
# I. INTRODUCCIÓN

El retorno de la guerra a Europa, con la agresión militar injustificada y no provocada de Rusia contra Ucrania, ha sido una seria advertencia para todos aquellos que ponen en tela de juicio el enfoque de la UE en materia de seguridad y defensa y su capacidad para promover su visión y defender sus intereses incluso en el ciberespacio. Los regímenes autoritarios están tratando de cuestionar y socavar el orden internacional basado en normas en el ciberespacio, convirtiéndolo en un ámbito cada vez más discutido, al igual que la tierra, el mar, el aire y el espacio. En los últimos años se han intensificado los comportamientos maliciosos en el ciberespacio por parte de agentes tanto estatales como no estatales, y se ha registrado en la UE un creciente número de ciberataques contra infraestructuras críticas militares y civiles, así como contra las misiones y operaciones desplegadas.

La frontera entre las dimensiones civil y militar del ciberespacio está desdibujada, como han demostrado los recientes ataques contra las redes energéticas, las infraestructuras de transporte y los activos espaciales. Estos sucesos ilustran también la interdependencia entre las infraestructuras físicas y digitales y el potencial de que los incidentes de ciberseguridad importantes alteren o dañen infraestructuras críticas. Nos ponen frente a la cruda realidad de que la UE necesita una estrecha cooperación militar y civil en el ciberespacio para ejercer con más firmeza su papel de garante de la seguridad

La UE debe asumir mayores responsabilidades, por su propia seguridad. Para ello, es preciso contar con unas fuerzas armadas europeas modernas e interoperables. Por consiguiente, los Estados miembros deben comprometerse, de forma urgente y prioritaria, a aumentar sus inversiones en capacidades de ciberdefensa de amplio espectro, incluidas las de defensa activa. Sin perjuicio de su inquebrantable compromiso con el cumplimiento del Derecho y las leyes internacionales aplicables en el ciberespacio, la UE debe manifestar su intención de utilizar estas capacidades de manera coordinada en caso de ciberataque contra un Estado miembro.

Para ello, debe afianzar su soberanía tecnológica y digital en el ámbito cibernético. La capacidad de actuación de la UE dependerá de su capacidad para dominar y desarrollar tecnologías de vanguardia para la ciberseguridad y la ciberdefensa en la UE. Habida cuenta de que las cibertecnologías encierran un alto potencial de doble uso, las industrias de ciberseguridad y ciberdefensa, la investigación y el desarrollo y las actividades de innovación deben generar muchas más sinergias para desarrollar unas mejores capacidades.

La prevención y la detección comunes son una parte importante de las capacidades de defensa de la UE; esta debe tener la capacidad de detectar ataques en fases precoces. Los datos de detección deben convertirse en inteligencia ejecutable que pueda ponerse al servicio tanto de la ciberseguridad como de la ciberdefensa. Esa cooperación entre las cibercomunidades de defensa y civil sienta los cimientos necesarios para mejorar una conciencia situacional común del ciberespacio y es, además, crucial a la hora de ofrecer una respuesta coordinada a las crisis tanto a nivel técnico como operativo.

El conflicto armado en Ucrania también ha puesto de relieve el valor de una estrecha cooperación con el sector privado y la necesidad de tener acceso a proveedores privados de confianza que sirvan de ciberreservas para ampliar la respuesta en caso de ciberataques de gravedad. Es por lo tanto necesario garantizar que los Estados miembros puedan contar con el apoyo, en condiciones seguras y coordinadas, de tales ciberreservas de confianza.

La presente Comunicación conjunta, aunque parte del marco político de ciberdefensa[[1]](#footnote-2), propone una estrategia ambiciosa que permita a la UE y sus Estados miembros actuar con aplomo y asertividad en el ciberespacio. Su objetivo es potenciar las capacidades de ciberdefensa a través de la acción individual o conjunta de los Estados miembros y reforzar la coordinación y la cooperación entre las cibercomunidades de la UE. Otro de sus objetivos es reducir las dependencias estratégicas de la UE en lo que respecta a las cibertecnologías críticas y a robustecer la base industrial y tecnológica de la defensa europea (BITDE). Esta política fijará las reglas del juego de la UE y propondrá formas de reforzar la solidaridad interna de la UE en materia de ciberdefensa, así como de cooperar con el sector privado para ampliar la respuesta a los ciberataques graves. Teniendo en cuenta la naturaleza transnacional de las ciberamenazas, creará asociaciones mutuamente beneficiosas y específicamente adaptadas a cada caso en el ámbito de la ciberdefensa, desarrollará las capacidades de ciberdefensa y mejorará la ciberresiliencia de los países socios.

Conforme a lo propuesto en el documento titulado «Brújula Estratégica para la Seguridad y la Defensa»[[2]](#footnote-3), adoptado por el Consejo en marzo de 2022, la presente política de ciberdefensa mejorará la capacidad de prevención, detección, defensa, recuperación y disuasión con respecto a los ciberataques dirigidos a la UE y a sus Estados miembros, recurriendo a todos los medios disponibles. Estos objetivos se ajustan a las prioridades digitales de la Comisión, a la ambición plasmada en la Estrategia de Ciberseguridad de la UE de 2020[[3]](#footnote-4), a lo anunciado por la presidenta Von der Leyen en su discurso sobre el estado de la Unión de 2021[[4]](#footnote-5) y a las Conclusiones del Consejo sobre el desarrollo de la posición cibernética de la Unión Europea[[5]](#footnote-6), de 23 de mayo de 2022. La Comunicación conjunta de 2022 sobre los déficits de inversión en defensa[[6]](#footnote-7) también animaba a la UE y a sus Estados miembros a que iniciasen una labor de desarrollo de una capacidad de ciberdefensa de amplio espectro: desde la investigación a la respuesta, pasando por la detección y la protección.

# II. UNA CIBERDEFENSA DE LA UE PARA LA PROTECCIÓN, DETECCIÓN, DISUASIÓN Y DEFENSA RESPECTO DE LOS CIBERATAQUES

**1. Acción común por una mejor ciberdefensa**

Los ciberataques suelen ser de carácter transfronterizo y pueden causar un impacto físico en infraestructuras críticas de la UE. Las perturbaciones provocadas por los incidentes de ciberseguridad importantes pueden llegar a ser demasiado graves como para que el Estado miembro o los Estados miembros afectados las gestionen por sí solos. A veces forman parte de los ataques híbridos de mayor envergadura perpetrados por terceros países con el objetivo de desestabilizar la economía y a la sociedad, debilitar las infraestructuras críticas necesarias para garantizar la seguridad de la UE o socavar y deteriorar el funcionamiento de las democracias, por ejemplo mediante ataques a las infraestructuras electorales.

En 2018, la UE identificó el ciberespacio como dominio de operaciones militares. La «Visión militar y estrategia sobre el ciberespacio como dominio de operaciones»[[7]](#footnote-8), adoptada en 2021, establece las condiciones marco y describe los fines, las formas y los medios necesarios para utilizar el ciberespacio como dominio de operaciones, en apoyo de las operaciones de la política común de seguridad y defensa (PCSD) de la UE. La ciberdefensa y la utilización de las capacidades correspondientes en todo el espectro de las operaciones militares en el ciberespacio es una prerrogativa nacional de los Estados miembros, si bien depende de un ecosistema más amplio del que forma parte una sólida base industrial respaldada por el desarrollo de capacidades a escala de la UE.

La comunidad de ciberdefensa de la UE, compuesta por las autoridades de defensa de los Estados miembros y apoyada por las instituciones, órganos y organismos de la UE (IOUE), presenta ciertas especificidades en comparación con las demás cibercomunidades[[8]](#footnote-9) y sigue un modelo de gobernanza diferente. La ausencia de un marco establecido para el intercambio de información y la cooperación entre los equipos militares de respuesta a emergencias informáticas de la UE (CERT militares), particularmente en apoyo de las misiones y operaciones militares de la PCSD, supone un problema ante el creciente nivel de las ciberamenazas por parte de agentes estatales y no estatales.

La cooperación entre las cibercomunidades civil, diplomática y policial y sus homólogas en el sector de la defensa aportará un alto valor añadido a todas las partes interesadas. Es, por lo tanto, fundamental propiciar dicha colaboración ofreciendo medios adecuados y seguros de intercambio de información y emprender ejercicios y demás actividades que generen una confianza y un entendimiento comunes.

Además, actualmente solo existe una asistencia operativa mutua limitada entre los Estados miembros Es necesario explorar la ampliación del concepto de ciberequipos de reacción rápida en toda la UE a partir del proyecto conexo sobre Equipos de Respuesta Telemática Rápida y de Asistencia Mutua en el ámbito de la Ciberseguridad (CRRT)[[9]](#footnote-10), de la cooperación estructurada permanente (CEP), y en el marco del artículo 42, apartado 7, del Tratado de la Unión Europea (TUE)[[10]](#footnote-11) («cláusula de asistencia mutua») y del artículo 222 del Tratado de Funcionamiento de la Unión Europea (TFUE)[[11]](#footnote-12) («cláusula de solidaridad»). En esa misma línea, una de las enseñanzas extraídas del éxito de la ciberdefensa ucraniana en el contexto de la guerra de agresión provocada por Rusia es el papel decisivo que desempeña el sector privado. Por lo tanto, debe estudiarse la medida en la que el sector privado podría contribuir también a mejorar la ciberrespuesta.

### 1.1 Refuerzo de la conciencia situacional y la coordinación de la comunidad de defensa

Dada la magnitud del riesgo asociado a los ciberataques, los Estados miembros deben adquirir la conciencia situacional colectiva más plena que sea posible y que incluya la capacidad de detección precoz, así como los recursos necesarios para ofrecer una respuesta adecuada y lograr una recuperación solidaria y coordinada.

Por lo que respecta a la conciencia situacional en el ámbito militar, es necesario crear un **Centro de Coordinación de la Ciberdefensa de la UE** que genere una mejor conciencia situacional en el seno de la comunidad de defensa, incluidos todos los mandos militares de la PCSD de la UE. El Alto Representante someterá a los Estados miembros, para su consideración, la propuesta correspondiente, que se basará en el proyecto de Centro de coordinación del ámbito del ciberespacio y de la información (CIDCC) de la CEP[[12]](#footnote-13). Su objetivo será ofrecer un análisis holístico del ciberespacio, el entorno electromagnético y el ámbito cognitivo, reuniendo con tal fin diferentes fuentes de información a los niveles estratégico y operativo militares. Deberán establecerse las conexiones adecuadas entre el Centro de Coordinación de la Ciberderfensa de la UE y el Centro de Inteligencia y de Situación de la UE (INTCEN), así como con la inteligencia del Estado Mayor de la UE en el marco de la Capacidad Única de Análisis de Inteligencia. Además de las fuentes de información externas, el Centro de Coordinación de la Ciberdefensa de la UE debe establecer e incorporar un sistema activo e independiente de sensores informáticos para reforzar el seguimiento de los centros estratégicos de la UE que apoyan las misiones y operaciones militares de la PCSD. Proporcionará unas mayores capacidades de detección y generará un nuevo estrato de datos que permitirá seguir ampliando la base de información para la evaluación de ciberriesgos y la conciencia situacional.

Su consecución requiere unas capacidades que posibiliten y aseguren el establecimiento y el mantenimiento, 24/7, de una imagen operativa —y, a ser posible, reconocida— del ciberespacio, lo que incluye las ciberoperaciones en curso e inminentes, tanto de adversarios como de fuerzas amigas. Disponer de esa imagen contribuiría a la planificación y la ejecución de las misiones y operaciones militares de la PCSD de la UE. Esa será, por lo tanto, la contribución del sector militar al objetivo de que la UE tenga una consciencia más clara de las acciones maliciosas en el ciberespacio y pueda responder a ellas.

Para mejorar el nivel de confianza e intercambiar información estratégica fiable y oportuna sobre incidentes cibernéticos importantes, se seguirá desarrollando y reforzando la **Conferencia de cibermandos de la UE**[[13]](#footnote-14). Este organismo, de cuya secretaría se encargará la Agencia Europea de Defensa (AED) y en el que participará el Estado Mayor de la UE, se reunirá al menos dos veces al año para debatir cuestiones operativas y otros temas de actualidad.

Con el apoyo de la AED, se creará una red operativa de **equipos militares de respuesta a emergencias informáticas de la UE (MICNET)**. Se insta a todos los Estados a que participen en la red MICNET, cuya entrada en funcionamiento está prevista para enero de 2023.

Al facilitar el intercambio de información entre los citados equipos militares, la red MICNET propiciará una respuesta más sólida y coordinada a las ciberamenazas que afectan a los sistemas de defensa de la UE, como los que sustentan las misiones y operaciones militares de la PCSD. MICNET también permitirá mantener, a lo largo del tiempo, los procesos de formación y la determinación continua de nuevos requisitos para la comunidad de equipos militares de respuesta a emergencias informáticas. Durante los cuatro próximos años, la AED, junto con los Estados miembros, desarrollará una infraestructura —con sus correspondientes herramientas y procedimientos— que facilite el intercambio de información entre estos equipos. MICNET también proporcionará el marco para la realización de un ejercicio anual que permita ensayar, validar e identificar nuevos requisitos y soluciones.

### 1.2. Aumento de la coordinación con las comunidades civiles

MICNET debe servir de marco y de infraestructura para el intercambio de información entre los distintos niveles de la comunidad de ciberdefensa y las partes interesadas externas.

A medida que dicha estructura vaya alcanzando un mayor nivel de madurez, la AED ayudará a los Estados miembros a explorar opciones de colaboración con la red de **equipos de respuesta a incidentes de seguridad informática (CSIRT)**, que reúne a los CSIRT nacionales y al equipo de respuesta a emergencias informáticas de las IOUE (CERT-UE). Esta colaboración podría incluir reuniones y ejercicios conjuntos. Debe también estudiarse la participación del sector privado en las actividades pertinentes de intercambio de información y respuesta a incidentes.

A fin de realizar una gestión más eficiente de las cibercrisis, la Conferencia de cibermandos de la UE debe colaborar con la red de organizaciones de enlace para la gestión de cibercrisis (CyCLONe) de la UE, que reúne a los Estados miembros y a la Comisión en la misión de apoyar la coordinación y la gestión de incidentes de ciberseguridad a gran escala en la UE. Esta colaboración combinará la experiencia militar y la conciencia situacional civil a nivel estratégico y operativo.

Si bien el Centro de Coordinación de la Ciberdefensa de la UE debe servir de eje central para recopilar, analizar, evaluar y, por último, distribuir la información relacionada con la ciberdefensa, en particular la destinada a las misiones y operaciones militares de la PCSD, también podría vincularse con el Grupo Operativo sobre Crisis Cibernéticas[[14]](#footnote-15), de carácter interinstitucional, creado para garantizar una toma de decisiones informada y una respuesta coordinada de las IOUE a las grandes cibercrisis a nivel estratégico y operativo.

El Centro de Coordinación de la Ciberdefensa de la UE también podrá intercambiar la información pertinente con un centro de análisis y situación cibernéticos que se está creando dentro de la Comisión con el apoyo de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el equipo de respuesta a emergencias informáticas de las IOUE para ofrecer análisis y un apoyo más eficaz para la gestión de crisis.

Además, la falta de herramientas y plataformas de comunicación seguras, compartidas e interoperables entre los Estados miembros y las IOUE pertinentes sigue siendo un gran obstáculo. La Comisión y las instituciones pertinentes están llevando a cabo actualmente un inventario de las herramientas existentes para establecer una comunicación segura en el ámbito cibernético. Sobre la base de ese inventario, la Comisión presentará a finales de 2022 sus recomendaciones al Consejo para acordar nuevas medidas.

**Cibersolidaridad de la UE para mejorar los procesos de detección común y la conciencia situacional**

Las acciones de apoyo civil pueden aumentar todavía más la conciencia situacional común. La comunidad de ciberdefensa podrá beneficiarse de las capacidades superiores de detección civil y conciencia situacional desarrolladas para la protección de las infraestructuras críticas de la UE. Con ese objetivo, la Comisión está preparando una iniciativa para promover el despliegue de una infraestructura de centros de operaciones de seguridad (COS) de la UE, cuya primera fase se pondrá en marcha en las próximas semanas y que, posteriormente, se ampliará y se desplegará a mayor escala[[15]](#footnote-16). Finalmente, quedaría compuesta por varias plataformas plurinacionales de COS, cada una de las cuales agruparía a diversos COS nacionales, y contaría con el apoyo del programa Europa Digital (PED)[[16]](#footnote-17) para complementar la financiación nacional. Los cambios legislativos en el PED permitirían ofrecer un apoyo financiero a más largo plazo para la adquisición conjunta de herramientas e infraestructuras ultraseguras de nueva generación. Ello permitiría a la infraestructura de COS de la UE prevista mejorar las capacidades de detección colectiva utilizando la inteligencia artificial (IA) y las técnicas de análisis de datos más recientes, lo que abarcaría las redes de comunicación civil. La posibilidad de generar inteligencia ejecutable sobre ciberamenazas permitiría alertar en tiempo útil a las autoridades y a las entidades pertinentes, las cuales podrían detectar los incidentes graves y responder a ellos con eficacia. La escala y el alcance de la infraestructura dependerán de la financiación global que pueda recabarse a nivel nacional y que pueda aportar la Unión dentro del presupuesto disponible en el marco financiero plurianual.

Estos COS plurinacionales podrían permitir la participación de entidades de defensa merced al establecimiento de un «pilar de defensa» en función de la gobernanza y del tipo de información compartida. Este «pilar de defensa» se desarrollaría junto con el Alto Representante podría incluir un mecanismo específico para el intercambio de información con los responsables militares y con el Centro de Coordinación de la Ciberdefensa de la UE, para el que podrían elaborarse normas de seguridad de defensa.

**Cibersolidaridad de la UE para las actividades de preparación, respuesta y recuperación**

Las perturbaciones provocadas por los incidentes de ciberseguridad importantes a menudo son demasiado graves como para que los Estados miembros afectados puedan gestionarlas por sí solos. En tales casos, los Estados miembros deben poder recurrir a la asistencia mutua y la solidaridad contempladas, por ejemplo, en el artículo 42, apartado 7, del TUE y en el artículo 222 del TFUE. El Alto Representante, en cooperación con la Comisión y los Estados miembros, estudiará las posibilidades de **ampliar el concepto de Equipos de Respuesta Telemática Rápida (CRRT)**, partiendo del proyecto correspondiente de la CEP, con el fin de ofrecer un mejor apoyo a los Estados miembros de la UE y a las misiones y operaciones de la PCSD. El papel de esos equipos consistiría en prestar, a corto plazo, asistencia personalizada y adaptada a las necesidades específicas de quienes la solicitasen. Para garantizar la eficacia de las acciones de respuesta y recuperación, también podría incluir, siempre que proceda, la posibilidad de recibir apoyo de socios privados de confianza.

Como parte de la Iniciativa de Cibersolidaridad de la UE, la Comisión está preparando medidas de refuerzo de las acciones de preparación y respuesta en toda la UE. Entre ellas se incluiría la **de someter a prueba a las entidades esenciales que explotan infraestructuras críticas para detectar posibles vulnerabilidades a partir de las evaluaciones de riesgos de la UE** —tomando como base las acciones ya emprendidas por la Comisión con ENISA—, así como acciones de respuesta para mitigar el impacto de incidentes graves, apoyar una recuperación inmediata o restablecer el funcionamiento de servicios esenciales[[17]](#footnote-18).

La Iniciativa de Cibersolidaridad de la UE podría apoyar el **establecimiento gradual de una ciberreserva a escala de la UE con servicios de proveedores privados de confianza** que estarían preparados para intervenir, a petición de los Estados miembros, en casos de incidentes transfronterizos significativos. Las funciones y responsabilidades deberían delimitarse claramente y estar perfectamente coordinadas con las de los organismos existentes, a fin de garantizar que esa ciberreserva a escala de la UE preste su apoyo allí donde sea necesario y complemente otras posibles formas de asistencia. Aunque el alcance de la acción y la asignación de los costes de las intervenciones específicas dependerían de los fondos de la UE disponibles, la UE añadiría también valor al garantizar la disponibilidad y la preparación de una reserva de esas características a escala de la UE. A fin de asegurar un alto nivel de confianza, la Comisión estudiará también las opciones que faciliten el desarrollo de regímenes de certificación de la ciberseguridad para estas empresas privadas de ciberseguridad.

Los ejercicios son un elemento clave del refuerzo de la preparación. Fomentan el desarrollo de una base de conocimientos y una comprensión comunes de la ciberdefensa, lo que a su vez mejora la preparación operativa. Los ejercicios comunes de ciberdefensa incrementarán también la interoperabilidad y la confianza entre las partes interesadas, en apoyo, entre otras cosas, de las misiones y operaciones militares de la PCSD. Basándose en la serie CYBER PHALANX[[18]](#footnote-19) y en los ejercicios de los equipos militares de respuesta a emergencias informáticas, la **AED creará un nuevo proyecto CyDef-X, que reunirá a todos los Estados miembros y servirá de marco para los ejercicios de ciberdefensa de la UE**. Este proyecto podría utilizarse para prestar la asistencia mutua contemplada en el artículo 42, apartado 7, del TUE. Es preciso explorar también el uso de entornos específicos de ensayo, formación y ejercicios de ciberdefensa (por ejemplo, la Federación de Campos de Maniobras Virtuales), por ejemplo mediante el proyecto de Federaciones de Campos de Maniobras Virtuales de la CEP[[19]](#footnote-20).

Los ejercicios también pueden desempeñar un importante papel para la mejora de la cooperación entre entidades civiles y militares. Al organizar sus ejercicios, ENISA, la AED y otras entidades pertinentes deben, por lo tanto, considerar sistemáticamente la posibilidad de incluir a participantes de otras cibercomunidades.

Como parte del refuerzo de la capacidad de la UE para la prevención, disuasión y respuesta a los ciberataques, y en consonancia con la Estrategia de Ciberseguridad de la UE de 2020 y la «Brújula Estratégica», el Alto Representante propondrá en 2023 diversas opciones para seguir fortaleciendo el conjunto de instrumentos de ciberdiplomacia de la UE[[20]](#footnote-21), tomando como inspiración los distintos elementos de la posición de la UE en materia cibernética y las enseñanzas extraídas de la aplicación de ese conjunto de instrumentos desde su creación.

|  |
| --- |
| ***Acciones de ciberdefensa**** Crear un Centro de Coordinación de la Ciberdefensa de la UE como base para una conciencia situacional militar común, y explorar las modalidades de cooperación con el Centro de Inteligencia y Situación de la Comisión.
* Desarrollar y seguir reforzando la Conferencia de cibermandos de la UE.
* Animar a los Estados miembros a participar activamente en MICNET, que es la red de equipos militares de respuesta a emergencias informáticas, y a trabajar para el establecimiento de una cooperación con la red civil de CSIRT.
* Desarrollar un nuevo proyecto marco CyDef-X en apoyo de los ejercicios de ciberdefensa de la UE.
* Explorar las posibilidades de seguir ampliando el concepto de equipos de respuesta telemática rápida, tomando como base el proyecto de los CRRT de la CEP.
* Estudiar las posibilidades de seguir desarrollando proyectos de Federaciones de Campos de Maniobras Virtuales.

***Acciones de apoyo civil*** * Preparar una Iniciativa de Cibersolidaridad de la UE de la que podría formar parte un acto legislativo que introduzca cambios en el Programa Europa Digital:
	+ para reforzar las capacidades comunes de detección, conciencia situacional y respuesta de la UE;
	+ para crear gradualmente una ciberreserva a escala de la UE de servicios por proveedores privados de confianza;
	+ para propiciar que se someta a prueba a las entidades críticas con el fin de detectar posibles vulnerabilidades a partir de las evaluaciones de riesgos de la UE.
* Explorar el desarrollo de regímenes de certificación de la ciberseguridad a escala de la UE para la industria de la ciberseguridad y las empresas privadas.
* Mejorar la cooperación a nivel estratégico, operativo y técnico entre las comunidades de ciberdefensa y otras cibercomunidades
 |

**2. Afianzamiento del ecosistema de defensa de la UE**

En los últimos años ha aumentado de forma espectacular el número de ciberataques, incluidos los dirigidos contra la cadena de suministro con fines de ciberespionaje, secuestro de archivos (*ransomware*) o perturbación de la actividad. En 2020, el ataque a la cadena de distribución de la empresa SolarWinds[[21]](#footnote-22) afectó a más de 18 000 organizaciones de todo el mundo, como corporaciones públicas, grandes empresas y empresas de defensa. El hecho de que se aprovechara un punto vulnerable del programa informático Log4J de Apache[[22]](#footnote-23) puso de relieve que incluso aquellos componentes del programa informático que no se consideran de alto riesgo ni críticos pueden servir de arma para atacar eficazmente en la UE a grandes empresas o administraciones, incluidas las del ámbito de la defensa. Esta situación pone de manifiesto la clara necesidad de reforzar todavía más la ciberresiliencia de las entidades que operan en el ecosistema de defensa de la UE, incluidas las entidades militares, la industria de la defensa y los operadores privados.

Las fuerzas armadas dependen en gran medida de las infraestructuras críticas civiles, ya sea para la movilidad, las comunicaciones o la energía. El ataque ruso a la red de satélites KA-SAT[[23]](#footnote-24), que interrumpió la comunicación entre varias autoridades públicas, así como en el seno de las fuerzas armadas ucranianas, es un ejemplo de esa interrelación. Esto demuestra la necesidad de afianzar estas infraestructuras críticas.

Para hacer frente a las cuestiones que afectan a la seguridad de sus sistemas de comunicación e información (SIC), los Estados miembros están desarrollando sus propias normas y requisitos de seguridad para los sistemas militares, sin tener siempre en cuenta la necesidad de interoperabilidad ni la existencia de normas civiles para productos de doble uso. Ello repercute negativamente en la capacidad de los Estados miembros para actuar conjuntamente en el ciberespacio, por ejemplo en el contexto de las misiones y operaciones militares de la PCSD, y entorpece la asistencia mutua. Además, es necesario también promover unas sinergias más fuertes entre los procedimientos de normalización militar y civil, ya que la obligación de cumplir normas similares, pero diferentes, por parte de los clientes civiles y militares aumenta los costes de producción para el desarrollo industrial de productos de doble uso.

***2.1. Mejora de la ciberresiliencia del ecosistema de defensa***

La mejora de la ciberresiliencia del ecosistema de defensa requiere acciones e inversiones específicas en una amplia gama de entidades, desde la infraestructura militar de los Estados miembros y las misiones y operaciones de la PCSD hasta las infraestructuras críticas, la industria de la defensa y las entidades de investigación pertinentes.

La protección de la información necesaria para tomar decisiones con conocimiento de causa es un factor necesario para el éxito de las misiones y operaciones de la PCSD. La UE y sus Estados miembros deben seguir reforzando sus estructuras militares de mando y control y desarrollar y proteger sus infraestructuras. También han de consolidarse las consultas político-militares en las fases tempranas de la gestión de crisis para un empleo efectivo del cuartel general de la operación, lo que afecta a la Capacidad Militar de Planificación y Ejecución (MPCC). Este aspecto se abordará, concretamente, mediante el desarrollo de la red de área amplia para operaciones de la UE.

En el contexto de las misiones y operaciones militares, los agentes de ciberdefensa procesan información de diferentes formatos y clasificaciones, procedentes de distintas fuentes. Esto hace que la aplicación de una tecnología segura y de última generación, como la IA, con el apoyo de la industria, sea de suma importancia.

La seguridad de la infraestructura de los SIC debe mejorarse mediante la aplicación de procedimientos de gestión adoptados de mutuo acuerdo, lo cual genera confianza entre las partes interesadas en cuanto a la integridad de la información disponible. Además, el Alto Representante, en su capacidad de director de la AED y con el apoyo de la Comisión, asistirá a los Estados miembros en el desarrollo de **recomendaciones no vinculantes para la comunidad de defensa**, **inspiradas en la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (SRI 2)**[[24]](#footnote-25), de cuyo ámbito de aplicación está precisamente excluida la defensa. Esto contribuirá a aumentar la madurez general de la ciberdefensa.

La propuesta de Ley de Ciberresiliencia[[25]](#footnote-26) presentada por la Comisión, que tiene por objeto establecer requisitos de ciberseguridad para los productos con elementos digitales, también reducirá todavía más la superficie de ataque de los productos de doble uso que utilizan, por ejemplo, la industria de la defensa y los responsables públicos de la defensa en sus SIC. Conforme a esta propuesta, los fabricantes estarán obligados a notificar en un plazo de 24 horas a ENISA —la cual informará a los CSIRT nacionales pertinentes— toda vulnerabilidad que haya sido activamente explotada. A este respecto, también sería importante garantizar que la comunidad de defensa sea rápidamente informada de las vulnerabilidades de los productos con elementos digitales, así como de los parches y las medidas de mitigación disponibles o ya aplicados.

**También es necesario seguir aumentando la protección de las infraestructuras críticas frente a ciberataques a gran escala**, máxime si se tiene en cuenta la dependencia del sector militar respecto de las infraestructuras críticas civiles. A petición del Consejo[[26]](#footnote-27), la Comisión, el Alto Representante y el Grupo de Cooperación SRI[[27]](#footnote-28) están elaborando escenarios de riesgo para la seguridad de las infraestructuras digitales. La atención se centrará, en primer lugar, en la ciberseguridad de los sectores de la energía, las telecomunicaciones y el transporte, y el espacio. Además, se prepararán evaluaciones específicas de los riesgos de ciberseguridad para las infraestructuras y redes de comunicaciones en la UE (incluidas las infraestructuras fijas y móviles, los satélites, los cables submarinos y el encaminamiento por internet)[[28]](#footnote-29). Por lo que respecta a la protección de las infraestructuras críticas frente a las amenazas de origen humano, incluidas las de carácter híbrido, en la propuesta de Recomendación del Consejo sobre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras críticas[[29]](#footnote-30) se insta a los Estados miembros a que aseguren la organización de pruebas de resistencia y una coordinación de crisis adecuada, entre otros aspectos. La protección de la infraestructura marítima crítica, de la que forman parte los cables de datos submarinos, se abordará con más detalle con ocasión de la próxima revisión de la Estrategia de Seguridad Marítima de la UE y su plan de acción. En el plan de acción de la UE para la digitalización del sistema energético se establecen nuevas medidas destinadas a reforzar la ciberseguridad de las infraestructuras críticas de ese sistema[[30]](#footnote-31).

Los servicios espaciales son cada vez más importantes para la defensa, ya sea desde el punto de vista de la vigilancia, de la conciencia situacional, del posicionamiento preciso o de la comunicación ultrasegura. Se trata, por lo tanto, de activos estratégicos clave para la soberanía tecnológica. La perturbación de los servicios espaciales podría tener un gran impacto en los sistemas de defensa, pero también en la sociedad y la economía en general. Dado que pueden ser el objetivo de ataques maliciosos, su resiliencia es fundamental para la resiliencia global de la ciberdefensa. Concretamente, como se ha observado con los ataques a las redes KA-SAT, los sistemas espaciales están cada vez más expuestos a ciberamenazas que pueden afectar a la disponibilidad o a la continuidad de los servicios espaciales. Ello supone un riesgo para los intereses estratégicos y de seguridad de la UE en el ámbito espacial, así como para las capacidades espaciales que posibilitan la ciberdefensa y contribuyen a ella. La estrategia espacial de la UE para la seguridad y la defensa anunciada en la «Brújula Estratégica»[[31]](#footnote-32) perfilará medidas con objeto de aumentar la robustez y la ciberresiliencia de las infraestructuras espaciales y los servicios conexos, así como con fines disuasorios y de respuesta a cualquier amenaza —especialmente las ciberamenazas— a los sistemas y servicios espaciales sensibles de la UE.

La Comisión urge además a los Estados miembros a que den aplicación a las medidas recomendadas en el conjunto de instrumentos de la UE para la ciberseguridad de las redes 5G[[32]](#footnote-33). Los Estados miembros que aún no hayan impuesto restricciones legales a los proveedores de alto riesgo deben hacerlo sin más demora, teniendo en cuenta que cualquier tiempo perdido puede aumentar la vulnerabilidad de las redes en la UE. Esos riesgos pueden afectar a los activos militares y tener un impacto en el entorno general de defensa de los Estados miembros.

Por lo que respecta a la **ciberresiliencia de la industria europea de defensa, así como de las entidades de investigación y desarrollo en materia de defensa**, dichos organismos están incluidos en el ámbito de aplicación de la Directiva SRI 2, salvo que los Estados miembros las hayan excluido explícitamente de él. Por lo tanto, deberían contar con un programa de gestión de riesgos de ciberseguridad que incluya la seguridad de la cadena de suministro y la notificación de incidentes. Habida cuenta de que el sector privado desempeña un papel importante de prestación de servicios de ciberseguridad dentro del ecosistema de defensa, los Estados miembros deben hacer un mayor uso de los regímenes de certificación de la ciberseguridad. Podría explorarse la posibilidad de establecer un **régimen de certificación de la ciberseguridad de la UE para las empresas que presten servicios a la industria de la defensa** como forma de introducir un nivel armonizado de confianza en el mercado, tomando como base de la experiencia de ENISA.

## 2.2. Garantía de interoperabilidad y coherencia de las normas en materia de ciberdefensa en la UE

La interoperabilidad y la homogeneidad son requisitos importantes que deben tenerse en cuenta desde la fase de diseño de las capacidades de ciberdefensa —sin olvidar las enseñanzas extraídas de las misiones y operaciones en curso y resaltadas bajo la dirección del Estado Mayor de la UE—, con el apoyo de la AED. Los principios, procesos y normas acordados en el marco de la Redes de Misiones Federadas (RMF)[[33]](#footnote-34) deberían considerarse los elementos rectores del desarrollo de las capacidades nacionales de ciberdefensa a fin de garantizar la interoperabilidad.

Los esfuerzos de colaboración pueden facilitarse armonizando los requisitos aplicables a las capacidades de ciberdefensa de nueva generación, lo que podría dar lugar a iniciativas conjuntas de desarrollo y contratación pública y a un apoyo integrado del ciclo de vida. Por este motivo, la AED y el Estado Mayor de la UE elaborarán **recomendaciones para un conjunto de requisitos de interoperabilidad de la ciberdefensa de la UE**. Esos requisitos deben tenerse en cuenta en todos los horizontes de planificación para garantizar la totalidad de los aspectos de la normalización como factor clave para la interoperabilidad. Los requisitos de ensayo, evaluación y certificación son otros tantos factores esenciales para facilitar avances en ese sentido.

La propuesta de Ley de Ciberresiliencia[[34]](#footnote-35) contendrá normas armonizadas de ciberseguridad para los productos y componentes de los equipos y programas informáticos que se aplicarán a todos los productos civiles y de doble uso con elementos digitales, que representan una gran proporción de los productos utilizados en el sector de la defensa. Siempre que sea posible, la Comisión fomentará la coherencia con las normas de ciberseguridad relacionadas con la defensa para los productos digitales. Tal como se establece en el Plan de acción sobre las sinergias entre las industrias civil, de la defensa y espacial[[35]](#footnote-36) (el «Plan de acción sobre sinergias»), la Comisión, en estrecha cooperación con las principales partes interesadas, presentará un plan destinado a promover el uso de las normas híbridas aplicables tanto al sector civil como al de defensa y la elaboración de otras nuevas. Debe seguir ampliándose la cooperación entre todas las partes interesadas pertinentes, incluidas las organizaciones europeas de normalización, la Organización del Tratado del Atlántico Norte (OTAN) y otros socios, recurriendo para ello de la manera más provechosa al Comité Europeo de Normalización de la Defensa. En esa misma línea, cuando los organismos de normalización militares desarrollen nuevas normas relacionadas con la ciberseguridad para productos con elementos digitales de uso en defensa, deberán tomar como punto de referencia las normas armonizadas que se elaboren con arreglo a la Ley de ciberresiliencia[[36]](#footnote-37).

***Acciones de ciberdefensa***

* Ayudar a los Estados miembros a elaborar recomendaciones jurídicamente no vinculantes destinadas a la comunidad de defensa, inspiradas en la SRI 2, con el fin de contribuir a aumentar la madurez general de la ciberdefensa a nivel nacional.
* Elaborar recomendaciones sobre los requisitos de interoperabilidad de la ciberdefensa de la UE.
* En el marco del Comité Europeo de Normalización de la Defensa, mejorar la cooperación con todos los agentes pertinentes en lo que respecta a las normas relacionadas con la defensa.

***Acciones de apoyo civil***

* Desarrollar escenarios de riesgo referentes a las infraestructuras críticas de importancia para la comunicación y la movilidad militares, con el fin de orientar las acciones de preparación, por ejemplo mediante pruebas de penetración.
* Fomentar la cooperación entre los organismos de normalización civiles y militares para el desarrollo de normas armonizadas aplicables a los productos de doble uso.

**3. Inversión en capacidades de ciberdefensa**

En los últimos años, las inversiones en ciberdefensa en la UE han aumentado en el contexto de las crecientes actividades informáticas maliciosas por parte de agentes estatales y no estatales. El refuerzo de las capacidades de ciberdefensa de la UE reviste una importancia crítica. La guerra de agresión de Rusia contra Ucrania intensifica más aún la necesidad de aumentar las inversiones con el fin de garantizar que los Estados miembros dispongan de capacidades de ciberdefensa punteras, tanto estacionarias como desplegables.

Las mejoras tecnológicas son esenciales para mantener una ventaja sobre los competidores y los adversarios, que también están haciendo cuantiosas inversiones en nuevas tecnologías. Por lo tanto, también la UE y los Estados miembros deben mejorar su cooperación e interoperabilidad en materia de ciberdefensa mediante el desarrollo conjunto de capacidades y el aumento de las inversiones en investigación y desarrollo.

Además, es preciso hacer frente a las vulnerabilidades derivadas de las dependencias estratégicas y la fragmentación de la base industrial y tecnológica de la defensa europea (BITDE)[[37]](#footnote-38). En particular, las capacidades y las competencias son esenciales para superar las dependencias estratégicas de la ciberseguridad y la ciberdefensa en Europa. La industria europea de la defensa debe conservar capacidades esenciales y adquirir capacidades nuevas para seguir en condiciones de ofrecer soluciones de alta tecnología en un entorno mundial.[[38]](#footnote-39). La falta de habilidades repercute de forma negativa en el sector de la defensa, ya que dificulta el desarrollo de capacidad en todos los ámbitos. Todas las acciones se ajustarán plenamente a los enfoques anunciados en el Plan de Acción sobre Sinergias, la Hoja de ruta sobre tecnologías críticas para la seguridad y la defensa («la hoja de ruta»)[[39]](#footnote-40) y el análisis de los déficits de inversión[[40]](#footnote-41)

## 3.1. Desarrollo de capacidades de ciberdefensa de vanguardia de amplio espectro

Los Estados miembros tienen la responsabilidad y la competencia de utilizar las capacidades de ciberdefensa, mientras que la UE desempeña un importante papel a la hora de apoyar el mayor desarrollo de capacidades militares específicas dentro del espectro «Doctrina, Organización, Formación, Material, Personal, Liderazgo, Instalaciones e Interoperabilidad (DOTMLPF-I)» para generar libertad de acción en el ciberespacio. Es necesario seguir unificando el enfoque aplicado a la ciberdefensa en todos los ámbitos de capacidades y adaptarlo al cambiante entorno geopolítico. Ello requiere identificar los elementos que faltan en las capacidades existentes y apoyar el desarrollo de nuevas capacidades de manera coordinada y mensurable.

Sin embargo, el nivel de implicación de los Estados miembros en los proyectos colaborativos de desarrollo de la ciberdefensa sigue siendo insuficiente, y debe aumentarse para maximizar su repercusión a escala de la UE. Todos los Estados miembros deben aumentar sus inversiones en el desarrollo de capacidades de ciberdefensa de amplio espectro y desarrollarlas de manera colaborativa. Los Estados miembros deben estudiar la posibilidad de **elaborar un conjunto de compromisos voluntarios para el desarrollo de capacidades nacionales de ciberdefensa**, incluidas capacidades multinacionales que vayan más allá de los proyectos de ciberdefensa de la CEP existentes[[41]](#footnote-42). El proceso de revisión anual coordinada de la defensa podría utilizarse para iniciar un diálogo con los Estados miembros acerca de los requisitos de ciberdefensa y los objetivos nacionales de desarrollo de capacidades de ciberdefensa, y evaluar el cumplimiento de los compromisos. La Comisión apoya y cofinancia actividades de investigación y desarrollo de capacidades de ciberdefensa de amplio espectro, incluidas las capacidades de defensa activa, a través del Fondo Europeo de Defensa (FED). Además, ya ha incrementado las inversiones en ciberdefensa a través del FED, lo que debería desembocar en el desarrollo de herramientas europeas comunes y/o interoperables para las operaciones y la gestión de incidentes en el ciberespacio, de operaciones defensivas en la guerra informativa y de medidas preventivas, así como de una mayor resiliencia de los sistemas de SIC. Estas inversiones se concentran en ámbitos como la conciencia cibersituacional, la «caza» de amenazas en tiempo real y las capacidades para operaciones de respuesta, las capacidades ciberoperativas y la formación y los ejercicios cibernéticos[[42]](#footnote-43). Para garantizar que los Estados miembros sean capaces de llevar a cabo ciberoperaciones conjuntas, en los próximos años se financiarán con cargo al FED operaciones de respuesta y capacidades ciberoperativas. Por último, se anima a los Estados miembros a que participen activamente en los diferentes marcos de cooperación y a que utilicen todos los instrumentos establecidos a escala de la UE, incluidos los de ciberdefensa del equipo del proyecto de la AED[[43]](#footnote-44).

La revisión en curso de las prioridades de desarrollo de capacidades de la UE emprendida en 2018[[44]](#footnote-45) constituye una oportunidad idónea para definir las prioridades actualizadas de desarrollo cooperativo y colaborativo, ejercicio que, a su vez, facilita el aumento del desarrollo cooperativo de capacidades. La revisión de la prioridad específica de ciberdefensa debe tener en cuenta los resultados de la revisión anual coordinada de la defensa de 2022, así como las conclusiones del análisis de déficits de inversión presentado a los Estados miembros en mayo de 2022. Posteriormente, la revisión anual coordinada de la defensa ofrecerá un marco periódico para examinar los avances en la aplicación de esta prioridad actualizada a nivel nacional y explorar las nuevas opciones que surjan para el desarrollo colaborativo de las capacidades de ciberdefensa con los Estados miembros. Las prioridades actualizadas de desarrollo de capacidades de la UE servirán de referencia básica para los proyectos de la CEP en materia de ciberdefensa.

A este respecto, sobre la base de las instrucciones del Comité Militar de la UE, el Estado Mayor de la UE elaborará el plan de ejecución de operaciones en el ámbito cibernético, en estrecha coordinación con los Estados miembros, con el fin de presentar el panorama general del estado de aplicación de las capacidades de ciberdefensa, así como de prestar a los Estados miembros un apoyo que les permita armonizar mejor sus esfuerzos y actividades. Estos esfuerzos se basan en el concepto de ciberdefensa de la UE para las operaciones y misiones militares dirigidas por la UE, que retoma los parámetros prioritarios del Plan de Desarrollo de Capacidades (PDC).

**Refuerzo de la actividad de investigación sobre tecnologías clave para la ciberdefensa**

Para sustentar unas capacidades de ciberdefensa de vanguardia, es preciso mantenerse totalmente al día en cuanto a los avances tecnológicos y sus aplicaciones en los sistemas de defensa, en particular las tecnologías emergentes y disruptivas (o EDT, por sus siglas en inglés: por ejemplo, la IA, el cifrado y la computación cuántica)[[45]](#footnote-46). En particular, la UE debe invertir en criptografía postcuántica para garantizar que sus sistemas de defensa sigan siendo seguros. Ante la rapidez del ritmo al que evoluciona la tecnología, los esfuerzos colaborativos de investigación y desarrollo tecnológico deben adaptarse con el fin de alcanzar un nivel de preparación tecnológica lo suficientemente avanzado como para que sus resultados puedan incorporarse con mayor rapidez a las capacidades existentes y futuras.

La Comisión está financiando con cargo al FED la innovación tecnológica para la defensa y apoyando el desarrollo de tecnologías emergentes y disruptivas, así como de tecnologías de vanguardia, en particular para la ciberdefensa. Hasta el 8 % del presupuesto de dicho Fondo se asigna a aspectos relacionados con las tecnologías disruptivas de defensa, algunos de ellos pertinentes para la ciberdefensa. En los próximos años se prestará una especial atención, en el marco del FED, a las acciones y proyectos de investigación dedicados a las nuevas tecnologías desarrolladas frente a las amenazas emergentes y cambiantes, así como al aumento de la resiliencia y la ciberseguridad y la integración de estas características en las capacidades de defensa.

En consonancia con el Plan de acción sobre tecnologías emergentes y disruptivas[[46]](#footnote-47), la AED presentará anualmente a los Estados miembros una visión panorámica de las tecnologías emergentes, incluidas las aplicables a la ciberdefensa. Además, ampliará la evaluación estratégica de las tecnologías emergentes y disruptivas europeas para ayudar a los Estados miembros a adoptar orientaciones estratégicas a largo plazo, identificando las sinergias y las oportunidades de colaboración. El Centro Europeo de Competencia en Ciberseguridad (CECC) adoptará una agenda estratégica para la inversión en ámbitos clave de la ciberseguridad que, a su vez, guiará la preparación de los futuros programas de trabajo de Europa Digital y Horizonte Europa en lo que respecta a la ciberseguridad, en apoyo, respectivamente, de la investigación, la innovación y la penetración en el mercado. Con el propósito de fomentar las sinergias, el CECC y la AED también elaborarán un acuerdo de trabajo para facilitar el intercambio de información entre el personal de ambas entidades acerca de las prioridades de la tecnología civil, de doble uso y de defensa.

**Medidas para satisfacer las necesidades tecnológicas de ciberdefensa**

Es preciso adoptar nuevas medidas y aumentar la coordinación para asegurar que el sector de la defensa se ajuste rápidamente a la rápida evolución tecnológica en el ámbito cibernético. Para ello, es preciso redoblar los esfuerzos que permiten localizar tecnologías críticas para la ciberdefensa y la ciberseguridad y a las que debe otorgarse prioridad para reducir las dependencias tecnológicas de la UE y determinar si el orden de prioridades y los instrumentos de financiación actuales son suficientes para ello.

Con tal fin, la Comisión, junto con la AED y los Estados miembros, propondrá en 2023 una **hoja de ruta tecnológica para las cibertecnologías críticas** basada en las consultas pertinentes, en las que participará la industria cuando proceda. La hoja de ruta tecnológica determinará cuáles son las cibertecnologías importantes para la soberanía tecnológica de la UE, abarcará tanto la ciberdefensa como la ciberseguridad, repertoriará los avances tecnológicos y las dependencias estratégicas y propondrá acciones para reducirlas. La hoja de ruta para las cibertecnologías fundamentará las prioridades estratégicas de los instrumentos de financiación de la UE y propondrá que se haga un uso exhaustivo de los programas de investigación y desarrollo y ampliación de capacidades y de los instrumentos de financiación, tanto en materia civil como de defensa, en consonancia con sus respectivas normas de gobernanza. También propondrá nuevas formas de fomentar el desarrollo de la investigación de doble uso, el desarrollo tecnológico y la innovación en materia de ciberseguridad y ciberdefensa a escala de la UE y de los Estados miembros.

En ese contexto, la Comisión[[47]](#footnote-48), en cooperación con el CECC y la AED, evaluará en 2023 las tecnologías que ya han sido identificadas como críticas para la ciberdefensa y, posiblemente con el apoyo del Observatorio de Tecnologías Críticas, localizará y definirá con mayor precisión las dependencias existentes[[48]](#footnote-49). Para ello, se tendrá en cuenta el trabajo realizado en el contexto del documento de seguimiento anual de la AED[[49]](#footnote-50) y de la evaluación estratégica europea de las tecnologías emergentes y disruptivas[[50]](#footnote-51). Además, el CECC podría poner en marcha un proyecto de apoyo específico para esta política capaz de contribuir al proceso de inventariado de la tecnología y de reunir a las partes interesadas de los ámbitos civil y militar, entablando un diálogo entre ellas.

Como parte de las medidas perfiladas en el Plan de acción sobre las sinergias, la hoja de ruta y el análisis de déficits de inversión, se están llevando a cabo ya varias acciones para reforzar las sinergias y aprovechar mejor todo el potencial de las tecnologías de doble uso, incluidas las aplicables en el ámbito cibernético.

Además, se anima a los Estados miembros a que hagan un pleno uso de las iniciativas existentes de apoyo a la investigación y el desarrollo tecnológicos, a saber, en el caso de la defensa, los grupos tecnológicos de capacidades de defensa de la AED[[51]](#footnote-52) y los correspondientes bloques tecnológicos del OSRA[[52]](#footnote-53), el marco ad hoc de la AED[[53]](#footnote-54), el FED y la CEP. En el caso de las tecnologías civiles y de doble uso, el CECC y la Red pueden gestionar proyectos con una dimensión tanto de defensa como civil, tal como se establece en su base jurídica[[54]](#footnote-55). Conforme a lo anunciado en el Plan de acción sobre las sinergias y en la hoja de ruta, la Comisión también intentará reforzar las sinergias entre las actividades del CECC y del FED en materia de ciberseguridad y ciberdefensa, en consonancia con las normas de gobernanza del FED.

## 3.2. Una industria europea de la defensa ágil, competitiva e innovadora

La UE necesita una industria europea de la defensa fuerte, ágil, competitiva e innovadora, capaz de ofrecer un espectro completo de capacidades de defensa de vanguardia (incluidas las de ciberdefensa). Sin embargo, en el ámbito de la ciberdefensa, la industria de la defensa de la UE depende actualmente en gran medida de soluciones civiles y de los mercados exteriores para ofrecer resultados punteros. Si bien los avances tecnológicos en el ámbito civil son veloces y el mercado de la información civil y los productos de ciberseguridad se está expandiendo con rapidez, existen necesidades militares específicas que no satisfacen los productos civiles disponibles en el mercado. Partes importantes de los equipos y programas informáticos que se utilizan actualmente para la ciberdefensa no se fabrican en la UE, lo que puede crear dependencias industriales y tecnológicas. Además, la UE tampoco tiene una fuerte presencia en la industria mundial de la ciberseguridad y la ciberdefensa. Su **BITDE**, muy fragmentada, reduce en gran medida su capacidad de mejorar su competitividad[[55]](#footnote-56); además, la mayoría de las empresas de ciberseguridad de la UE son pequeñas y medianas empresas (pymes)[[56]](#footnote-57). La existencia de una capacidad industrial tecnológicamente soberana es una piedra angular de la capacidad de actuación de la UE.

La UE apoya el desarrollo de una BITDE sólida a través de una serie de programas e iniciativas. Así como el FED financia la innovación tecnológica para la defensa y apoya el desarrollo de tecnologías que, posteriormente, conducen al desarrollo de capacidades militares de vanguardia, el cual contribuye a su vez a la competitividad de la industria de la defensa de la UE, los programas Horizonte Europa y Europa Digital apoyan la investigación en materia de ciberseguridad y el desarrollo de tecnologías de doble uso, como la cuántica, el cifrado, la nube segura y la inteligencia artificial[[57]](#footnote-58).

Deben emprenderse nuevas acciones relacionadas con las tecnologías críticas para la ciberdefensa y las necesidades industriales según destaca la **hoja de ruta tecnológica para las cibertecnologías críticas**. Es necesario determinar unos flujos de ayuda apropiados que permitan, por ejemplo, estimular los esfuerzos comunes de contratación pública, en particular a través del futuro Programa Europeo de Inversiones en Defensa, o facilitar el acceso a capital y préstamos a través del Fondo Europeo de Inversiones y el Banco Europeo de Inversiones.

Para lograr una BITDE fuerte, es necesario explotar y aprovechar las sinergias entre las empresas civiles y las de defensa. Las acciones de innovación propuestas en el Plan de Innovación de la UE en materia de Defensa (EUDIS), como la colaboración con las pymes y la prospección tecnológica, podrían tener repercusiones positivas para la industria de la defensa de la UE y la BITDE.

Además, la Comisión iniciará un diálogo sectorial con el propósito de desarrollar la industria de ciberdefensa de la UE, con la participación de la AED cuando proceda.

La Comisión y el Alto Representante proponen poner implantar varias medidas para garantizar que la industria esté equipada para cumplir sus objetivos a corto y largo plazo. Esto implica, de forma inmediata, la realización de un inventario exhaustivo de las capacidades de fabricación de la industria de defensa de la UE que permita identificar con precisión las lagunas y los ámbitos en los que es necesario intensificar la actividad.

La reducción de las dependencias críticas en el ámbito cibernético, como las determinadas en la hoja de ruta tecnológica, también podría emprenderse mediante el nuevo Fondo para la Soberanía Europea anunciado por la presidenta Von der Leyen en su discurso sobre el estado de la Unión de septiembre de 2022.

El marco de control de las inversiones extranjeras directas de la UE seguirá utilizándose para mitigar los riesgos de adquisición de tecnologías o soluciones europeas que presenten riesgos para la defensa y la seguridad. Los Estados miembros que aún no hayan establecido los mecanismos nacionales de control deben hacerlo sin más tardanza.

## 3.3. Mano de obra en ciberdefensa de la UE

Europa se enfrenta a un déficit real y alarmante de cibercapacidades: la Organización Europea de Ciberseguridad (ECSO) estima que en 2022 se necesita ya un total de 500 000 profesionales. Este déficit de capacidades merma la capacidad de la UE para desarrollar nuevas tecnologías y defender nuestras infraestructuras críticas. En el caso de los organismos públicos, como los ministerios de defensa y el ejército, la feroz competencia por conseguir personal cualificado y los atractivos salarios ofrecidos por el sector privado agravan aún más las dificultades para atraer y retener personal con talento en este campo.

En el contexto del Año Europeo de las Competencias 2023, **la Comisión pondrá en marcha una iniciativa para la creación de una Academia de cibercapacidades**. Se tratará de una iniciativa de alcance general con el objetivo de aumentar el número de profesionales formados en ciberseguridad. Englobará las numerosas iniciativas diferentes que existen sobre cibercapacidades y garantizará la coordinación, la integración y una comunicación común en torno a ellas. Organizada sobre varios pilares de acción, como la financiación, el apoyo de las comunidades, la formación y la certificación, la participación de las partes interesadas y la generación de conocimientos, la Academia de cibercapacidades también podrá aportar ventajas a la mano de obra que trabaja en ciberdefensa. La Escuela Europea de Seguridad y Defensa (EESD) estudiará la manera de facilitar el intercambio de las mejores prácticas y de crear nuevas sinergias entre los ámbitos militar y civil en lo que respecta a la formación y al desarrollo de capacidades militares específicas para el ciberespacio.

A partir de un análisis de los requisitos de formación de la UE y de las necesidades de formación, la EESD, la AED y los Estados miembros seguirán preparando y organizando actividades y ejercicios de formación en ciberdefensa para las instituciones de la UE, las operaciones y misiones de la PCSD y los funcionarios de los Estados miembros. Se explorará también la **ampliación de la Plataforma de la EESD sobre educación, formación, ejercicios y evaluación en materia cibernética (ETEE)** para generar nuevas capacidades de formación. Esa ampliación debería incluir asimismo cursos de formación para ámbitos operativos específicos y operaciones en dominios múltiples. En particular, deben buscarse sinergias con el proyecto de Centro de la Unión Europea para el Mundo Académico y la Innovación en el Ámbito del Ciberespacio (CAIH UE) de la CEP [[58]](#footnote-59).

Se anima a los Estados miembros a que creen programas educativos específicos en el ámbito de la ciberdefensa, involucrando a las instituciones académicas y de enseñanza superior (civiles y militares) en el desarrollo y la elaboración de planes de estudios comunes en materia de ciberdefensa, compartiendo las mejores prácticas, creando asociaciones y proyectos comunes y facilitando los intercambios de formadores y personal en prácticas. Para garantizar la interoperabilidad y una cultura común en toda la UE, la EESD fomentará un intercambio entre Estados miembros a través de la ETEE.

Los Estados miembros deben impulsar una cooperación más amplia entre los responsables de la formación y la educación, combinando los aspectos civiles y militares en los ámbitos técnico, operativo, estratégico y jurídico, sentando las bases para la creación de programas de formación comunes y homologados a distintos niveles para las comunidades civil, policial y judicial, diplomática y de ciberdefensa. Además, los Estados miembros deben colaborar con los proveedores de formación del sector privado europeo, así como con las correspondientes instituciones académicas, con el fin de aumentar los niveles de competencias y de capacidades del personal de las misiones y operaciones militares de la PCSD.

Por otra parte, debe promoverse la cooperación con respecto a las normas de formación y certificación en materia de ciberdefensa entre los Estados miembros, las IOUE, los socios internacionales y otros actores, con la participación del sector privado y el mundo académico. A partir de iniciativas civiles ya existentes, como el Marco Europeo de Capacidades en Ciberseguridad (ECSF) desarrollado por ENISA, la EESD creará un marco de certificación de las capacidades de ciberdefensa. La Comisión también podría estudiar los diversos enfoques para la certificación de cibercapacidades existentes en el mercado y en el ámbito académico, tratando de fomentar al mismo tiempo las sinergias entre estos enfoques a través de la Academia de cibercapacidades y de colmar lagunas, en particular con financiación específica de la UE.

***Acciones de ciberdefensa***

* Desarrollar una evaluación estratégica de las tecnologías emergentes y disruptivas en apoyo de las decisiones de inversión estratégica a largo plazo.
* Desarrollar una hoja de ruta tecnológica correspondiente a las cibertecnologías críticas para la UE que abarque las tecnologías críticas para la ciberdefensa y la ciberseguridad, a fin de evaluar el nivel de las dependencias.
* Proponer soluciones para reducir las dependencias utilizando todos los instrumentos de la UE, incluidos los programas Europa Digital y Horizonte Europa y el FED, y anticipar el desarrollo tecnológico con el fin de aumentar la soberanía tecnológica y garantizar la capacidad de actuación.
* Apoyar el desarrollo del marco de certificación de las capacidades de ciberdefensa.
* Crear ejercicios de ciberdefensa de la UE y estudiar la manera de seguir desarrollando la ciberplataforma ETEE de la EESD para generar nuevas capacidades de formación.

***Acciones de apoyo civil***

* Crear una Academia de cibercapacidades de la UE, teniendo en cuenta las necesidades de competencias específicas para los diferentes perfiles profesionales y sectores de actividad, sin olvidar al personal del sector de la defensa.
* Analizar los distintos enfoques de certificación de cibercapacidades, tratando al mismo tiempo de propiciar sinergias y de colmar lagunas, a través, entre otros medios, de la financiación de la UE.

**4. La asociación como forma de afrontar los retos comunes**

Los miembros de una posible asociación saldrán beneficiados de una UE más capaz y resiliente en el ciberespacio, así como de la asistencia y el desarrollo de capacidades en materia de ciberdefensa de la UE que se ofrezcan a través de los instrumentos pertinentes de la UE. La UE tratará de establecer asociaciones adaptadas a la situación en el ámbito de la ciberdefensa cuando sean mutuamente beneficiosas. La cuestión de las asociaciones de ciberdefensa también se abordará en el contexto de la participación de los países socios en las misiones y operaciones militares de la PCSD.

Cuando proceda, esta actividad se basará en los diálogos sobre ciberseguridad ya abiertos, así como en los diálogos sobre seguridad y defensa. El Alto Representante explorará también las sinergias entre la **red informal de ciberdiplomacia de la UE y la red de agregados militares en las delegaciones de la UE**.

***4.1. Cooperación con la OTAN***

La asociación estratégica de la UE con la OTAN sigue siendo un factor esencial para la seguridad euroatlántica, tal y como se subraya en la «Brújula Estratégica» y en el Concepto Estratégico de la OTAN de 2022[[59]](#footnote-60). La UE sigue plenamente comprometida con el refuerzo de esta asociación crucial, particularmente en el ámbito de la ciberdefensa. Es preciso adoptar nuevas medidas para desarrollar soluciones comunes a las amenazas y los desafíos comunes. De conformidad con las Declaraciones conjuntas de Varsovia y Bruselas sobre la cooperación UE-OTAN[[60]](#footnote-61) y con arreglo a los principios de transparencia, reciprocidad e inclusividad y apertura, y a la autonomía decisoria de ambas organizaciones, la ciberseguridad y la ciberdefensa constituyen uno de los ámbitos prioritarios esenciales para la cooperación de la UE.

En aplicación de la reciprocidad, la UE seguirá intercambiando información con la OTAN acerca del marco conceptual militar relativo a la integración de los aspectos de ciberdefensa en la planificación y ejecución de las misiones y operaciones militares de la PCSD. La UE se esforzará por garantizar la compatibilidad con los conceptos y la doctrina de la OTAN en materia de ciberdefensa.

Por lo que se refiere a la elevada demanda de capacidades de ciberdefensa, la UE promoverá las sinergias y la complementariedad con la OTAN a través de las fronteras organizativas y nacionales. La UE se asociará con la OTAN a fin de reforzar la interoperabilidad técnica y procedimental de las capacidades de ciberdefensa, lo que también requerirá el desarrollo de las capacidades en consonancia con la iniciativa de las RMF. Ello allanará el camino para el desarrollo y la utilización de las capacidades de ciberdefensa en el marco de un apoyo mutuo potencial. Debe otorgarse una especial consideración a la interoperabilidad de las normas, aspecto que contribuye a la ciberresiliencia y la interoperabilidad de los sistemas militares de comunicación e información, para lo que se recabará la participación de la industria del sector siempre que proceda.

Para que la formación impartida al personal de ciberdefensa de las distintas organizaciones sea coherente, la UE reforzará también según corresponda la cooperación con la OTAN para la armonización de las necesidades de formación y el análisis de los requisitos, elaborando planes de estudios, cursos y ejercicios conjuntos. Conforme a los principios de reciprocidad y no discriminación, la EESD abrirá sus cursos de formación en ciberdefensa al personal de la OTAN y creará una plataforma para anunciar los cursos comunes. La UE también promoverá la participación del personal de la OTAN en ciberejercicios y ejercicios de gestión de crisis con elementos cibernéticos.

La UE y la OTAN se ocuparán también de seguir mejorando la conciencia situacional mutua y de explorar nuevas vías de coordinación, como el refuerzo de la cooperación entre el Equipo de capacidad de respuesta ante incidentes informáticos de la OTAN (NCIRC) y CERT-UE. Para fomentar la cooperación en relación con las implicaciones y los aspectos cibernéticos de la gestión y la respuesta a las crisis, la UE contribuirá al intercambio de personal asignado a iniciativas militares, civiles y comunes y, cuando proceda, a la creación de posibles sinergias entre los respectivos marcos e iniciativas de gestión de crisis, en el caso también de incidentes a gran escala. Con el fin de garantizar la complementariedad mutua y de evitar la duplicación innecesaria de esfuerzos, la UE tratará de estrechar la cooperación y el intercambio de información con la OTAN sobre las medidas de desarrollo de capacidades en materia de ciberdefensa en los países socios.

***4.2. Cooperación con socios afines***

El Alto Representante incluirá de manera más sistemática las cuestiones relativas a la ciberdefensa en los diálogos actuales y futuros con sus socios en materia cibernética, de seguridad y de defensa. A medida que las cuestiones de ciberdefensa se vayan integrando en los diálogos bilaterales, aumentarán las posibilidades de introducir estos aspectos en otros formatos de cooperación con los socios de la UE.

La asociación estratégica de la UE con los **Estados Unidos** seguirá intensificando la cooperación en materia de seguridad y defensa en beneficio mutuo, en particular mediante un intercambio estructurado de información sobre conciencia situacional. Los diálogos periódicos UE-EE. UU. en materia cibernética y en materia de seguridad y defensa confirman la existencia de una sólida asociación transatlántica. Cuando así proceda, el Alto Representante introducirá en estos diálogos los aspectos pertinentes de la ciberdefensa.

Junto con sus socios internacionales, la UE seguirá apoyando a **Ucrania**, en particular a través de un diálogo en materia cibernética. Vista la experiencia de Ucrania en el desarrollo de capacidades de ciberresiliencia y ciberdefensa, proseguirá y se ampliará el intercambio de las mejores prácticas en materia de ciberdefensa, así como de la información sobre la perspectiva de amenazas y la conciencia situacional y sobre la evolución de las correspondientes políticas de interés común.

Una asociación basada en la afinidad es muy importante para mantener un ciberespacio mundial, abierto, estable y seguro y puede complementar la capacidad de la UE para la prevención, disuasión y respuesta a los comportamientos malintencionados en el ciberespacio. La UE sigue abierta a un compromiso amplio, ambicioso y mutuamente beneficioso en materia de seguridad y ciberdefensa con todos los socios que le son afines.

***4.3. Apoyo al desarrollo de capacidades de ciberdefensa en los países socios***

Los retos mundiales y regionales han aumentado la interdependencia entre la UE y sus socios y puesto de relieve la necesidad de establecer asociaciones más estrechas en materia de seguridad y defensa. Esta afirmación es especialmente cierta en el caso de los países candidatos a la adhesión a la UE. Los recientes ciberataques a gran escala muestran cuán necesario es reforzar la implicación y la asociación de la UE en materia de ciberseguridad y ciberdefensa a partir de los programas vigentes. Debido al carácter transnacional de las ciberamenazas, la mejora de la ciberresiliencia de los países socios, especialmente aquellos con un menor nivel de madurez cibernética, contribuirá a un ciberespacio más seguro y protegido. Por lo tanto, la UE estaría en mejores condiciones para prevenir, detectar y repeler los ciberataques, y para defenderse de ellos.La UE intensificará la cooperación en materia de seguridad y defensa con los países socios para reforzar la ciberresiliencia de estos, a través, entre otros medios, de los diálogos ya abiertos. Siempre que sea viable y redunde en beneficio mutuo, la UE colaborará con sus socios —en particular aquellos que se hayan alineado con la política exterior y de seguridad común de la UE y la política común de seguridad y defensa— en sus esfuerzos por impulsar el desarrollo de capacidades de ciberdefensa. Esa colaboración podría incluir el apoyo a la creación de marcos estratégicos y legislativos y actividades de formación, asesoramiento, tutoría y equipamiento de las fuerzas armadas y las fuerzas de seguridad de los socios. Los Estados miembros podrían, si así lo decidiesen, prestar asistencia operativa en materia de ciberdefensa a los socios. Además, la UE ayudará a sus socios a reforzar su capacidad para contribuir a las misiones y operaciones militares de la PCSD como una valiosa contribución a los esfuerzos mutuos por promover la paz y la seguridad.

El Fondo Europeo de Apoyo a la Paz (FEAP) seguirá sustentando los esfuerzos de la UE por ayudar a desarrollar las capacidades de defensa —incluida la ciberdefensa— en los países socios, especialmente los de la vecindad de la UE, complementando con ello las medidas de gestión de crisis de la PCSD. A este respecto, cuando sea necesario, la UE establecerá también unos vínculos más sólidos entre la asistencia para ciberdefensa y el desarrollo de capacidades civiles de ciberseguridad, en particular a través del Consejo para el desarrollo de la capacidad cibernética de la UE. El éxito de las acciones de ciberdefensa y desarrollo de capacidades en materia de ciberseguridad de la UE requerirá una coordinación eficiente entre los programas e instrumentos pertinentes de la UE, incluido el FEAP, y los Estados miembros.

Además de prestar apoyo a los países socios en sus esfuerzos de desarrollo de capacidades de ciberdefensa, la UE colaborará estrechamente con otros donantes para desarrollar la conciencia situacional y crear plataformas de coordinación con el fin de proporcionar el mejor apoyo individualizado posible, garantizar la coherencia y evitar la duplicación de esfuerzos.

***Acciones de ciberdefensa***

* Reforzar la cooperación UE-OTAN en el ámbito de la formación, la educación, la conciencia situacional y los ejercicios sobre ciberdefensa.
* Incluir los temas de ciberdefensa en los diálogos con los países socios sobre ciberseguridad y sobre seguridad y defensa dirigidos por la UE.
* Cooperar con países afines, en particular en el contexto del desarrollo de capacidades de ciberdefensa y ciberresiliencia.
* Ampliar la asistencia a los socios para el desarrollo de capacidades de ciberdefensa, en particular a través del Fondo Europeo de Apoyo a la Paz (FEAP), en particular en los países vecinos de la UE y en apoyo de los países candidatos a la adhesión a la UE.

***Acciones de apoyo civil***

* Reforzar la cooperación UE-OTAN en el ámbito de la ciberseguridad en lo que respecta a la conciencia situacional, la respuesta a las crisis, la protección de las infraestructuras críticas y la normalización y certificación.

# III. CONCLUSIÓN

El Alto Representante, en su capacidad de director de la AED, y la Comisión piden a los Estados miembros que desarrollen los aspectos pertinentes de esta política de ciberdefensa. Se pondrán en contacto con ellos a fin de determinar las medidas prácticas para su aplicación. Podría establecerse un plan de aplicación en cooperación con los Estados miembros. Los resultados de la aplicación de la política de ciberdefensa de la UE contribuirán a los objetivos generales tanto de la Estrategia de Ciberseguridad de la UE como de la «Brújula Estratégica».

Se presentará un informe anual al Consejo que permitirá supervisar y evaluar los avances en la aplicación de la política de ciberdefensa. Se anima a los Estados miembros a que contribuyan con sus aportaciones sobre los avances de las medidas de aplicación que se inscriban tanto en formatos nacionales como en formatos de cooperación.

1. Marco político de ciberdefensa de la UE (actualización de 2018), 19 de noviembre de 2018, http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/es/pdf [↑](#footnote-ref-2)
2. [Una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales](https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf) [↑](#footnote-ref-3)
3. «La Estrategia de Ciberseguridad de la UE para la Década Digital», [JOIN/2020/18 final](https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=JOIN:2020:18:FIN). [↑](#footnote-ref-4)
4. https://ec.europa.eu/commission/presscorner/detail/es/SPEECH\_21\_4701 [↑](#footnote-ref-5)
5. [9364/22](https://www.consilium.europa.eu/media/56358/st09364-es22.pdf) [↑](#footnote-ref-6)
6. [JOIN(2022) 24 final](https://ec.europa.eu/info/sites/default/files/join_2022_24_2_en_act_part1_v3_1.pdf) [↑](#footnote-ref-7)
7. EEAS(2021) 706 REV4 [↑](#footnote-ref-8)
8. Cibercomunidades civil, diplomática y policial [↑](#footnote-ref-9)
9. Equipos de Respuesta Telemática Rápida y de Asistencia Mutua en el ámbito de la Ciberseguridad [↑](#footnote-ref-10)
10. Tratado de la Unión Europea, versión consolidada: Diario Oficial C 326 de 26.10.2012, p. 1. [↑](#footnote-ref-11)
11. Tratado de Funcionamiento de la Unión Europea, versión consolidada: Diario Oficial C 326 de 26.10.2012 p. 1. [↑](#footnote-ref-12)
12. El objetivo del proyecto es desarrollar, establecer y gestionar un Centro de Coordinación del Ámbito del Ciberespacio y de la Información (CIDCC) multinacional, como elemento militar multinacional permanente. [↑](#footnote-ref-13)
13. Tras las conclusiones de las dos primeras reuniones de las conferencias estratégicas de cibermandos europeos (CyberCo) celebradas en enero y junio de 2022, los cibermandos de la UE han decidido crear un foro más permanente a su nivel. [↑](#footnote-ref-14)
14. Grupo informal compuesto por los servicios pertinentes de la Comisión, el SEAE, la Agencia de la Unión Europea para la Ciberseguridad (ENISA), el equipo de respuesta a emergencias informáticas de las IOUE y Europol, y copresidido por la Comisión y el Alto Representante. [↑](#footnote-ref-15)
15. Estrategia de Ciberseguridad de la UE para la Década Digital (JOIN/2020/18 final) y Estrategia de la UE para una Unión de la Seguridad [COM(2020) 605]. [↑](#footnote-ref-16)
16. De conformidad con el 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, DO L 166 de 11.5.2021, p. 1 (sujeto a una posible modificación). [↑](#footnote-ref-17)
17. [Llamamiento de Nevers para reforzar las capacidades de ciberseguridad de la UE](https://presse.economie.gouv.fr/08-03-2022-rmi-telecom-les-etats-membres-appellent-les-entreprises-du-secteur-numerique-a-renforcer-la-lutte-contre-la-desinformation-en-ligne/) [↑](#footnote-ref-18)
18. https://eda.europa.eu/publications-and-data/factsheets/factsheet-cyber-phalanx [↑](#footnote-ref-19)
19. https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/ [↑](#footnote-ref-20)
20. Conclusiones del Consejo sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia») [↑](#footnote-ref-21)
21. https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/ [↑](#footnote-ref-22)
22. https://english.ncsc.nl/topics/log4j-vulnerability [↑](#footnote-ref-23)
23. Declaración del Alto Representante, en nombre de la Unión Europea, sobre las actividades informáticas malintencionadas llevadas a cabo por piratas informáticos y grupos de piratas informáticos en el contexto de la agresión de Rusia contra Ucrania: https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/ [↑](#footnote-ref-24)
24. Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión y por la que se deroga la Directiva (UE) 2016/1148, recientemente aprobada por los colegisladores y cuya adopción formal está prevista para finales de este año. [↑](#footnote-ref-25)
25. Propuesta de Reglamento 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](https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52022PC0454) [↑](#footnote-ref-26)
26. Conclusiones del Consejo sobre la elaboración de la posición de la Unión Europea en materia cibernética ST09364/22, 23 de mayo de 2022 [↑](#footnote-ref-27)
27. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group [↑](#footnote-ref-28)
28. [Llamamiento de Nevers para reforzar las capacidades de ciberseguridad de la UE](https://presse.economie.gouv.fr/08-03-2022-rmi-telecom-les-etats-membres-appellent-les-entreprises-du-secteur-numerique-a-renforcer-la-lutte-contre-la-desinformation-en-ligne/) [↑](#footnote-ref-29)
29. Propuesta de RECOMENDACIÓN DEL CONSEJO sobre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras críticas [COM/2022/551 final](https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022DC0551&qid=1666351317270). [↑](#footnote-ref-30)
30. Digitalizar el sistema energético: plan de acción de la UE, COM/2022/552 final [↑](#footnote-ref-31)
31. Una Brújula Estratégica para la Seguridad y la Defensa, 21 de marzo de 2022, https://www.eeas.europa.eu/sites/default/files/documents/strategic\_compass\_en3\_web.pdf. [↑](#footnote-ref-32)
32. [Ciberseguridad de las redes 5G: conjunto de instrumentos de la UE para mitigar los riesgos|Configurar el futuro digital de Europa (europa.eu).](https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures) [↑](#footnote-ref-33)
33. https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx [↑](#footnote-ref-34)
34. COM(2022) 454 final. [↑](#footnote-ref-35)
35. COM(2021) 70 final [↑](#footnote-ref-36)
36. Actualmente se está llevando a cabo, sobre la base del Reglamento Delegado (UE) 2022/30, una labor de normalización de los requisitos de ciberseguridad relativos a los equipos radioeléctricos. Si la Comisión deroga o modifica ese Reglamento Delegado, con la consecuencia de que deje de aplicarse a determinados productos sujetos a la Ley de Ciberresiliencia, la Comisión y las organizaciones europeas de normalización deberán tener en cuenta el trabajo de normalización llevado a cabo en el contexto de la Decisión de Ejecución C(2022)5637 de la Comisión acerca de la solicitud de normalización del citado Reglamento Delegado en la preparación y el desarrollo de normas armonizadas para facilitar la aplicación de la Ley de Ciberresiliencia. [↑](#footnote-ref-37)
37. Por ejemplo, tal como se indica en el análisis de los déficits de inversión en materia de defensa. [↑](#footnote-ref-38)
38. Se han puesto en marcha varias iniciativas, por ejemplo la Asociación Europea de Capacidades de Defensa. [↑](#footnote-ref-39)
39. En la Hoja de ruta sobre tecnologías críticas, la Comisión reclamó que se intensificaran tanto la cooperación en tecnologías que son esenciales para la seguridad y la defensa a largo plazo de Europa como los esfuerzos por reducir las dependencias estratégicas correspondientes. [↑](#footnote-ref-40)
40. La Comunicación conjunta sobre el análisis de los déficits de inversión en materia de defensa y el camino a seguir, en la que la Comisión y el Alto Representante han propuesto varias medidas para garantizar que la industria de la UE esté convenientemente equipada para lograr resultados tanto a corto como a largo plazo. [↑](#footnote-ref-41)
41. Equipos de Respuesta Telemática Rápida y de Asistencia Mutua en el ámbito de la Ciberseguridad (CRRT), Centro de Coordinación del Ámbito del Ciberespacio y de la Información (CIDCC), plataforma de intercambio de información sobre ciberamenazas e incidentes (CTIRISP), Federaciones de Campos de Maniobras Virtuales (CRF), Centro de la Unión Europea para el Mundo Académico y la Innovación en el Ámbito del Ciberespacio (CAIH UE). [↑](#footnote-ref-42)
42. En el marco del Programa Europeo de Desarrollo Industrial en materia de Defensa (PEDID), se han financiado seis proyectos (PANDORA, DISCRETION, CYBER4DE, ECYSAP, SMOTANET y HERMES) con un presupuesto de 39 millones EUR. En virtud del FED 2021, casi 40 millones EUR se destinarán a tres proyectos colaborativos de investigación y desarrollo en materia de ciberdefensa seleccionados para su financiación (ACTING, Aception, EU-GUARDIAN) [↑](#footnote-ref-43)
43. El equipo de proyecto sobre ciberdefensa constituye un foro en el que los Estados miembros pueden debatir asuntos de ciberdefensa con implicaciones militares. [↑](#footnote-ref-44)
44. Ficha informativa del Plan de Desarrollo de Capacidades (PDC) de la AED (28.6.2018): [Ficha informativa sobre el PDC](https://eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0fInsert%20) [↑](#footnote-ref-45)
45. Tal como se indica en la Agenda estratégica de investigación en ciberdefensa y en el programa estratégico general de investigación (OSRA) [↑](#footnote-ref-46)
46. El documento (en inglés) *Emerging Disruptive Technologies (EDTs):* *A capability-driven Action Plan* fue aprobado por la Junta Directiva de la AED (en su formación de directores de investigación y tecnología) el 16 de diciembre de 2021. [↑](#footnote-ref-47)
47. Incluido el JRC [↑](#footnote-ref-48)
48. Observatorio de Tecnologías Críticas anunciado en el Plan de acción sobre las sinergias entre las industrias civil, de la defensa y espacial. [↑](#footnote-ref-49)
49. Primera fase del Plan de Acción para 2021 de la AED. [↑](#footnote-ref-50)
50. Segunda fase del Plan de Acción para 2021 de la AED. [↑](#footnote-ref-51)
51. Estos grupos, o CapTechs, proporcionan a los expertos de los Estados miembros foros de trabajo en red y un marco flexible para los proyectos de colaboración Para más información sobre los CapTechs cibernéticos (cibernética, información, componentes) consúltese la página siguiente: https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs). [↑](#footnote-ref-52)
52. El programa estratégico general de investigación (OSRA) delimita los ámbitos de I+D que son pertinentes para la defensa y detalla las oportunidades de colaboración concretas. Hay diecisiete bloques tecnológicos, junto con sus hojas de ruta tecnológicas asociadas a las cibertecnologías, sobre la conciencia situacional de la ciberdefensa, la protección de los sistemas de comunicación militar, el tratamiento de información procedente de fuentes heterogéneas, la modelización y la simulación, la computación cuántica y la criptografía, que exploran las sinergias entre las ciberoperaciones y la guerra electrónica. La inteligencia artificial y los macrodatos desempeñan un papel clave en el tratamiento de la información. [↑](#footnote-ref-53)
53. El marco *ad hoc* de la AED se define en la Decisión (PESC) 2015/1835 del Consejo. En la actualidad, se hallan en fase de ejecución seis proyectos con elementos cibertecnológicos en este marco, con un presupuesto aproximado de 20 millones EUR (ANQUOR, CERERE, AED SOC 2, MASFAD II, PABRE II y ASSAI). [↑](#footnote-ref-54)
54. Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación [↑](#footnote-ref-55)
55. Como destaca la Comunicación conjunta sobre el análisis de los déficits de inversión en materia de defensa y el camino a seguir. [↑](#footnote-ref-56)
56. Se estima que en la UE opera un total de 2 500 pymes en las cadenas de suministro del sector de la defensa, que son multidimensionales y, a menudo, transfronterizas. Prestan sus servicios a los clientes del ámbito de la defensa, y un 7,8 % de sus actividades están relacionadas con aspectos cibernéticos. [↑](#footnote-ref-57)
57. El programa Horizonte Europa prevé que las sinergias con el FED redundarán en beneficio de la investigación civil y en defensa, aunque las actividades del Programa Marco se centrarán exclusivamente en las aplicaciones civiles. [↑](#footnote-ref-58)
58. https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/ [↑](#footnote-ref-59)
59. https://www.nato.int/strategic-concept/ [↑](#footnote-ref-60)
60. Firmadas en 2016 y 2018, respectivamente [↑](#footnote-ref-61)