Guerra entre Rusia y Ucrania, lo cual acentúa la necesidad de que los EEMM posean capacidades destacadas en este ámbito.

[70] CENTRO DE DOCUMENTACIÓN EUROPEA DE ALMERÍA. *La UE necesita una mayor cooperación para mitigar los riesgos de las infraestructuras marítimas críticas* [en línea]. Fecha de consulta: 26 de junio de 2023. Disponible en: https://www.cde.ual.es/la-ue-necesita-una-mayor-cooperacion-para-mitigar-los-riesgos-de-las-infraestructuras-maritimas-criticas/

[71] COMISIÓN EUROPEA. *Empiezan a aplicarse nuevas normas más estrictas para la resiliencia cibernética y física de las entidades y redes críticas* [en línea]. Fecha de consulta: 23 de marzo de 2023. Disponible en: https://digital-strategy.ec.europa.eu/es/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks

El desarrollo tecnológico es una pieza clave para obtener superioridad frente a otras potencias como Rusia, China o Corea del Norte que amenazan la competitividad de la UE. En consecuencia, se debe perfeccionar la cooperación entre los EEMM en materia de ciberdefensa mediante las inversiones en I+D. En este sentido, la Comisión ha aumentado la inversión en ciberdefensa a través del FED.

Entre 2014 y 2020 que se llevó a cabo una Acción Preparatoria sobre Investigación de Defensa, que posteriormente derivó en el lanzamiento por parte de la Comisión Europea de una comunicación por la que se creaba el FED, como de una propuesta de Reglamento en el que se establecía el Programa Europeo de Desarrollo Industrial en materia de Defensa (en adelante PEDID)[72].

Atendiendo a los acontecimientos geopolíticos que se dan hoy en día, la ciberdefensa se ha convertido en una de las materias a las que se le está dando el sitio que le corresponde. Debido a esto, la Comisión, el Alto Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad establecieron que era de vital importancia establecer ámbitos de colaboración en este ámbito[73]. En este sentido, el art. 3 del Reglamento (UE) 2021/697 por el que se establece el Fondo Europeo de Defensa, cuya finalidad es estimular la competitividad, la eficiencia y la capacidad de innovación de la BITDE en toda la Unión.

[72] AGENCIA EUROPEA DE DEFENSA. *European Defence Fund (EDF)* [en línea]. Fecha de consulta: 2 de abril de 2023. Disponible en: https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-%28edf%29

[73] Reglamento (UE) 2021/697 del Parlamento Europeo y del Consejo de 29 de abril de 2021 por el que se establece el Fondo Europeo de Defensa y por el que se deroga el Reglamento (UE) 2018/1092 (Texto pertinente a efectos del EEE). Diario Oficial de la Unión Europea L 170, 12.5.2021, pp. 149–177. Fecha de consulta: 2 de abril de 2024. Disponible en: http://data.europa.eu/eli/reg/2021/697/oj Considerando 34 del Reglamento (UE) 2021/697 del Parlamento Europeo y del Consejo de 29 de abril de 2021 por el que se establece el Fondo Europeo de Defensa y por el que se deroga el Reglamento (UE) 2018/109: *"La ciberseguridad y la ciberdefensa son desafíos cada vez más importantes, y la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad reconocieron la necesidad de establecer sinergias entre las acciones en materia de ciberdefensa dentro del ámbito de aplicación del presente Reglamento […]"*

En el apartado primero del art. 24 del Reglamento 2021/697 se establece que los fondos europeos se ejecutarán a través de los programas de trabajo, y a su vez, según el apartado tercero, estos programas serán los que establecerán los temas de investigación que serán apoyados por los Fondos, entre los que se encuentra en la ciberdefensa. Concretamente, se ha destinado hasta un 8% del presupuesto del FED, es decir, alrededor de seiscientos cuarenta millones de euros al ámbito de las tecnologías disruptivas y defensa. Asimismo, una parte de estas inversiones también se destinaron a varios proyectos del PEDID, particularmente en seis proyectos (PANDORA, DISCRETION, CYBER4DE, ECYSAP, SMOTANET y HERMES) que se encargan de detectar amenazas en tiempo real y llevar a cabo formaciones y ejercicios cibernéticos[74].

Para mantenerse en la cresta de la ola en el ámbito de la ciberdefensa, es necesario estar al día en cuanto a las nuevas tecnologías, concretamente en las tecnologías emergentes disruptivas como la inteligencia artificial y la computación cuántica[75]. En este sentido, la UE debería mirar más allá, invirtiendo en criptología post-cuántica, aumentando así la seguridad en caso de que se lleve ataques a través de ordenadores cuánticos[76].

A raíz de la Guerra en Ucrania se prestó una especial atención para satisfacer las necesidades tecnológicas de ciberdefensa, por lo que la AED y los EEMM plantearon

[74] COMISIÓN EUROPEA. *European Defence Industrial Development Programme (EDIDP)* [en línea]. Fecha de consulta: 28 de marzo de 2023. Disponible en: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_es
Véase también FONDO EUROPEO DE DEFENSA. *EU-GUARDIAN* [en línea]. Fecha de consulta: 28 de marzo de 2023. Disponible en: https://defence-industry-space.ec.europa.eu/system/files/2022-07/Factsheet_EDF21_EU-GUARDIAN.pdf
El proyecto EU GUARDIAN que tiene como objetivo dar soluciones a la gestión de incidentes de ciberdefensa mediante la inteligencia artificial.

[75] AGENCIA EUROPEA DE DEFENSA. *Overarching Strategic Research Agenda and CapTech SRAs Harmonisation* [en línea]. Fecha de consulta: 28 de marzo de 2023. Disponible en: https://eda.europa.eu/docs/default-source/brochures/eda-osra-brochure.pdf

[76] GARCÍA CID, Marta Irene. *Criptografía cuántica: hacia una autonomía estratégica* [en línea]. Fecha de consulta: 28 de marzo de 2023. Disponible en: https://www.linkedin.com/pulse/criptograf%C3%ADa-cu%C3%A1ntica-hacia-una-autonom%C3%ADa-estrat%C3%A9gica-indra/?trk=organization_guest_main-feed-card_feed-article-content&originalSubdomain=es

para 2023 una hoja de ruta tecnológica para las cibertecnologías críticas. En esta línea la hoja de ruta tecnológica para las cibertecnologías críticas consistiría en un plan estratégico para mejorar la competitividad y la resiliencia de la industria de la defensa europea fomentando una estrecha colaboración entre el ámbito civil y el militar, con la posibilidad de crear una "ventanilla" para la incorporación de nuevas empresas en este terreno.[77]

### 2.3.1. Personal y captación en ciberdefensa.

La UE no cuenta con suficientes profesionales formados en ciberdefensa por lo que se produce una disminución de las capacidades en el sector público a la hora de combatir las ciberamenzas para proteger así las infraestructuras críticas. Además, de la falta de conocimientos en la materia, existe una salvaje competencia en el sector privado para hacerse con los servicios de los profesionales existentes.

Los perfiles más demandados son los técnicos, concretamente los encargados de la gestión de entidades, seguridad y monitorización. Sin embargo, también es necesario tener conocimientos en otras áreas como gobierno, riesgo o de dirección de seguridad que está más asociados con la parte de gestión, así como como en geopolítica o geoestrategia, que sean capaces de adaptarse a diferentes contextos y entornos en función de la labor a desarrollar.

Concretamente, en España existen profesionales tanto de perfil técnico como no técnico, pero el problema está en la precariedad laboral en este ámbito, por lo que la mayoría de los profesionales suelen irse a terceros países como EE. UU. o Japón, produciéndose una fuga de talentos casi imposible de parar. Ante esta situación, la Comisión pondrá en funcionamiento el Marco Europeo de Habilidades en Ciberseguridad (en adelante ECSF) con el objetivo de aumentar el número de profesionales, intentando

[77] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. *Hoja de ruta sobre tecnologías críticas para la seguridad y la defensa* COM(2022) 61 final[en línea]. Fecha de consulta: 5 de abril de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022DC0061&from=ES

crear un lenguaje común en el ámbito de la ciberseguridad y promover la captación, educación y desarrollo de estos profesionales para lograr una fidelización de los profesionales en Europa[78].

Atendiendo a las necesidades de aumentar el número de profesionales en este ámbito, la Escuela Europea de Seguridad y Defensa (en adelante EESD), AED y los EEMM estudiaran la posibilidad de aumentar el número de cursos de formación en la Plataforma de EESD. En este caso, es necesario destacar el EU CAIH[79] que agrega valor a una red innovadora para la captación y educación de personas en ciberdefensa y seguridad, actuando como punto de coordinación para llevar a cabo ciberejercicios, mejorando así la cooperación.

### 2.4. Cooperación para afrontar retos comunes.

La UE llevará a cabo una serie de asociaciones en materia de ciberdefensa siempre y cuando, esta y los socios o las organizaciones con las que colaboren consigan beneficiarse. Esto podrá darse gracias a múltiples herramientas a través de acuerdos o colaboración para llevar a cabo operaciones o ejercicios de formación, sin olvidarse de los nuevos instrumentos como la ciberdiplomacia o una red de militares en las distintas delegaciones de la UE.

#### 2.4.1. Cooperación UE-OTAN.

La base jurídica de la cooperación entre la UE y la OTAN deriva de la PCSD regulada en los arts. 42 al 46 del TUE y a los que se incorpora el protocolo 10 de los TUE y TFUE en los que ahonda en la CEP. El art. 42.1 del TUE viene a establecer que la PESC

[78] ENISA. *European Cybersecurity Skills Framework (ECSF)* [en línea]. Fecha de consulta: 6 de abril de 2023. Disponible en: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

[79] PESCO PROJECTS. *EU Cyber Academia and Innovation Hub* [en línea]. Fecha de consulta: 6 de abril de 2023. Disponible en: https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/

es un instrumento de la Política Exterior de Seguridad y Defensa (en adelante PESD) en la UE ofrecerá medios tantos civiles como militares para llevar a cabo operaciones[80].

El TUE brinda dos apartados a cerca de las relaciones con la OTAN, concretamente los apartados 2 y 7 del art. 42 del TUE. En el apartado segundo, reconoce una cierta primacía de la OTAN en aquellos casos que los EEMM estimen que esta les proporcione una mayor seguridad. Y en el apartado séptimo, se reafirma esa primacía respecto a la defensa colectiva de los EEMM.

La UE y la OTAN tienen unos valores e intereses estratégicos similares en materia de seguridad, lo que será un punto a favor a la hora de mejorar la cooperación y el desarrollo de cibercapacidades para prevenir, detectar y disuadir ciberataques, así como a la hora de gestionar un incidente cibernético ante las conductas agresivas por parte de China, Rusia y Corea del Norte y los múltiples ciberataques llevados contra organismos gubernamentales y entes privados. Debido a esta razón, esta cooperación debería optar por centrarse en invertir y desarrollar nuevas tecnologías, así como asegurar unas redes de alta velocidad que custodien de una forma segura los datos y las comunicaciones cumpliendo las normas nacionales y de la UE.

En la Cumbre de Gales se vislumbraba la necesidad de llevar a cabo una respuesta más eficaz frente a las crisis en materia de ciberdefensa, por esa razón se determinó incorporar al art. 5 del Tratado de Washington de 1949[81] los ciberataques. En apoyo a esta corriente, en la Cumbre de Varsovia de 2016 se firmó la Declaración OTAN-UE que

[80] INSITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. Política de Defensa Común. *Revista del Instituto Español de Estudios Estratégicos*. 2017, n.º 9, pp. 121-159.

[81] Tratado de Washington de 4 de abril de 1949, art. 5: *"Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudará a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Cualquier ataque armado de esta naturaleza y todas las medidas adoptadas en consecuencia serán inmediatamente puestas en conocimiento del Consejo de Seguridad. Estas medidas cesarán cuando el Consejo de Seguridad haya tomado las disposiciones necesarias para restablecer y mantener la paz y la seguridad internacionales".*

incluye una serie de desafíos en siete ámbitos, entre los que se encuentra las amenazas híbridas y la ciberdefensa[82].

En la 31ª cumbre de la OTAN celebrada en Bruselas el 14 de junio de 2021 se determinó lanzar el Acelerador de Innovación de Defensa del Atlántico Norte (en adelante DIANA) con el objetivo de impulsar la cooperación transatlántica en el campo de las tecnologías emergentes, estimulando así otro tipo de tecnologías como la inteligencia artificial, tecnologías cuánticas, biotecnología, etc.[83]. Pues en este sentido, a mi parecer, podría establecerse algún tipo de cooperación entre este proyecto y HEIDI, ya mencionado, con la intención de estar a la vanguardia en ciertos aspectos como las capacidades industriales o la investigación en materia de defensa.

En la pasada Cumbre de Madrid celebrada en junio de 2022 se planteó un nuevo concepto estratégico en el que la agresión de Rusia a Ucrania ha sido un punto de inflexión para agilizar la transformación digital, así como mejorar las ciberdefensas, redes e infraestructuras[84].

La OTAN y la UE frente al contexto bélico que se está dando en el Este de Europa, han expresado su total apoyo al pueblo ucraniano y su derecho a defenderse. Siguiendo estos acontecimientos, el 10 de enero de 2023, estas dos organizaciones firmaron la Declaración conjunta en Bruselas[85], en la que exponen que combatirán unidas frente a la amenaza rusa, ya que supone un verdadero peligro para Europa. En esta declaración se

[82] MORA BENAVENTE, Enrique. La OTAN y la Unión Europea, ¿por fin una cooperación eficaz? *Cuadernos de Estrategia*. 2017, N.º 191, 2017, pp. 123-158.
[83] CAMPUS INTERNACIONAL PARA LA SEGURIDAD Y LA DEFENSA (CISDE). *El COVID-19 acelera la transformación tecnológica de la OTAN* [en línea]. Fecha de consulta: 9 de abril de 2023. Disponible en: https://observatorio.cisde.es/actualidad/el-covid-19-acelera-la-transformacion-tecnologica-de-la-otan/
[84] NOGUERA GÓMEZ, Fernando; MARTINEZ MARTÍNEZ, Dolores Fuensanta; FERNÁNDEZ VALERA, María Magdalena y PÉREZ CÁCERES, María Concepción. La UE y la OTAN ante los nuevos escenarios de la seguridad y la defensa. *Revista Española de Defensa*. Diciembre 2022, págs. 50-52.
[85] Consejo de Europa. *Declaración conjunta sobre la cooperación UE-OTAN (comunicado de prensa 10/01/2023*). Fecha de consulta: 9 de abril de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/01/10/eu-nato-joint-declaration-10-january-2023/

manifiesta que ambos entes incrementaran aún más la cooperación en varios aspectos, entre los que se encuentran las amenazas híbridas y cibernéticas, así como en las tecnologías emergentes y disruptivas.

A pesar de la preocupación mostrada en la actual política de ciberdefensa, la importancia de la cooperación entre la OTAN y la UE viene de años atrás, cuando el equipo de NCIRC y el CERT UE firmaron en 2016 un Acuerdo Técnico de colaboración para reforzar la cooperación en la defensa cibernética facilitando un marco más ágil para el intercambio de información[86], con el objetivo de mejorar la prevención, detección y dar una respuesta más eficaz ante posibles ciberataques, como así lo refleja la Resolución sobre la situación de las capacidades de ciberdefensa en la UE[87].

De igual modo, se estudian nuevas formas de cooperación entre ambas organizaciones a través del Centro de Excelencia para la Ciberdefensa Cooperativa (en adelante CCDCOE) de la OTAN y la Academia de las Comunicaciones y de la Información de la OTAN, por lo que se podrían llevar a cabo reuniones o diálogos para favorecer la confianza mutua y el intercambio de información entre los EEMM y la OTAN.

Los ejercicios en materia de ciberdefensa son otras de las herramientas esenciales para la cooperación entre ambas organizaciones, en las que el personal de ambos entes intercambian información para adquirir nuevos conocimientos y desarrollan actividades de "fuego real" para poner en práctica lo aprendido. En este sentido, toma un papel muy relevante "Cyber Coalition" un ejercicio anual en el que se pone a prueba las

[86] DEPARTAMENTO DE SEGURIDAD NACIONAL. *La OTAN y la UE aumentan la cooperación en ciberseguridad* [en línea]. Fecha de consulta: 10 de abril de 2023. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/otan-ue-aumentan-cooperaci%C3%B3n-ciberseguridad

[87] Resolución del Parlamento Europeo, de 7 de octubre de 2021, sobre la situación de las capacidades de ciberdefensa de la UE (2020/2256(INI)). Diario Oficial de la Unión Europea C 132 de 24.3.2022, p. 102-112. Fecha de consulta: 10 de abril de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021IP0412&qid=1681121453845

cibercapacidades de la OTAN. El Informe de Ciberdefensa de 2018 de la UE[88] declara que la participación de miembros de la UE en este ejercicio, así como en cualquier otro, deriva en un avance bidireccional en esta materia.

En lo relativo a la industria de ciberdefensa, el concepto estratégico de la OTAN de 2022[89] insta a que la UE y los miembros de la OTAN refuercen su cooperación atendiendo a los conflictos bélicos o no bélicos, que pueden derivar en ciberataques a infraestructuras, actos de sabotaje hasta llegar a chantajes alimentarios o energéticos. En este caso, ambas organizaciones saben que están ante una nueva era tecnológica en la que es necesario llevar a cabo inversiones e incentivar a la industria militar, con el objetivo de prosperar en ciberseguridad y ciberdefensa a través de una serie de ejercicios y compartiendo buenas prácticas. No obstante, algunos EEMM sienten recelos a la hora de compartir información con ciertos países pertenecientes a la OTAN, ya que han visto como los fondos económicos europeos han ido destinados a financiar políticas de estados que no son miembros de la UE.

### 2.4.2. Cooperación con otros socios.

#### 2.4.2.1. EE. UU.

La asociación entre la UE y la OTAN se basan en fuertes lazos con vínculos políticos, culturales e históricos, compartiendo así una serie de valores e intereses comunes, por lo que resultará más fácil llevar a cabo una serie de mecanismos para la coordinación tanto para las amenazas tradicionales como para las amenazas a través de medios tecnológicos.

La Resolución sobre el futuro de las relaciones entre la UE y EE. UU.[90] incitan aún más a que se refuerce la cooperación en el ámbito de la ciberdefensa, pidiendo que

[88] PARLAMENTO EUROPEO. Informe sobre ciberdefensa (2018/2004(INI)). Fecha de consulta: 11 de abril de 2023. Disponible en: https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_ES.html
[89] CENTRE DELÀS D'ESTUDIS PER LA PAU. Informe 53*: «La OTAN, construyendo inseguridad global»*. Fecha de consulta: 12 de abril de 2023. Disponible en: https://centredelas.org/wp-content/uploads/2022/06/informe53_OTANConstruyendoInseguridadGlobal_CAST.pdf
[90] Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre el futuro de las relaciones entre la Unión y los EE. UU. (2021/2038(INI)).

se desarrollen unas defensas eficaces para combatir los ciberataques. Por supuesto, se deben crear y desarrollar una serie de cibercapacidades entre ENISA y la oficina homóloga en EE. UU., en la que la ciberdefensa tenga un lugar especial, en la que se incluyan tanto técnicas defensivas como ofensiva, siempre y cuando se respete la normativa del Derecho Internacional.

Como consecuencia de la agresión de Rusia a Ucrania en relación con materia cibernética, surgió la necesidad de estrechar la cooperación para prevenir, detectar y responder frente a ciberataques, por lo que el día 15 y 16 de diciembre de 2022 tuvo lugar el 8º Diálogo Cibernético entre UE-EE. UU.[91] en el que declararon que se deben promover tres ámbitos, como son: el fortalecimiento de las cibercapacidades; mantener un ciberespacio seguro y estable con la cooperación de otras organizaciones internacionales como la OSCE, la Unión Internacional de Telecomunicaciones, el Foro para la Gobernanza de Internet o el G20; y en último lugar, una mejora de la ciberresiliencia, en la que se incide especialmente en la protección de infraestructura críticas, en la que ambas organizaciones comparten enfoques diferentes y buenas prácticas atendiendo cada cual a su normativa, en el caso de la UE, la Directiva NIS 2 y en caso de EE. UU., Ley de notificación de incidentes cibernéticos para infraestructuras críticas.

Asimismo, y como no podía ser de otra manera, se dejó un espacio al sector privado tanto de la industria europea como estadounidense para que estudiaran posibles vías de cooperación para la seguridad del ciberespacio.

#### 2.4.2.2.Ucrania.

Los objetivos de los acuerdos de cooperación entre la UE y Ucrania no son otros que la colaboración en el ámbito de la PCSD, además, unido a la agresión rusa al territorio ucraniano han dado lugar a la 24.ª Cumbre entre la UE y Ucrania en la que se han

[91] CENTRO DE DOCUMENTACIÓN EUROPEA DE ALMERÍA. *Ciberseguridad: La UE celebra su 8º diálogo con Estados Unidos* [en línea]. Fecha de consulta: 14 de abril de 2023. Disponible en: https://www.cde.ual.es/ciberseguridad-la-ue-celebra-su-8o-dialogo-con-estados-unidos/

establecidos debates sobre diversas temáticas, como la respuesta de la UE frente a la agresión rusa, iniciativas de paz, cooperación en el ámbito de la energía, entre otras. No obstante, han dejado un pequeño espacio para la lucha contra las ciberamenazas, en el que han recalcado un compromiso en la cooperación en materia de ciberseguridad, ciberdefensa, en lucha contra la desinformación, así como en la mejora de la ciberresiliencia[92].

Esta asociación se considera como un elemento clave para mantener un ciberespacio seguro ante la agresión rusa, convirtiéndose en un compromiso beneficioso para ambos socios.

Por último, no podría faltar la aportación de las Fuerzas Armadas españolas a Ucrania, que se encargaran de instruir a oficiales en ciberdefensa y en el que entregaran un Centro de Operaciones desplegable. No obstante, esta ayuda será realizada de manera bilateral hasta que se ponga en marcha la misión de entrenamiento de la UE ya aprobada[93].

## 3. CLÁUSULA DE SOLIDARIDAD Y CLÁUSULA DE DEFENSA MUTUA EN CIBERDEFENSA.

La cláusula de solidaridad prevista en el art. 222 del TFUE y la cláusula de defensa mutua en el art. 42.7 del TUE no tienen su origen en el Tratado de Lisboa sino en el Tratado Constitutivo, en el que se establece una doble vía para reforzar la colaboración y la capacidad de respuesta de la UE frente a las amenazas. En este sentido, el Tratado de Lisboa introduce en el TUE varios preceptos relacionados con la defensa de la UE y con la ejecución de la PESC basada en la solidaridad entre los EEMM[94].

---

[92] CONSEJO EUROPEO. *Joint statement following the 24th EU-Ukraine Summit* [en línea]. Fecha de consulta: 14 de abril de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/02/03/joint-statement-following-the-24th-eu-ukraine-summit/

[93] LA RAZÓN. *España entrenará a militares ucranianos en ciberdefensa* [en línea]. Fecha de consulta: 14 de abril de 2023. Disponible en: https://www.larazon.es/espana/20221031/sk4mjp7j3razfmx3ifasa6ezcm.html

[94] RUBIO GARCIA, Dolores. Las cláusulas de asistencia mutua y solidaridad introducidas por el Tratado de Lisboa: el refuerzo de la seguridad y la defensa en la Unión Europea. Documento de Trabajo 57/2011.

En relación con esto, parece ser que se introdujeron estos dos instrumentos por varios motivos entre los que se encuentra la relaciones entre la UE y la OTAN, las amenazas terroristas y la nueva estrategia de seguridad de la UE[95].

En este contexto, los EEMM tienen a su disposición la cláusula de defensa mutua, así como la cláusula de solidaridad, en caso de que se produzca un ciberataque.

### 3.1. Cláusula de solidaridad.

Los trabajos preparatorios sobre la cláusula de solidaridad para proporcionar a la UE una herramienta útil y eficaz para la lucha contra el terrorismo tuvieron en consideración los atentados terroristas del 11-S de 2001 y los del 11-M de 2004.

El Tratado de Lisboa reforzó la cláusula de solidaridad en el Derecho primario, concretamente en el art. 222 del TFUE, Título VII de la Quinta parte del TFUE relacionada con la acción exterior de la UE, y que se desarrolla por la Decisión del Consejo de 24 de junio de 2014 relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad[96]. Pero, además, de desarrollar cada una de esas modalidades, también indica que, el Consejo coordinará la respuesta en caso de que se invoque dicha cláusula.

El art. 222 del TFUE, al igual que el art. 2 de esta Decisión establecen que esta cláusula se podrá invocar en caso de ataque terrorista, catástrofe natural o de origen humano, conforme al TFUE, *"la Unión movilizará todos los instrumentos de que disponga, incluidos los medios militares puestos a su disposición por los Estados miembros"*.

Fecha de consulta: 14 de abril de 2023. Disponible en: https://fundacionalternativas.org/wp-content/uploads/2022/07/64e45a1fa5202c4ef7c1d5e5d58fff4f.pdf

[95] RUBIO GARCIA. Dolores. Las relaciones UE-UEO/OTAN en el contexto del siglo XXI. El Ministerio de Defensa. Creación, desarrollo y consolidación, II Congreso Internacional de Historia de la Defensa, Madrid, Instituto Universitario General Gutiérrez Mellado-UNED, 2008, pp. 134-135.

[96] Decisión del Consejo, de 24 de junio de 2014, relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad. Diario Oficial de la Unión Europea L 192, 1.7.2014, pp. 53–58. Fecha de consulta: 23 de abril de 2023. Disponible en: http://data.europa.eu/eli/dec/2014/415/oj

Esta cláusula ha tenido y tiene una especial incidencia en el ámbito de la defensa, y en particular en la ciberdefensa, como así lo demuestran las diferentes estrategias de ciberseguridad de la UE. La estrategia de ciberseguridad de 2013 apuntaba a que se podría invocar la cláusula de solidaridad, como así lo corrobora la revisión de la estrategia en 2017[97]. Viendo que los ataques cibernéticos se han convertido en unas de las principales amenazas a la seguridad, y que los EEMM son los principales responsables ante una gestión, el Parlamento Europeo en 2012 estimó indispensable establecer a través de una resolución *"solidaridad vinculante entre los Estados miembros y una respuesta coordinada ante dichas amenazas"*[98].

La lectura de este precepto abre algunos interrogantes, puesto que a la hora de la posible aplicación de esta cláusula no se establece si el ataque terrorista es internacional o interno, ni tampoco sobre su gravedad, por lo que conlleva a una cierta ambigüedad que puede derivar en múltiples interpretaciones por parte de los EEMM.

Sin embargo, en el art. 3 b) de la Decisión relativa a las modalidades de la aplicación de la cláusula de solidaridad aparece definido ataque terrorista como delito de terrorismo, tal y como se define en la Decisión marco del Consejo sobre la lucha contra el terrorismo[99], que fue sustituida por la Directiva (UE) 2017/541 relativa a la lucha contra el terrorismo como así lo marca su art. 27[100]. En este contexto, la principal diferencia

[97] Comunicación JOIN (2017) 450 final, pp.
[98] Resolución del Parlamento Europeo, de 22 de noviembre de 2012, sobre las cláusulas de defensa mutua y de solidaridad de la UE: dimensiones política y operativa (2012/2223(INI)). Diario Oficial de la Unión Europea C 419, 16.12.2015, pp. 138–145. Fecha de consulta: 23 de abril de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012IP0456.
[99] Decisión marco del Consejo de 13 de junio de 2002 sobre la lucha contra el terrorismo (2002/475JAI). Diario Oficial de la Unión Europea L 164, 22.6.2002, pp. 3-7. Fecha de consulta: 23 de abril de 2023. Disponible en: http://data.europa.eu/eli/dec_framw/2002/475/oj
[100] Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo, de 15 de marzo de 2017, relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo. Diario Oficial de la Unión Europea L 88, 31.3.2017, pp. 6–21. Fecha de consulta: 23 de abril de 2023. Disponible en: http://data.europa.eu/eli/dir/2017/541/oj, art. 27: *"Queda sustituida la Decisión marco 2002/475/JAI con respecto a los Estados miembros vinculados por la presente Directiva, sin perjuicio de las obligaciones de los Estados miembros en lo concerniente al plazo de transposición de dicha Decisión marco al Derecho interno.*

entre la Directiva de 2002 y la de 2017, es que esta última enmarca los ciberataques como delitos de terrorismo en base a su art. 3 letra i) que dice así: *"la interferencia ilegal en los sistemas de información a tenor del artículo 4 de la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, en los casos en los que sea de aplicación su artículo 9, apartado 3 o apartado 4, letras b) o c), y la interferencia ilegal en los datos a tenor de su artículo 5, en los casos en los que sea de aplicación su artículo 9, apartado 4, letra c)"*.

Respecto al último precepto mencionado, el ataque terrorista se considerará como delito de terrorismo cuando haya interferencias legales que supongan una *"obstaculización o la interrupción significativa del funcionamiento de un sistema de información, introduciendo, transmitiendo, dañando, borrando, deteriorando, alterando, suprimiendo o haciendo inaccesibles datos informáticos, intencionalmente y sin autorización"*, en los casos que se hayan cometido intencionalmente, siempre que hayan afectado a un número significativo de sistemas o cuando para cometerlas se haya utilizado uno de los instrumentos a que se refiere el artículo 7, como un programa informático, una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

De igual modo, el art. 9.4 de la Directiva 2013/40/UE se refiere a las infracciones mencionadas en los art. 4 y 5 de esta misma Directiva, es decir, a la interferencia ilegal en los sistemas de información, ya mencionada, y a la interferencia ilegal, cuando causen daños graves según la letra b), o se cometan contra el sistema de información de una infraestructura crítica, según la letra c).

Aclarando la duda que plantea la literalidad del art. 222 del TFUE, la Decisión del Consejo de 2014 manifiesta que el ataque terrorista puede suceder tanto dentro como fuera del territorio de los EEMM. No obstante, tanto el art. 222 TFUE como el art. 2 de

*Por lo que respecta a los Estados miembros vinculados por la presente Directiva, las referencias a la Decisión marco 2002/475/JAI se entenderán hechas a la presente Directiva."*

la Decisión señalan que el ámbito de aplicación está limitado al territorio de los EEMM, particularmente al territorio del Estado Miembro afectado.

El art. 222 del TFUE, así como la Decisión relativa a las modalidades de la aplicación de la cláusula de solidaridad no forman parte de la PCSD. Esta cláusula no hace mención del uso de la fuerza ni de uso de recursos militares, pero tampoco los prohíbe, y de hecho se ha mantenido que no habría un obstáculo legal para que la UE movilice todos los instrumentos que disponga, incluyendo los militares[101].

Los ciberataques que no recojan todas las características requeridas por la Directiva 2013/40/UE no podrán considerarse como delitos de terrorismo, sino como catástrofe. En este sentido, la Decisión de 2014, en su art. 3 a) define el concepto de catástrofe de la siguiente manera: *"toda situación que tenga o pueda tener efectos graves para las personas, el medio ambiente o los bienes, incluido el patrimonio cultural"*. De modo que, la UE parece que ha escogido por no limitar la aplicabilidad del art. 222 del TFUE, sino, que ha optado por mantener un abanico amplio para que la cláusula de solidaridad pueda ser invocada.

En este contexto, el CCDCOE, pone como ejemplo un ataque de denegación de servicio de larga duración contra las redes públicas y privadas de un país, siendo este totalmente dependiente de los servicios eléctricos, por lo que derivaría en una grave perturbación para los servicios esenciales y para la población[102]. Tras este este ejemplo, puede definirse catástrofe cibernética como aquella catástrofe generada por un ciberataque suficientemente serio como para provocar grandes daños, siendo equivalente a una catástrofe natural y, por tanto, sería una catástrofe de origen humano de las que también reconoce esta cláusula como posibles justificaciones para su invocación.

[101] PIERNAS LÓPEZ, Juan Jorge. Ciberdiplomacia y ciberdefensa…, *op. cit.*, pp. 176.
[102] CCDCOE. *EU Solidarity Clause and 'Cyber Disaster'* [en línea]. Fecha de consulta: 26 de abril de 2023. Disponible en: https://ccdcoe.org/incyder-articles/eu-solidarity-clause-and-cyber-disaster/

Para concluir, los EEMM pueden invocar la cláusula de solidaridad recogida en el art. 222 del TFUE en caso de sufrir un ciberataque grave, ya sea considerado como un delito de terrorismo o como una catástrofe cibernética.

### 3.2.Cláusula de defensa mutua.

La cláusula de defensa mutua se articuló por primera vez en los art. I-40.7 del Tratado Constitucional y en el art. III-214 del Proyecto de Tratado por el que se instituye una Constitución Europea[103], pero actualmente se encuentra prevista en el art. 42.7 del TUE por el cual *"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 Naciones Unidas. Ello se entiende sin perjuicio del carácter específico de la política de seguridad y defensa de determinados Estados miembros".*

El art. 42.7 del TUE forma parte del PCSD, en el que se refleja su carácter bilateral e intergubernamental[104], siendo este el tipo de asistencia ideal en caso de que un Estado Miembro pretenda usar las estructuras políticas y militares de los EEMM.

A lo largo de la política de ciberdefensa de 2022, se observa cómo se hace mención del término de asistencia o defensa mutua, sobre todo, cuando los EEMM sufran incidentes de ciberseguridad graves y no sean capaces de gestionar la situación por ellos mismos. Los conocimientos adquiridos a través de los múltiples ciberejercicios puedan utilizarse para prestar esta cláusula, y en el ámbito de la CEP, concretamente en el desarrollo de los CRRT.

Antes de profundizar en esta temática es necesario equiparar ataque armado al de agresión armada, a pesar de que el término del art. 42.7 del TUE abarca, incluso, casos

[103] URREAS CORRES, Mariola. La política (común) de seguridad y defensa en el Tratado de Lisboa: La eficacia como objetivo, la flexibilidad como instrumento y la ambición como propuesta. *Revista Española de Derecho Europeo.* 2010, n.º 33, pp. 91-120.
[104] RUBIO GARCIA, Dolores. Las cláusulas de asistencia mutua y solidaridad*..., op. cit*., pp. 39.

en los que los EEMM ha sido perjudicado por un ataque que no alcanza el umbral de la legítima defensa ex art. 51 de la Carta de Naciones Unidas[105]. Las razones por las que se va a utilizar agresión armada como sinónimo de ataque armado van desde la mera traducción que se realizó del inglés y del francés[106], hasta un motivo que resulta de vital importancia, ya que si el concepto de agresión armada y de ataque armado ex art. 51 de la Carta fueran distintos no sería posible la invocación de dicha cláusula en caso de ciberataque, como así lo establece la jurisprudencia y la doctrina relativa al art. 51 de la Carta y el Manual de Tallin 2.0.

### 3.2.1. Los ciberataques como agresión armada.

El Comité Político Social aprobó unas directrices de aplicación del conjunto de instrumentos de ciberdiplomacia, que ya en su proyecto[107] establecía, que cuando se produjesen "casos graves" derivados de actividades malintencionadas, los EEMM podrán ejercer su derecho inherente de legítima defensa individual o colectiva recogido en el art. 51 de la Carta.

De conformidad, con el Derecho Internacional, concretamente en su jurisprudencia, la Sentencia del Tribunal Internacional de Justicia de 1986 del caso de las actividades militares y paramilitares en y contra Nicaragua, permite alegar legítima defensa no cuando un Estado se vea afectado por un "uso menor de la fuerza", sino cuando se dé "un uso de la fuerza armada grave" considerada como agresión o ataque armado según el art. 51 de la Carta. En este sentido, lo considerado en esta sentencia se podría aplicar a los ciberataques.

---

[105] SARI, Aurel. The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats. *Harvard National Security Journal*. 2019, n.º 10, pp. 417-419.

[106] El término agresión armada en francés (agresión armée) ha sido traducido a otros idiomas, como al inglés armed attack.

[107] Council of the European Union. Draft implementing guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities 13007/17: *"In grave instances, malicious cyber activities could amount to a use of force or an armed attack within the meaning of the Charter of the United Nations. In this latter case, Member States may choose to exercise their inherent right of individual or collective self-defense as recognized in Article 51 of the Charter of the United Nations […]"*

Si el ciberataque produce la muerte o lesión de personas, daños físicos o la destrucción de infraestructuras críticas de manera significativa pueden generar el derecho de legítima defensa. En este caso, el uso de la fuerza o la gravedad de este puede ser equiparable al que resultarían del uso de armas convencionales[108], incluso podría producir unos efectos comparables al de un ataque nuclear como así lo sugiere STRAUB [109].

En cuanto al grado de gravedad, no se evaluará atendiendo al criterio instrumental, que tiene en cuenta los medios empleados, como así lo señala GUTIERREZ ESPADA[110], ni tampoco el criterio basado en el objetivo[111], en el cual si se lleva a cabo un ciberataque contra una infraestructura crítica se considerará un ataque armado independientemente si ha causado daños o no, sino que habrá que seguir el criterio de las consecuencias, concretamente el alcance, duración, inmediatez (a mayor separación entre acción y efecto, más difícil resulta afirmar "uso de la fuerza") e intrusión, como lo ha afirmado MARTINEZ ATIENZA[112].

Hasta el día de hoy no ha habido ningún ciberataque que haya cumplido los requisitos para considerarse como ataque armado, es necesario traer a colación el ciberataque acontecido en Estonia en 2007, siendo este la primera operación cibernética que afecta de una forma contundente a la seguridad nacional de un país[113]. Esta agresión

[108] MINISTÈRE DE ARMÉES. *Droit International appliqué aux operations dans le cyberspace* [en línea]. Fecha de consulta: 4 de mayo de 2023. Disponible en: https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf

[109] THE CONVERSATION. *A cyberattack could wreak destruction comparable to a nuclear weapon* [en línea]. Fecha de consulta: 1 de mayo de 2023. Disponible en: https://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173#:~:text=A%20cyberattack%20could%20cause%20an,of%20years%20into%20the%20future.

[110] GUTIERREZ ESPADA, Cesáreo. *La legítima defensa y el ciberespacio.* Granada: Comares, 2020, párrafo 24.

[111] LLORENS, M.ª P. Los desafíos del uso de la fuerza en el ciberespacio. *Anuario Mexicano de Derecho Internacional.* 2017, n. º 17, pp. 785-816.

[112] MARTÍNEZ ATIENZA, G. *Ataques en el ciberespacio: conflictos armados y seguridad nacional.* Barcelona: Ediciones Experiencia, 2020, pp. 85. Fecha de consulta: 1 de mayo de 2023. Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/167813?page=1

[113] GANZUA ARTILES, Nestor. Situación de la ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia.* 2011, n.º 149, pp. 165-214.

se produjo tras la retirada de la Estatua del Soldado de Bronce del centro de la capital Tallin, que conmemora a los soldados soviéticos caídos en la II Guerra Mundial. Este tipo de ciberataque denominado DDoS, es decir, de denegación de servicios, todo parece indicar que se lanzó desde Rusia, afectando a bancos y organismos gubernamentales entre otros, originando un gran número de altercados e incluso hubo una persona falleció[114]. Tras estos hechos, Estonia, como víctima del ciberataque y miembro de la OTAN desde el 2004, barajó la posibilidad de aplicar el art. 5 del Tratado de Washington al compararlo con un ataque armado, pero no fue hasta el año 2014, en la Cumbre de Gales, donde se introdujo los ciberataques en dicho Tratado.

El ataque a Estonia fue considerado el primer ciberataque que afectó de una forma contundente. No obstante, a pesar del aumento exponencial de los ciberataques, actualmente, ninguno de ellos cumple con los requisitos para ser calificado como un ataque armado[115].

Por otra parte, pueden que los ciberataques ejecutados de forma individual no traspasen el umbral del art. 51 de la Carta. Sin embargo, el Ministerio de Defensa Francés establece que la acumulación de estos puede ser equiparables al de un ataque armado[116]. De igual manera, cabría ejercitar la legitima defensa cuando se lleven a cabo conjuntamente tanto operaciones físicas como ciberataques, siempre y cuando estén dirigidas a un mismo objetivo[117]. En este contexto, la UE responde a través de una comunicación conjunta de 2016[118] elaborada por la Comisión y por el SEAE, que en caso de que se dieran un conjunto de amenazas híbridas graves, estas podrían constituir una agresión armada contra un EEMM, por lo que se podrían invocar el art. 42.7 del TUE. En

[114] EL CONFIDENCIAL. *La batalla del Soldado de Bronce: lecciones del primer episodio de ciberguerra con Rusia* [en línea]. Fecha de consulta: 1 de mayo de 2023. Disponible en: https://www.elconfidencial.com/mundo/2017-10-02/batalla-estatua-estonia-ciberguerra-rusia_1451408/
[115] Ministère des Armées. *Droit International…*, *op. cit.*, pp. 9
[116] Ministère des Armées. *Droit International…*, *op. cit.*, pp. 9
[117] Ministère des Armées. *Droit International…, op. cit.*, pp. 9
[118] Comunicación Conjunta al Parlamento Europeo y al Consejo. *Comunicación conjunta sobre la lucha contra las amenazas híbridas. Una respuesta de la UE.* JOIN(2016) 18 final. Fecha de acceso: 6 de mayo de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52016JC0018

este sentido, para la UE, la guerra híbrida no solamente supone el uso de operaciones físicas y ciberataques, sino también el del chantaje económico o energético y el uso de la desinformación, como así lo afirma el Coronel SANTAMARÍA VILLASCUERNA y la comunicación conjunta de 2016[119].

Acerca de la posibilidad de invocar la cláusula del art. 42.7 del TUE ante un ciberataque inminente, el derecho a la legítima defensa solo se podría ejercitar en caso de que un Estado sufriera un ataque armado por otro. GUTIERREZ ESPADA entendió que la existencia de un ataque armado es *conditio sine qua non* de una defensa legítima, pero debido a la evolución de la tecnología podría darse esta cláusula cuando el agresor llevó a cabo una consecución de hechos que podrían derivar en un ataque armado[120].

A este respecto, PIERNAS LOPEZ estima que debería poder invocarse el art. 42.7 del TUE, siempre y cuando se cumplan los requisitos de necesidad y proporcionalidad, de conformidad con la jurisprudencia del Tribunal Internacional de Justicia. Sin embargo, en el ámbito de la ciberguerra existe un gran desequilibrio (tecnológico, material, personal) entre las partes pudiendo derivar en una "guerra sin restricciones"[121].

Resulta bastante complicado que se cumplan los principios anteriormente mencionados en relación con un ciberataque, por lo que cabría mejor optar por medidas de Derecho Penal armonizadas a nivel nacional o medidas restrictivas de ciberdiplomacia como las establecidas en la Decisión (PESC) 2019/797 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros, o en el Reglamento (UE) de ejecución 2020/1125 por el que se aplica el Reglamento (UE)

---

[119] SANTAMARÍA VILLASCUERNA, M.A. Amenaza híbrida. La guerra imprevisible. Ministerio De Defensa. XVII Curso Internacional de Defensa, Jaca, Cátedra Miguel de Cervantes Academia General Militar-Universidad de Zaragoza, 2019, pp. 14. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/a/m/amenaza_hibrida._la_guerra_imprevisible.pdf
Véase también Comunicación Conjunta al Parlamento Europeo y al Consejo. Comunicación conjunta sobre la lucha contra las amenazas híbridas*…, op. cit.*, pp.5.

[120] GUITERREZ ESPADA. De la legítima de defensa…, *op. cit.*, párrafo 11.

[121] MARTÍNEZ ATIENZA, G. Ataques en el ciberespacio*…, op. cit.,* pp. 86.

2019/796 relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros[122].

### 3.2.2. Invocación del art. 42.7 contra ciberataques de actores no estatales.

En principio, conforme a la jurisprudencia del Tribunal Internacional de Justicia, el art. 51 de la Carta, solo cabría el derecho de legítima defensa en caso de un ataque armado de un Estado contra otro[123], es decir, es necesario que los ciberataques se hayan cometido por las fuerzas armadas de otro Estado.

No obstante, si se adapta el art. 3 g) de la Resolución 3314 de las Naciones Unidas sobre la definición de agresión[124]a esta cuestión, bandas, grupos u organizaciones podrían llevar a cabo ciberataques en nombre de un Estado, lo que abrió la puerta para la invocación de esta cláusula ante ciberataques llevados a cabo por actores no estatales. Asimismo, cabe destacar que las opiniones dadas por los jueces Koojimans y Simma[125] discrepan de la mayoría, ya que un Estado que sea objeto de un ataque armado no se le puede excluir la posibilidad de la aplicación de la legítima defensa en caso de un ataque armado de un actor no estatal. Pues bien, esta tesis caló tan hondo que el Instituto de Derecho Internacional, adoptó una resolución[126]en la que se podía aplicar, en principio, el art. 51 de la Carta en caso de ataque armado por un actor no estatal.

---

[122] PIERNAS LÓPEZ, Juan Jorge. Ciberdiplomacia y ciberdefensa…, *op. cit.,* pp. 101.
[123] ORGANIZACIÓN DE NACIONES UNIDAS. Opinión Consultiva de la Corte Internacional de Justicia sobre las consecuencias jurídicas de la construcción de un muro en el territorio palestino ocupado, A/ES-10/273. Disponible en: https://www.icj-cij.org/public/files/advisory-opinions/advisory-opinions-2004-es.pdf
[124] Resolución 3314 (XXIX) de la Asamblea General de Naciones Unidas "Definición de la agresión", A/RES/3314, de 14 de diciembre de 1974. Disponible en: https://www.acnur.org/fileadmin/Documentos/BDL/2007/5517.pdf, art. 3 g): *"El envío por un Estado, o en su nombre, de bandas armadas, grupos irregulares o mercenarios que lleven a cabo actos de fuerza armada contra otro Estado de tal gravedad que sean equiparables a los actos antes enumerados, o su sustancial participación en dichos actos"*.
[125] Opinión del juez Simma en la sentencia de 19 de diciembre de 2005, párrafos 8 y 12. Opinión del juez Koojimans, párrafo 27-29.
[126] REISMAN. Michael. Problèmes actuels du recours à la force en droit international. *Annuaire de l'Institut de Droit International*. 2007, n.º 1, pp. 127-237.

En virtud de lo anterior, a juicio de PIERNAS LOPEZ se debe permitir responder a ciberataques de actores no estatales como así lo respalda el caso de Francia, que tras los atentados perpetrados por el Daesh el 13 de noviembre de 2015 en territorio francés, el gobierno galo invocó esta cláusula[127]. Sin embargo, es cierto, que la jurisprudencia del Tribunal Internacional de Justicia no reconoce el derecho de la legítima defensa a los actos perpetrados por actores no estatales, pero el Director de los Servicios Jurídicos del Ministerio de Asuntos Exteriores de Francia manifestó que los ataques efectuados por el Daesh eran graves y que debido al control territorial que ejercía podría ser considerado un proto-Estado[128]o como un "cuasi-estado" como lo definía el Ministerio de Defensa Francés[129]. Además, el Parlamento había respaldado el uso de la legítima defensa de Francia de conformidad con la Carta de Naciones Unidas[130].

En este caso, Francia podía haber invocado cualquier cláusula de las mencionadas hasta el momento, como el art. 5 del Tratado de Washington, la cláusula de solidaridad prevista en el art. 222 del TFUE o la que finalmente fue invocada, la cláusula de defensa mutua ubicada en el art. 42.7 del TUE. Uno de los motivos por lo que se aplicó el art. 42.7 del TFUE y no el art. 222 del TFUE es porque este último estaba limitado al territorio de los EEMM, mientras que el primero no limitaba las actuaciones al territorio de los EEMM, ya que Francia pretendía combatir al Daesh fuera de las fronteras de la UE.

En este contexto, el Estado Miembro que se viera afectado por un ciberataque podrá realizar operaciones con el objetivo de poner fin a estos mediante operaciones dirigidas contra el lugar desde el que se estén produciendo, por lo que resulta recomendable la invocación de la cláusula de defensa mutua en vez de la cláusula de

[127] PIERNAS LÓPEZ, Juan Jorge. Ciberdiplomacia y ciberdefensa*…, op. cit.*, pp. 172.
[128] ALABRUNE, François. Fondements juridiques de l'intervention militaire française contre Daech en Irak et en Syrie. *Revue generale de droit international public.* 2016, n.º 1, pp. 41-50.
[129] Ministère des Armées. *Droit International…, op. cit.,* pp. 9
[130] Resolución del Parlamento Europeo, de 22 de noviembre de 2012, sobre las cláusulas de defensa mutua y de solidaridad de la UE: dimensiones política y operativa (2012/2223(INI)). Fecha de consulta: 23 de abril de 2023. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012IP0456.

solidaridad[131]. Ahora bien, se dejó abiertas las puertas con la posibilidad de poder adoptar una serie de medidas contra el Daesh en un futuro, siendo más conveniente aplicar la cláusula de defensa mutua[132].

No solamente la UE tiene un instrumento que asegure la disuasión, sino que la OTAN cuenta con el art. 5 del Tratado de Washington, unas herramientas que a priori pueden parecer similares, sin embargo, la cláusula de la OTAN está más limitada que la de la UE, ya que solo es posible aplicarla en una esfera militar, mientras que la cláusula de defensa mutua ofrece un abanico muy amplio en diversas materias como la económica, diplomática, información, legislación o comercio[133].

[131] PIERNAS LÓPEZ, Juan Jorge. Ciberdiplomacia y ciberdefensa*…, op. cit.,* pp. 183

[132] FALEG, Giovani. European security after the Paris attacks. Commentary, 24 November 2015. Documento político. Fecha de consulta: 16 de mayo de 2023. Disponible en: http://aei.pitt.edu/id/eprint/69683

[133] PONTIJAS CALDERÓN, José Luis. Unión Europea: ciberseguridad y ciberdefensa. Documento de Opinión IEEE 04/2023, pp. 12. Fecha de consulta: 16 de mayo. Disponible en: https://www.ieee.es/Galerias/fichero/docs_analisis/2023/DIEEEA04_2023_JOSPON_Europa.pdf

## 4. CONCLUSIONES.

**Primera-.** El uso de Internet y de las TIC se ha vuelto totalmente indispensable en las sociedades avanzadas, no siendo una excepción la UE, en la que sus ciudadanos, instituciones o empresas utilizan más que nunca, este entorno denominado ciberespacio, que al igual que presenta un mundo lleno de posibilidades, también está colmado de riesgos y amenazas. En este sentido, cada vez más infraestructuras críticas se encuentran en el ciberespacio y hoy pensar en una economía contemporánea sin red es realmente imposible, es decir, el futuro está en el ciberespacio.

**Segunda-.** La ciberdefensa de la UE se ha visto expuesta a una gran evolución desde sus orígenes, conformándose como un sostén para la estrategia de seguridad nacional de los EEMM, ya que este ámbito es tan delicado y complejo que confluyen diferentes versiones entre cada uno de los países, por lo que resulta bastante complicado configurar una política común en este ámbito. A pesar de las dificultades es necesario poner de relevancia los valores e intereses compartidos, aunque no fueran perfectamente concordantes.

No obstante, el año 2017, marco un punto de inflexión en la ciberdefensa con la llegada de la Comunicación sobre la resiliencia, disuasión y defensa para fortalecer la ciberseguridad de la UE, y, por otro lado, la CEP a través de la cual se pone de relevancia la cooperación de defensa en esta materia.

Respecto de la CEP, los primeros pasos para que la UE se convierta en una figura relevante en materia de ciberdefensa pasa por el programa PESCO y por los FED, que lograría que la UE se convirtiera en un competidor de EE. UU. En este sentido, resulta irónico que las objeciones para llevar a cabo este proyecto provengan de EE. UU., por lo que se vería con buenos ojos desde Rusia y China. Pese a ello, EE. UU seguirá siendo un fiel socio de la UE debido a los valores y principios que comparten estas dos potencias, aunque no hay que olvidar los impedimentos que también conllevan.

**Tercera-.** La UE no es capaz de desarrollar con más eficacia su política de ciberdefensa por dos motivos. Por un lado, hace varios años atrás países como Francia, Reino Unido,

en su momento, o Alemania, en menor medida, limitaban las posibilidades de que brote la UE como una gran potencia en esta esfera, ya que tienen una gran capacidad de decisión en estos temas y ven la ciberdefensa como un elemento central de su defensa, un componente secreto para la defensa del territorio. Por otro lado, el papel de la OTAN en la ciberdefensa, al igual que en todo el espectro de defensa, es firme e insoslayable, lo que supone en cierta manera, aceptar el mandato de Washington, quien dirige a su antojo dicha organización, lo cual conlleva una dejación de la autonomía europea, aceptando un planteamiento que, en ciertas ocasiones, será contrario a los propios intereses de la UE. A este respecto, la UE debe creerse que es un protagonista a nivel mundial, es decir, Bruselas debe ser capaz de aplicar, en este caso la política de ciberdefensa, en cooperación con otras potencias, cuando los intereses coincidan y debe rechazar aquellos intereses que puedan mermar el porvenir de Europa. Asimismo, es importante destacar que la ciberdefensa de la UE, por supuesto deberá reforzar su ciberdefensa sin caer en duplicidades con la OTAN.

En resumen, la actuación de la UE no consistirá en actuar al margen de EE. UU. sino en ser capaces de actuar cuando estén juego intereses europeo y Washington no esté dispuesto a intervenir.

**Cuarta-.** Atendiendo al voluble contexto geopolítico que vivimos hoy en día, unido a diversos acontecimientos que se han ido dando, como el Brexit, que ha supuesto que el Reino Unido abandone la UE, lo que ha dejado ha supuesto la pérdida de una gran cantidad de expertos de ciberdefensa. Tras este hecho, Francia o Alemania que en un principio se veían reticentes a compartir cierta información en esta materia dieron paso adelante para fortalecer esta disciplina en la UE. Además, es fundamental destacar que la evasión del multilateralismo por parte de la administración Trump, que, aunque estemos a 2023 todavía se ve reflejada, ha crecido una voluntad entre los dirigentes de alcanzar una autonomía estratégica, destacando como un elemento fundamental la ciberdefensa.

**Quinta-.** En diversas ocasiones, se ha planteado la posibilidad de crear un Ejército Europeo, y con ello la posibilidad de especializar a las tropas en un ámbito en concreto, como es la ciberdefensa para así hacer frente a las ciberamenzas, ciberincidentes y ciberataques de los enemigos. Parece ser que desde hace ya unos años los líderes europeos debaten sobre esta cuestión, sin embargo, no se ha hecho un gran esfuerzo para hacerlo realidad ya que, entre las dos grandes potencias de la UE, como son Francia o Alemania, pueden surgir discrepancias en cuanto a la organización, estructura, localización o mandos del posible futuro Ejército Europeo. Además, implicaría una cesión de su soberanía y a su vez derivaría en obstáculos en los EEMM siendo incapaces de proteger sus intereses propios.

**Sexta-.** Siguiendo en una esfera geopolítica es digno de desatacar no solamente la aparición de EEMM como elementos de almacenamiento e intercambio de información, sino que se produce una irrupción técnico-corporativa de las esferas sociales -políticas en la que se encuentra empresas como Facebook que adquiere una gran cantidad de información con posibilidad de generar un impacto económico, como es el caso de cambios de influencia en cambio electorales, que derivan en nuevas lógicas políticas ¿Qué es información privada? ¿Qué compartimos? ¿Qué no compartimos? En ocasiones cuando se descarga una aplicación en alguno de nuestros dispositivos, lo que estamos permitiendo es que tengan acceso a nuestro comportamiento y esa información, en teoría, se utiliza para ofrecerte una mejor publicidad.

De esta forma, en la actualidad, uno de los desafíos que encontramos es la falta de ética producida por una gran cantidad de vacíos legales en el ciberespacio ¿Cómo interactúan las personas? ¿Cómo se han generado empresas con algoritmos que tratan de decodificar el comportamiento de seres humanos? ¿Cómo funciona el tema de reconocimiento de la vigilancia en las ciudades?

**Séptima-.** A raíz de lo anterior, se encuentran otra serie de debates como la desinformación, en esta ocasión muchas veces estas campañas se disfrazan en una gran

multitud de comentarios como: me equivoqué, no fue a propósito y en la que aparecen el concepto de "fake news" que consiste en dar mala información adrede, intentando viralizar noticias falsas para generar un impacto social, político o económico.

**Octava-.** Los EEMM cuentan con una serie de instrumentos para hacer frente a los ciberataques, en particular, la cláusula de solidaridad y de defensa mutua, prevista en el art. 222 del TFUE y el art. 42.7 del TUE. Los Estados podrán aplicar estas herramientas atendiendo a sus intereses y a unos criterios legales establecidos, que estarán influenciados por las decisiones políticas del propio Estado, asimismo, se tendrá en cuenta la incidencia que tendrá sobre las instituciones europeas.

**Novena-.** Un factor a tener en cuenta a la hora de aplicar una u otra cláusula sería el ámbito territorial, menguando la capacidad de respuesta ante ciberataques en caso de que se elija la cláusula de solidaridad, ya que la decisión más acertada si se quiere actuar militarmente sería la cláusula de defensa mutua.

## 5. BIBLIOGRAFÍA.


ALABRUNE, François. Fondements juridiques de l'intervention militaire française contre Daech en Irak et en Syrie. *Revue generale de droit international public.* 2016, n.º 1.

ALONSO LECUIT, Javier. Evolución de la agenda de ciberseguridad de la Unión Europea. Real Instituto Elcano. 2018, n.º 121.

CAMPUS INTERNACIONAL PARA LA SEGURIDAD Y LA DEFENSA (CISDE). *El COVID-19 acelera la transformación tecnológica de la OTAN* [en línea]. Fecha de consulta: 9 de abril de 2023. Disponible en: https://observatorio.cisde.es/actualidad/el-covid-19-acelera-la-transformacion-tecnologica-de-la-otan/

CCDCOE. *EU Solidarity Clause and 'Cyber Disaster'* [en línea]. Fecha de consulta: 26 de abril de 2023. Disponible en: https://ccdcoe.org/incyder-articles/eu-solidarity-clause-and-cyber-disaster/

CENTRO DE DOCUMENTACIÓN EUROPEA DE ALMERÍA. *Ciberseguridad: La UE celebra su 8º diálogo con Estados Unidos* [en línea]. Fecha de consulta: 14 de abril de 2023. Disponible en: https://www.cde.ual.es/ciberseguridad-la-ue-celebra-su-8o-dialogo-con-estados-unidos/

CENTRO DE DOCUMENTACIÓN EUROPEA DE ALMERÍA. *La UE necesita una mayor cooperación para mitigar los riesgos de las infraestructuras marítimas críticas* [en línea]. Fecha de consulta: 26 de junio de 2023. Disponible en: https://www.cde.ual.es/la-ue-necesita-una-mayor-cooperacion-para-mitigar-los-riesgos-de-las-infraestructuras-maritimas-criticas/

CENTRE DELÀS D'ESTUDIS PER LA PAU. Informe 53: «La OTAN, construyendo inseguridad global». Fecha de consulta: 12 de abril de 2023. Disponible en: https://centredelas.org/wp-content/uploads/2022/06/informe53_OTANConstruyendoInseguridadGlobal_CAST.pdf

CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL. La cooperación estructurada permanente en el marco de la Unión Europea. Documentos de seguridad y defensa 42. Fecha de consulta: 1 de junio de 2023. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF81.pdf

COMISIÓN EUROPEA. *Empiezan a aplicarse nuevas normas más estrictas para la resiliencia cibernética y física de las entidades y redes críticas* [en línea]. Fecha de consulta: 23 de marzo de 2023. Disponible en: https://digital-strategy.ec.europa.eu/es/news/new-stronger-rules-start-apply-cyber-and-physical-resilience-critical-entities-and-networks

COMISIÓN EUROPEA. *Preguntas y respuestas: La política de ciberdefensa de la UE* [en línea], Fecha de consulta: 6 de marzo de 2023. Disponible en: https://ec.europa.eu/commission/presscorner/detail/es/qanda_22_6643

COMISIÓN EUROPEA. *European Defence Industrial Development Programme (EDIDP)* [en línea]. Fecha de consulta: 28 de marzo de 2023. Disponible en: https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_es

CONSEJO EUROPEO. *Joint statement following the 24th EU-Ukraine Summit* [en línea]. Fecha de consulta: 14 de abril de 2023. Disponible en: https://www.consilium.europa.eu/es/press/press-releases/2023/02/03/joint-statement-following-the-24th-eu-ukraine-summit/

CÓZAR MURILLO, Beatriz. La cooperación estructurada permanente: ¿El impulso definitivo que necesita la política común de seguridad y defensa? Boletín IEEE. 2017, n.º 8.

DEPARTAMENTO DE SEGURIDAD NACIONAL. *Acuerdo Cyber Pledge de la OTAN* [en línea]. Fecha de consulta: 19 de junio de 2023. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/acuerdo-cyber-pledge-otan

DEPARTAMENTO DE SEGURIDAD NACIONAL. *La OTAN y la UE aumentan la cooperación en ciberseguridad* [en línea]. Fecha de consulta: 10 de abril de 2023. Disponible en: https://www.dsn.gob.es/es/actualidad/sala-prensa/otan-ue-aumentan-cooperaci%C3%B3n-ciberseguridad

DEPARTAMENTO DE SEGURIDAD NACIONAL. *Unión Europea-Ciberseguridad* [en línea]. Fecha de consulta: 7 de marzo de 2023. Disponible en: https://www.dsn.gob.es/en/actualidad/seguridad-nacional-ultima-hora/uni%C3%B3n-europea-%E2%80%93-ciberseguridad-15

EL CONFIDENCIAL. *La batalla del Soldado de Bronce: lecciones del primer episodio de ciberguerra con Rusia* [en línea]. Fecha de consulta: 1 de mayo de 2023. Disponible en: https://www.elconfidencial.com/mundo/2017-10-02/batalla-estatua-estonia-ciberguerra-rusia_1451408/

ENISA. *Blue OLEx 2022 tests the Standard Operating Procedures of the EU CyCLONe* [en línea]. Fecha de consulta: 15/03/2023. Disponible en: https://www.enisa.europa.eu/news/blue-olex-2022-tests-the-standard-operating-procedures-of-the-eu-cyclone

ENISA. *European Cybersecurity Skills Framework (ECSF)* [en línea]. Fecha de consulta: 6 de abril de 2023. Disponible en: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

AGENCIA EUROPEA DE DEFENSA. Fact sheet: *Capability Development Plan* [en línea]. Fecha de consulta: 1 de junio de 2023. Disponible en: https://eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0f

AGENCIA EUROPEA DE DEFENSA. Fact Sheet: *Cyber Phalanx* [en línea]. Fecha de consulta: 1 de marzo de 2023. Disponible en: https://eda.europa.eu/docs/default-source/eda-factsheets/cyph-fact-sheet_v04.pdf

AGENCIA EUROPEA DE DEFENSA. CYBER PHALANX: *EDA's dedicated cyber training for Operation Planners wraps in Portugal* [en línea]. Fecha de consulta: 8 de marzo de 2023. Disponible en: https://eda.europa.eu/news-and-events/news/2021/10/05/EDA-cyber-phalanx-wraps-in-portugal

AGENCIA EUROPEA DE DEFENSA. *European Defence Fund (EDF)* [en línea]. Fecha de consulta: 2 de abril de 2023. Disponible en: https://eda.europa.eu/what-we-do/EU-defence-initiatives/european-defence-fund-%28edf%29

AGENCIA EUROPEA DE DEFENSA. *European defence standardisation* [en línea]. Fecha de consulta: 16 de marzo de 2023. Disponible en: https://eda.europa.eu/what-we-do/all-activities/activities-search/materiel-standardisation

AGENCIA EUROPEA DE DEFENSA. *European Defence Standards Reference System (EDSTAR)* [en línea]. Fecha de consulta: 16 de marzo de 2023. Disponible en: https://edstar.eda.europa.eu/

AGENCIA EUROPEA DE DEFENSA. Fact sheet: *Hub for Defence Innovation (HEIDI)* [en línea]. Fecha de consulta: 6 de marzo de 2023. Disponible en: https://eda.europa.eu/docs/default-source/brochures/hedi-factsheet-(final).pdf

AGENCIA EUROPEA DE DEFENSA. *Overarching Strategic Research Agenda and CapTech SRAs Harmonisation* [en línea]. Fecha de consulta: 28 de marzo de 2023. Disponible en: https://eda.europa.eu/docs/default-source/brochures/eda-osra-brochure.pdf

AGENCIA EUROPEA DE DEFENSA. *Second EDA Live Cyber Exercise for Military CERTs Concluded* [en línea]. Fecha de consulta: 6 de marzo de 2023. Disponible en: https://eda.europa.eu/news-and-events/news/2022/01/26/second-eda-live-cyber-exercise-for-military-certs-concluded

FALEG, Giovani. European security after the Paris attacks. Commentary, 24 November 2015. Documento político. Fecha de consulta: 16 de mayo de 2023. Disponible en: http://aei.pitt.edu/id/eprint/69683

FUNDACIÓN GALICIA EUROPEA. *Ciberdefensa: hacia unas capacidades más sólidas de la UE en pro de una cooperación operativa eficaz, la solidaridad y la resiliencia* [en línea]. Fecha de consulta: 19 de mayo de 2023. Disponible en: https://fundaciongaliciaeuropa.eu/es/ciberdefensa-cara-a-unhas-capacidades-mais-solidas-da-ue-en-prol-dunha-cooperacion-operativa-eficaz-a-solidariedade-e-a-resiliencia/

GANZUA ARTILES, Nestor. Situación de la ciberseguridad en el ámbito internacional y en la OTAN. *Cuadernos de estrategia.* 2011, n.º 149.

GARCÍA CID, Marta Irene. Criptografía cuántica: hacia una autonomía estratégica [en línea]. Fecha de consulta: 28 de marzo de 2023. Disponible en: https://www.linkedin.com/pulse/criptograf%C3%ADa-cu%C3%A1ntica-hacia-una-autonom%C3%ADa-estrat%C3%A9gica-indra/?trk=organization_guest_main-feed-card_feed-article-content&originalSubdomain=es

GUTIERREZ ESPADA, Cesáreo. La ciberguerra y el Derecho internacional. En MARTÍNEZ PÉREZ, Enrique. Las amenazas a la seguridad internacional hoy. Valencia: Tirant lo Blanch, 2017.

GUTIERREZ ESPADA, Cesáreo. La legítima defensa y el ciberespacio. Granada: Comares, 2020.

INSTITUTO ESPAÑOL DE ESTUDIOS ESTRATÉGICOS. Política de Defensa Común. *Revista del Instituto Español de Estudios Estratégicos*. 2017, n.º 9.

LA RAZÓN. *España entrenará a militares ucranianos en ciberdefensa* [en línea]. Fecha de consulta: 14 de abril de 2023. Disponible en: https://www.larazon.es/espana/20221031/sk4mjp7j3razfmx3ifasa6ezcm.html

LLORENS, M.ª P. Los desafíos del uso de la fuerza en el ciberespacio. Anuario Mexicano de Derecho Internacional. 2017, n. º 17.

MACHIN OSÉS, Nieva y GAZAPO LAPAYESE, Manuel. La ciberseguridad como factor crítico en la seguridad de la Unión Europea. *Revista UNISCI*. 2016, n.º 42.

MARTÍNEZ ATIENZA, G. *Ataques en el ciberespacio: conflictos armados y seguridad nacional.* Barcelona: Ediciones Experiencia, 2020. Fecha de consulta: 1 de mayo de 2023. Disponible en: https://elibro-net.unileon.idm.oclc.org/es/ereader/unileon/167813?page=1

MINISTÈRE DE ARMÉES. *Droit International appliqué aux operations dans le cyberspace* [en línea]. Fecha de consulta: 4 de mayo de 2023. Disponible en: https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf

NOGUERA GÓMEZ, F, MARTINEZ MARTÍNEZ, D, FERNANDEZ VALERA y PÉREZ CÁCERES, M. La UE y la OTAN ante los nuevos escenarios de la seguridad y la defensa. Revista Española de Defensa. Diciembre 2022.

OFICINA DE PUBLICACIONES DE LA UNIÓN EUROPEA. *Cooperación estructurada permanente en materia defensa y seguridad* [en línea]. Fecha de consulta: 1 de junio de 2023. Disponible en: https://publications.europa.eu/resource/cellar/354b8739-f4aa-11e8-9982-01aa75ed71a1.0003.02/DOC_1

ORGANIZACÓN DE NACIONES UNIDAS. Opinión Consultiva de la Corte Internacional de Justicia sobre las consecuencias jurídicas de la construcción de un muro en el territorio palestino ocupado, A/ES-10/273. Disponible en: https://www.icj-cij.org/public/files/advisory-opinions/advisory-opinions-2004-es.pdf

PARLAMENTO EUROPEO. *Cyber: How big is the threat?* [en línea]. Fecha de consulta: 19 de junio de 2023. Disponible en: https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/637980/EPRS_ATA(2019)637980_EN.pdf

PARLAMENTO EUROPEO. Informe sobre ciberdefensa (2018/2004(INI)). Fecha de consulta: 11 de abril de 2023. Disponible en: https://www.europarl.europa.eu/doceo/document/A-8-2018-0189_ES.html

PESCO PROJECTS. *Cyber Ranges Federation* [en línea]. Fecha de consulta: 8 de marzo de 2023. Disponible en: https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/

PESCO PROJECTS. *EU Cyber Academia and Innovation Hub* [en línea]. Fecha de consulta: 6 de abril de 2023. Disponible en: https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/

PIERNAS LÓPEZ, Juan Jorge. Ciberdiplomacia y ciberdefensa en la Unión Europea. Cizur Menor (Navarra): Aranzadi, 2020, pp. 143.

PONTIJAS CALDERÓN, José Luis. Unión Europea: ciberseguridad y ciberdefensa. Documento de Opinión IEEE 04/2023, pp. 12. Fecha de consulta: 16 de mayo. Disponible en: https://www.ieee.es/Galerias/fichero/docs_analisis/2023/DIEEEA04_2023_JOSPON_Europa.pdf

REISMAN. Michael. Problèmes actuels du recours à la force en droit international. *Annuaire de l'Institut de Droit International.* 2007, n.º 1.

RUBIO DAMIÁN, Francisco. Necesidad de una nueva estrategia europea de seguridad. *Revista Ejército*. 2012, n.º 860.

RUBIO GARCIA, Dolores. Las cláusulas de asistencia mutua y solidaridad introducidas por el Tratado de Lisboa: el refuerzo de la seguridad y la defensa en la Unión Europea. Documento de Trabajo 57/2011. Fecha de consulta: 14 de abril de 2023. Disponible en: https://fundacionalternativas.org/wp-content/uploads/2022/07/64e45a1fa5202c4ef7c1d5e5d58fff4f.pdf

RUBIO GARCIA. Dolores. Las relaciones UE-UEO/OTAN en el contexto del siglo XXI. El Ministerio de Defensa. Creación, desarrollo y consolidación, II Congreso Internacional de Historia de la Defensa, Madrid, Instituto Universitario General Gutiérrez Mellado-UNED, 2008.

SANTAMARÍA VILLASCUERNA, M.A. Amenaza híbrida. La guerra imprevisible. Ministerio De Defensa. XVII Curso Internacional de Defensa, Jaca, Cátedra Miguel de Cervantes Academia General Militar-Universidad de Zaragoza, 2019. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/a/m/amenaza_hibrida._la_guerra_imprevisible.pdf

SARI, Aurel. The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats. Harvard National Security Journal. 2019, n.º 10.

THE CONVERSATION. *A cyberattack could wreak destruction comparable to a nuclear weapon* [en línea]. Fecha de consulta: 1 de mayo de 2023. Disponible en: https://theconversation.com/a-cyberattack-could-wreak-destruction-comparable-to-a-nuclear-weapon-112173#:~:text=A%20cyberattack%20could%20cause%20an,of%20years%20into%20the%20future.

TRINBERG, Lorena. *EU Cyber Defence Policy Framework Presents More Than 40 Action Measures* [en línea]. Fecha de consulta: 26 de mayo de 2023. Disponible en: https://ccdcoe.org/incyder-articles/eu-cyber-defence-policy-framework-presents-more-than-40-action-measures/

URREAS CORRES, Mariola. La política (común) de seguridad y defensa en el Tratado de Lisboa: La eficacia como objetivo, la flexibilidad como instrumento y la ambición como propuesta. *Revista Española de Derecho Europeo*. 2010, n.º 33.