



Estrasburgo, 15.2.2022
COM(2022) 60 final

**COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL
CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE
LAS REGIONES**

Contribución de la Comisión a la defensa europea

1. Introducción

En el mundo actual, la Unión Europea se enfrenta a una inestabilidad mundial y a fricciones geopolíticas crecientes, como reconoce el primer análisis exhaustivo de amenazas de la UE, realizado en noviembre de 2020 en preparación de la próxima Brújula Estratégica de la UE. Los conflictos y las crisis en nuestra vecindad y fuera de ella tienen repercusiones directas en nuestra propia seguridad, mientras que nuestras sociedades y economías son el blanco de sofisticadas amenazas híbridas, incluidos ciberataques y campañas de desinformación que tienen su origen en el extranjero. Al mismo tiempo, la crisis climática y la pérdida de biodiversidad crean retos para la seguridad mundial en general y para las operaciones civiles y militares en particular.

Lo que ha sucedido y sigue sucediendo en nuestras fronteras terrestres, aéreas y marítimas, y en torno a ellas, así como en el ciberespacio, a lo largo de importantes rutas marítimas y en el espacio ultraterrestre, pone de relieve nuestra necesidad de estar mejor preparados y ser más capaces y resilientes. En el contexto de una carrera tecnológica acelerada entre Estados Unidos y China, la Unión Europea debe afianzar y garantizar su ventaja tecnológica. A medida que evolucionan las relaciones geopolíticas y cambia nuestro entorno, la Unión debe evolucionar de manera similar e intensificar y acelerar sus capacidades colectivas para defender y proteger sus valores fundamentales y a sus ciudadanos. **El salto cualitativo de la defensa europea forma parte integrante e indispensable de la protección de la Unión y de sus ciudadanos en los próximos años y décadas.**

Los acontecimientos actuales y pasados sirven de llamada de atención para que los europeos colaboren más estrechamente en el ámbito de la defensa a fin de garantizar su propia seguridad y convertirse en un proveedor de seguridad más fuerte para otros, utilizando el conjunto de instrumentos excepcionalmente amplio de la Unión. La UE ya se ha comprometido a abordar los múltiples conflictos abiertos y enquistados en nuestra vecindad oriental y meridional, así como en diferentes regiones de África, nuestro continente vecino. El reciente **despliegue militar ruso a lo largo de la frontera oriental de Ucrania, en Bielorrusia y en la región del Mar Negro**, junto con los intentos de Moscú de alterar, dividir y redefinir la arquitectura de seguridad en Europa, ponen en tela de juicio el orden internacional basado en normas. También nos recuerdan que tenemos que hacer realidad una defensa europea más fuerte, en estrecha colaboración con la Organización del Tratado del Atlántico Norte (OTAN). El abrupto fin de la misión militar internacional en **Afganistán**, en agosto de 2021, nos enseñó que Europa necesita estar mejor preparada para hacer frente, por sí sola, a tareas complejas de estabilización y a emergencias repentinas. Hemos visto cómo la inestabilidad puede convertirse en caldo de cultivo del terrorismo y desarraigar a las personas, y cómo las potencias mundiales y regionales pueden utilizar estas situaciones para acrecentar su influencia y acceder a los recursos. A la complejidad de la situación hay que añadir el efecto multiplicador del cambio climático en el potencial de conflictos dentro de los Estados y entre ellos.

Al mismo tiempo, la UE debe reforzar su propia preparación, capacidad y resiliencia para proteger mejor a sus ciudadanos. **Las amenazas a la seguridad de la UE de carácter no solo militar van en aumento.** Nos enfrentamos a ciberataques más dañinos contra nuestras entidades

críticas, que paralizan plantas industriales, instalaciones de suministro de energía, administraciones municipales y hospitales, mientras que la manipulación de la información y las injerencias extranjeras afectan también a la esencia misma de nuestras democracias. El ataque híbrido patrocinado por el régimen de Lukashenko, que instrumentaliza a los migrantes con fines políticos, es un claro ejemplo de la naturaleza cambiante de las campañas híbridas destinadas a subvertirnos, coaccionarnos y manipularnos por debajo del umbral de la agresión armada. La UE ha respondido a esta situación con ayuda humanitaria, contactos diplomáticos con terceros países, apoyo a nuestros Estados miembros y sanciones contra los responsables. Mientras tanto, la pandemia de COVID-19 también puso de relieve la necesidad de reforzar la resiliencia, con las fuerzas armadas prestando asistencia logística, de seguridad y médica a las autoridades civiles a comienzos de 2020. En este entorno de rápida evolución, **la Unión Europea debe seguir reforzando su preparación, sus capacidades y su resiliencia, en particular, mejorando los mecanismos de absorción de choques y creando su caja de herramientas en todos los sectores pertinentes.**

Los Estados miembros están trabajando para hacer frente con mayor firmeza a todas las amenazas y retos a través de la nueva **Brújula Estratégica de la UE sobre seguridad y defensa** («Brújula Estratégica»), que los Estados miembros adoptarán en marzo de 2022. Establecerá una visión estratégica común para la próxima década y esbozará la manera en que la UE reforzará su capacidad para actuar y responder a diversas crisis y retos; afianzará sus intereses y protegerá a sus ciudadanos; invertirá e innovará para desarrollar conjuntamente las capacidades y tecnologías necesarias; e intensificará las asociaciones basadas en los valores e intereses de la UE. Con la presente Comunicación, la Comisión Europea contribuye en mayor medida a esta labor.

La Unión Europea debe actuar ahora para impulsar sus capacidades de defensa en el contexto actual y equipar también a la UE para hacer frente a los futuros campos de batalla, que abarcan una nueva generación de tecnologías de vanguardia capaces de abordar las amenazas derivadas de los sistemas autónomos y colaborativos cibernéticos, híbridos y espaciales, basados en la conectividad y la inteligencia artificial (IA). Al mismo tiempo, el ecosistema industrial que la defensa conforma junto con el sector aeroespacial y de la seguridad constituye un **ecosistema industrial de alta tecnología**, que no solo es un motor esencial para la autonomía estratégica abierta y la soberanía tecnológica de Europa, sino que también contribuye de forma fundamental al crecimiento y la innovación. Además de contribuir a la seguridad de los ciudadanos de la Unión Europea, el sector europeo de la defensa puede apoyar la **recuperación económica** tras la pandemia y acrecentar el carácter innovador general de un ecosistema que puede suponer una enorme contribución para la transición ecológica y dar lugar a efectos indirectos positivos para uso civil.

La consecución de nuestros objetivos solo es posible mediante **el desarrollo, la adquisición y la utilización conjunta de material de defensa**. La UE ha puesto en marcha nuevas herramientas

e instrumentos¹ para invertir las prolongadas fragmentaciones que obstaculizan la eficiencia del sector europeo de la defensa y reducen la capacidad de la UE y de sus Estados miembros de crear las capacidades de defensa de nueva generación que serán esenciales para la seguridad futura de Europa y su capacidad de garantizar la seguridad en su vecindad y fuera de ella.

En particular, el Fondo Europeo de Defensa (FED)², con un presupuesto cercano a los 8 000 millones EUR para el período 2021-2027, ya es un punto de inflexión para establecer un ecosistema europeo de defensa capaz de proporcionar tecnologías y equipos de defensa interoperables de última generación que refuercen la libertad de acción de la Unión y su soberanía y competitividad tecnológicas.

En este contexto difícil, la Comisión Europea seguirá colaborando estrechamente con el Alto Representante y los Estados miembros para:

- garantizar una **aplicación eficaz y específica** de los instrumentos e iniciativas innovadores que hemos puesto en marcha, como el FED y el Plan de Acción sobre Movilidad Militar, en particular a través de una serie de medidas adicionales que se exponen en la presente Comunicación;
- apoyar una **cooperación más estrecha en materia de defensa entre los Estados miembros y entre las industrias**, respaldada por los recursos financieros necesarios y un mayor gasto colaborativo en consonancia con los compromisos existentes, para mejorar la rentabilidad, reforzar la interoperabilidad, fomentar la innovación y aumentar la competitividad y la resiliencia industriales;
- reforzar nuestra capacidad de **responder a crisis agudas**, incluidos los ciberataques y las campañas híbridas, así como de hacer frente a los **retos a más largo plazo y las controversias geopolíticas en ámbitos estratégicos**, sobre la base de un enfoque que implique a toda la administración y reforzando las sinergias civiles y militares del doble uso a través de una amplia variedad de políticas, herramientas e instrumentos dirigidos por la Comisión;
- mantener y mejorar la **estrecha interacción con la OTAN**, en consonancia con los compromisos asumidos y los principios acordados que guían la cooperación UE-OTAN en virtud de las declaraciones conjuntas, así como con otros socios internacionales clave, como las Naciones Unidas y los socios bilaterales afines, incluidos los Estados Unidos de América, Noruega³ y Canadá.

En este contexto geopolítico y tecnológico en constante evolución, y con vistas a la próxima cumbre informal que se celebrará en París los días 10 y 11 de marzo de 2022, la presente Comunicación esboza **nuevas medidas e iniciativas concretas en una serie de ámbitos críticos**

¹ Incluidos el Fondo Europeo de Defensa, la Cooperación Estructurada Permanente (CEP) y la revisión anual coordinada de la defensa (CARD).

² PE/11/2021/INIT.

³ Como miembro del Espacio Económico Europeo.

y señala los principales factores de éxito para lograr un mercado europeo de la defensa más competitivo y armonizado. Se trata, en particular, de:

- **incrementar las inversiones en investigación en materia de defensa y en las capacidades desarrolladas en los marcos de cooperación de la UE;**
- **facilitar las sinergias entre la investigación y la innovación en los ámbitos civiles y de la defensa y reducir las dependencias estratégicas;**
- **incentivar la adquisición conjunta de capacidades de defensa desarrolladas de manera colaborativa dentro de la UE;**
- **instar a los Estados miembros a que sigan avanzando hacia prácticas de control de las exportaciones racionalizadas y más convergentes, en particular en lo que respecta a las capacidades de defensa desarrolladas en un marco de la UE;**
- **consolidar la dimensión de seguridad y defensa del espacio a escala de la UE;**
- **reforzar la resiliencia europea, por ejemplo, intensificando la ciberseguridad y luchando contra las ciberamenazas y cualquier otra amenaza híbrida, mejorando la movilidad militar y abordando los retos del cambio climático para la defensa.**

Sobre estas bases, y aprovechando las sinergias entre las políticas interiores y exteriores, incluidas las promovidas en el marco de la Estrategia para una Unión de la Seguridad de 2020, en los próximos años la Comisión seguirá contribuyendo activamente al proceso de construcción de una **Unión Europea de Defensa** con iniciativas y proyectos específicos, utilizando todo el abanico de instrumentos a su disposición para responder mejor a las amenazas rápidamente cambiantes y de múltiples niveles a las que nos enfrentamos.

2. Incrementar las inversiones en investigación en materia de defensa y en las capacidades desarrolladas en marcos de cooperación de la UE

El FED es un **programa ambicioso, equilibrado e integrador** que garantiza una fuerte participación de los Estados miembros para que los proyectos financiados satisfagan las necesidades operativas de las fuerzas armadas, allanando el camino para la producción y la adquisición. Sus **criterios de admisibilidad** mantienen el mercado abierto, reforzando al mismo tiempo la competitividad de la industria europea de la defensa y protegiendo la seguridad y los intereses estratégicos de la UE.

Para finales de 2022, la Comisión Europea habrá invertido 1 900 millones EUR en proyectos de investigación y desarrollo de capacidades en materia de defensa que respondan a las necesidades de capacidades de los Estados miembros. De este modo, **pondrá en marcha proyectos clave de desarrollo colaborativo de capacidades a gran escala** que aborden deficiencias críticas, al tiempo que **estimulará la innovación en materia de defensa**, en particular en ámbitos especializados. Esto incluye proyectos de menor escala y convocatorias abiertas que amplían la participación transfronteriza de las empresas emergentes y las pequeñas y medianas empresas (pymes), dedicando hasta el 8 % de su presupuesto de 2021 a la financiación de tecnologías disruptivas para la defensa, y alrededor del 6 % a convocatorias abiertas para las pymes. Estas representan el 48 % de las 1 100 entidades que han presentado propuestas y el 20 % de la

demanda total de financiación⁴ para las convocatorias del FED de 2021⁵. La Comisión seguirá promoviendo la participación de las pymes en toda la UE, fomentando, en particular, la integración de las más innovadoras y competitivas en las cadenas de suministro.

Las primeras convocatorias de propuestas publicadas en **2021 ya prevén asignar unos 700 millones EUR a proyectos que abordan plataformas y sistemas de defensa complejos y a gran escala**, como sistemas de combate de nueva generación, flotas de vehículos terrestres, buques patrulla de alta mar polivalentes y modulares, y sistemas de defensa contra misiles balísticos.

También a través de su programa precursor del desarrollo⁶, **dos grandes proyectos de desarrollo de capacidades de gran importancia estratégica recibieron una subvención total de unos 140 millones EUR**. El Sistema MALE RPAS apoya el desarrollo de un dron de altitud media y gran autonomía. Contribuye a la consolidación de la soberanía tecnológica en drones, un activo fundamental para las fuerzas armadas de los Estados miembros. La Radio Europea Segura definida por Software (ESSOR) impulsará la interoperabilidad mediante la normalización europea de las tecnologías de comunicación seguras en el ámbito de la defensa. Otros proyectos destacados que reciben financiación se centran, entre otras cosas, en el mando y control, la toma de decisiones basada en la IA, el combate colaborativo, la ciberdefensa o la observación espacial.

El desarrollo de las capacidades de defensa es un proceso a largo plazo que requiere una planificación coordinada y previa. **La orientación estratégica del FED se proporciona a través de las prioridades en materia de capacidades de defensa comúnmente acordadas por los Estados miembros en el marco de la Política Común de Seguridad y Defensa (PCSD)** y, en particular, en el contexto del Plan de Desarrollo de Capacidades (PDC) y en coherencia con otras iniciativas de la UE relacionadas con la defensa, como la revisión anual coordinada de la defensa (CARD) y la Cooperación Estructurada Permanente (CEP).

Además, con el fin de proporcionar transparencia y previsibilidad, especialmente con vistas a la planificación de los presupuestos nacionales de defensa, la Comisión ha elaborado una **perspectiva plurianual indicativa y flexible** para los próximos cuatro años, que se revisará cada año a la luz de la evolución de la situación. Garantiza la coherencia de los proyectos colaborativos de capacidades de defensa y de los programas de trabajo a lo largo de la duración del FED, al tiempo que proporciona transparencia y previsibilidad. En este contexto, la Comisión y los Estados miembros seguirán reforzando la perspectiva anual plurianual **teniendo en cuenta las capacidades clave y los catalizadores estratégicos señalados como prioridades por los Estados miembros tras la adopción de la Brújula Estratégica**.

⁴ Incluidos los subcontratistas.

⁵ En el marco del programa precursor, el Programa Europeo de Desarrollo Industrial en materia de Defensa (PEDID), en 2020, año para el que se dispone de resultados, las pymes representaron el 35 % de las entidades y se beneficiaron del 30 % de la financiación total de los 26 proyectos, y esto sin tener en cuenta la participación de subcontratistas, que a menudo son pymes.

⁶ Programa Europeo de Desarrollo Industrial en materia de Defensa (PEDID).

Gracias a su efecto catalizador, el FED seguirá allanando el camino para inversiones específicas en defensa en apoyo de la base industrial y tecnológica de la defensa europea (BITDE) y adaptándose a las prioridades comúnmente acordadas por los Estados miembros dentro de la UE. Para apoyar mejor el desarrollo de proyectos de capacidades de defensa a gran escala, debe evaluarse la posibilidad de programas de trabajo plurianuales en el contexto de la revisión intermedia del FED. Es igualmente importante **garantizar que otras políticas horizontales**, como las iniciativas sobre finanzas sostenibles, **sigan siendo coherentes con los esfuerzos de la Unión Europea para facilitar a la industria europea de la defensa un acceso suficiente a la financiación y a la inversión.**

Con el fin de seguir mejorando tanto la cooperación en el marco del FED como la integración del mercado interior de la defensa, la Comisión también seguirá trabajando con los Estados miembros para aprovechar las posibilidades que ofrece la Directiva 2009/43/CE⁷, relativa a la transferencia de productos relacionados con la defensa dentro de la UE, con vistas a facilitar las transferencias relacionadas con proyectos colaborativos financiados por la UE. Al asesorar sobre las normas y procedimientos en virtud de la Directiva 2009/43/CE y trabajar para alcanzar el consenso entre los Estados miembros, la Comisión tratará de simplificar la transferencia de productos relacionados con la defensa dentro del mercado interior, en particular en el marco de proyectos colaborativos financiados por la UE, y de facilitar el intercambio de las mejores prácticas.

Es fundamental incrementar la coordinación, el enfoque y el nivel de las inversiones colaborativas en defensa para mejorar la eficiencia global de los gastos de defensa dentro de la UE, teniendo en cuenta al mismo tiempo los compromisos existentes, como los asumidos en el contexto de la CEP, de aumentar periódicamente los presupuestos de defensa. El suministro colectivo de capacidades estratégicas de defensa solo puede lograrse mediante una planificación coordinada, así como mediante inversiones públicas nacionales y de la UE centradas en prioridades comunes de investigación y desarrollo en materia de defensa.

En este contexto, la Comisión también **desarrollará nuevos incentivos para estimular las inversiones colaborativas de los Estados miembros en capacidades estratégicas de defensa, especialmente cuando se desarrollen o adquieran dentro de marcos de cooperación de la Unión Europea.** La Comisión incluirá un capítulo con observaciones sobre la evolución, las oportunidades y los obstáculos relacionados con los **proyectos multinacionales de capacidades de defensa en el informe anual sobre el mercado único**, que suele publicarse junto con el paquete de otoño del Semestre Europeo. En este contexto, la Comisión también podría estudiar la manera de intensificar los esfuerzos colectivos para garantizar y coordinar la cofinanciación de los Estados miembros canalizada a través del FED con vistas a garantizar una mayor rentabilidad.

Camino a seguir

⁷ Directiva 2009/43/CE del Parlamento Europeo y del Consejo, de 6 de mayo de 2009, sobre la simplificación de los términos y las condiciones de las transferencias de productos relacionados con la defensa dentro de la Comunidad.

- Con el FED, la Comisión seguirá animando encarecidamente a los Estados miembros a definir con mayor precisión las prioridades y los catalizadores estratégicos en materia de capacidades de defensa tras la adopción de la Brújula Estratégica a través del Plan de Desarrollo de Capacidades revisado y de los resultados de la revisión anual coordinada de la defensa. También contribuirá a armonizar la planificación de la defensa y el gasto colectivo para apoyar su desarrollo.
- La Comisión desarrollará incentivos complementarios para estimular las inversiones colaborativas de los Estados miembros en capacidades estratégicas de defensa, en particular las que se desarrollen o adquieran conjuntamente en los marcos de cooperación de la Unión Europea, e informará sobre la evolución, las oportunidades y los obstáculos relacionados con los proyectos multinacionales de capacidades de defensa en el informe anual sobre el mercado único.
- En 2022, la Comisión continuará colaborando con los Estados miembros para seguir facilitando la transferencia de productos de defensa financiados por la UE dentro del mercado interior, en particular apoyando el pleno aprovechamiento de las posibilidades que ofrece la Directiva 2009/43/CE.

3. Facilitar las sinergias entre la investigación y la innovación en los ámbitos civiles y de la defensa y reducir las dependencias estratégicas

En su hoja de ruta sobre tecnologías críticas para la seguridad y la defensa, adoptada junto con la presente Comunicación⁸, la Comisión esboza una vía para impulsar la investigación, el desarrollo tecnológico y la innovación, y para reducir las dependencias estratégicas de la UE en tecnologías críticas y cadenas de valor para la seguridad y la defensa.

Sobre la base de la «Actualización del nuevo modelo de industria de 2020: Creación de un mercado único más sólido para la recuperación de Europa»⁹ y el Plan de acción sobre las sinergias entre las industrias civil, de la defensa y espacial¹⁰, propone un camino a seguir para que la UE y los Estados miembros:

- señalen las tecnologías críticas para la seguridad y la defensa de la UE;
- promuevan, desde el principio, un enfoque estratégico y coordinado a escala de la UE para estas tecnologías críticas, aprovechando los programas de investigación, desarrollo tecnológico e innovación;
- reduzcan las dependencias estratégicas.

Esto requiere una mayor concienciación sobre el carácter crítico de determinadas tecnologías — como los semiconductores— para los sectores de la seguridad y la defensa, una mejor determinación de las dependencias estratégicas conexas y posibles medidas de mitigación,

⁸ COM(2022) 61 final.

⁹ COM(2021) 350 final.

¹⁰ COM(2021) 70 final.

teniendo en cuenta la diversidad de las fuentes y la posibilidad de que el uso operativo de la tecnología pueda verse comprometido o denegado¹¹. El Observatorio de Tecnologías Críticas¹² (en lo sucesivo, «el Observatorio») establecerá un mecanismo específico para identificar dichas evaluaciones, sobre la base de las aportaciones de los Estados miembros y de la industria. Las conclusiones del Observatorio serán decisivas para impulsar la investigación, el desarrollo tecnológico y la innovación de la UE en estas tecnologías, con un enfoque coordinado a escala de la UE. Este trabajo complementa los esfuerzos más amplios para abordar la seguridad del suministro de bienes civiles esenciales, en ámbitos como la salud y la energía¹³.

La Comisión también preparará un **enfoque para fomentar el doble uso para la investigación y la innovación a escala de la UE**, y desplegará un plan de innovación en materia de defensa para apoyar la innovación y el espíritu empresarial en tecnologías críticas, en estrecha coordinación con el centro de innovación en materia de defensa que creará la Agencia Europea de Defensa (AED).

Por último, con el fin de reducir las dependencias estratégicas, la Comisión seguirá evaluando sistemáticamente las consideraciones de seguridad y defensa a la hora de aplicar y revisar los instrumentos de la UE existentes o de diseñar nuevos instrumentos.

4. Incentivar la adquisición conjunta de capacidades desarrolladas de manera colaborativa dentro de la UE

La **adquisición conjunta de capacidades de defensa europeas** por parte de los Estados miembros **aumenta sustancialmente la interoperabilidad** de las fuerzas armadas nacionales europeas y **apoya la competitividad de la BITDE**, en particular a través de mayores economías de escala.

Sin embargo, los Estados miembros aún no han alcanzado el valor de referencia colectivo de adquisición de equipos en régimen de cooperación europea¹⁴, es decir, el 35 % del gasto en material de defensa, que han confirmado en el marco de la CEP¹⁵. Según la AED, en 2020 los Estados miembros¹⁶ gastaron alrededor de 37 000 millones EUR en adquisición de material de defensa (es decir, adquisición de nuevo material de defensa). De este importe, solo alrededor del 11 % (en torno a 4 100 millones EUR)¹⁷ se destinó a gastos de adquisición de material de

¹¹ Por lo que se refiere a los semiconductores, véase la hoja de ruta sobre tecnologías críticas para la seguridad y la defensa que acompaña a la presente Comunicación, sección 2.2, y la Comunicación de la Comisión «Ley de Chips para Europa», COM(2022) 45 final.

¹² En asociación con los servicios pertinentes de la Comisión y con la Agencia Europea de Defensa.

¹³ En consonancia con las propuestas de la Comisión COM(2021) 577, de 16.9.2021, sobre un marco de medidas para garantizar el suministro de contramedidas médicas pertinentes para la crisis en caso de emergencia de salud pública, COM(2021) 660, de 13.10.2021, sobre medidas de actuación y apoyo para hacer frente al aumento de los precios de la energía, y COM(2021) 350, sobre la actualización de la nueva estrategia industrial.

¹⁴ En noviembre de 2007, el Comité de Dirección Ministerial de la AED aprobó cuatro valores de referencia colectivos para la inversión, incluido el 35 % del gasto total en material para la adquisición de material en régimen de cooperación europea.

¹⁵ [EUR-Lex - 32021H1117\(01\) - ES - EUR-Lex \(europa.eu\)](#)

¹⁶ Excepto DK.

¹⁷ Sobre la base de los datos facilitados por once Estados miembros.

defensa en régimen de cooperación europea (es decir, adquisición de nuevo material de defensa en colaboración con otros Estados miembros). Esto significa que la mayor parte de los gastos de adquisición de material de defensa de los Estados miembros (alrededor del 89 %) se realizaron a escala nacional o en cooperación con terceros países.

El año 2020 no es una excepción e incluso puede considerarse parte de una tendencia que ha empeorado en los últimos años. De hecho, el porcentaje de la adquisición de material de defensa en régimen de cooperación europea ha disminuido constantemente desde 2016, y la cifra de 2020 es la más baja desde que se recopilan estos datos (2005).

Dos instrumentos de la UE ya allanan el camino a la adquisición pública conjunta. Como condición para el apoyo financiero a las acciones de desarrollo, el Reglamento del FED exige que los Estados miembros tengan la intención de adquirir el producto final o utilizar la tecnología de manera coordinada. La **Directiva 2009/81/CE sobre contratación pública en el ámbito de la defensa** contempla la exclusión específica de las normas de contratación pública para los proyectos cooperativos basados en la investigación y el desarrollo (I+D)¹⁸. Esta exclusión se aplica también a las fases del ciclo de vida posterior a la I+D si los contratos se adjudican en el marco del mismo proyecto cooperativo. En 2019, la Comisión publicó una Comunicación¹⁹ en la que proporcionaba orientaciones sobre diversas posibilidades de contratación cooperativa ofrecidas en virtud de la Directiva. Los Estados miembros podrán disponer de más apoyo, en particular a través del Grupo de Expertos sobre Contratación Pública en materia de Defensa y Seguridad.

La Comisión pretende **incentivar en mayor medida la adquisición conjunta de capacidades de defensa europeas por parte de los Estados miembros**, también en relación con las operaciones y el mantenimiento. Sin embargo, hay una serie de obstáculos prácticos, financieros y fiscales, que deben abordarse a tal fin.

La Comisión examinará la posibilidad de una exención del **impuesto sobre el valor añadido (IVA) para apoyar la adquisición conjunta y la copropiedad de las capacidades de defensa que se desarrollen de forma colaborativa dentro de la UE**. Estas capacidades estarán disponibles para su uso por los Estados miembros para misiones y operaciones en el marco de la PCSD²⁰ o en el contexto de las actividades de las Naciones Unidas, la OTAN y nacionales. Esta medida podría resultar especialmente beneficiosa para las capacidades desarrolladas en los marcos cooperativos de la UE (FED o CEP o en el seno de la AED). En este contexto, podría considerarse el establecimiento de un marco jurídico inspirado en el Consorcio de Infraestructuras de Investigación Europeas²¹ que se beneficiaría de una exención del IVA sobre el material que los consorcios de los Estados miembros compraran y poseyeran.

¹⁸ Artículo 13 de la Directiva 2009/81/CE.

¹⁹ 2019/C 157/01.

²⁰ En consonancia con las fuerzas multinacionales contempladas en el artículo 42, apartado 3, del Tratado de la Unión Europea.

²¹ El Consorcio de Infraestructuras de Investigación Europeas (ERIC) es una forma jurídica específica que facilita la creación y el funcionamiento de infraestructuras de investigación de interés europeo.

Del mismo modo, sobre la base de las enseñanzas extraídas de la evaluación intermedia del FED, la Comisión estudiará la posibilidad de reforzar el actual **sistema de bonificación del FED, a fin de ofrecer un incentivo financiero** a condición de que **los Estados miembros se comprometan a adquirir o poseer conjuntamente las capacidades de defensa en fase de desarrollo**²². Esto ofrecería mayores incentivos para garantizar que la colaboración prosiga más allá de las fases de I+D, es decir, en las fases de adquisiciones, operaciones y mantenimiento.

Además, sobre la base del trabajo del Grupo de expertos de instrumentos financieros, las **nuevas soluciones de financiación** podrían dar lugar a un mayor uso por parte de los Estados miembros de entidades de adquisición conjunta ya existentes, como la AED o la Organización Conjunta de Cooperación en Materia de Armamento (OCCAR). En particular, la Comisión evaluará si las disposiciones del Reglamento del FED, como las relativas a la contratación precomercial²³, pueden proporcionar apoyo financiero a los poderes adjudicadores y a las entidades de adquisición conjunta para seguir coordinando sus procedimientos de adquisición, en particular cubriendo los costes administrativos o de transacción relacionados con la adquisición conjunta de servicios de investigación y desarrollo en materia de defensa.

Camino a seguir

- Para principios de 2023, la Comisión presentará una propuesta que permita una **exención del IVA** para apoyar la adquisición conjunta y la copropiedad de las capacidades de defensa desarrolladas de forma colaborativa dentro de la UE, garantizando al mismo tiempo el cumplimiento de las normas de la Organización Mundial del Comercio.
- Para mediados de 2023, la Comisión se basará en el trabajo del Grupo de expertos de instrumentos financieros con vistas a proponer **nuevas soluciones de financiación** para facilitar la adquisición conjunta de capacidades estratégicas de defensa de la UE por parte de los Estados miembros sobre la base de los conocimientos ya disponibles.
- Tras la evaluación intermedia del FED²⁴, la Comisión estudiará una posible modificación del artículo 13 del Reglamento (UE) 2021/697, por el que se establece el Fondo Europeo de Defensa, para reforzar **el sistema de bonificación del FED cuando los Estados miembros se comprometan a adquirir o poseer conjuntamente las capacidades de defensa en fase de desarrollo**.

5. Instar a los Estados miembros a que sigan avanzando hacia prácticas de control de las exportaciones racionalizadas y más convergentes

Si bien los Estados miembros se encargan de expedir las licencias de exportación de equipos militares, evalúan sus decisiones sobre la base de la Posición Común del Consejo²⁵ que define

²² Más allá del requisito de subvencionabilidad especificado en el artículo 21, apartado 3, letra a), del Reglamento del FED, que exige la intención de adquirir el producto final o de utilizar la tecnología de manera coordinada.

²³ Artículo 17 del Reglamento del FED.

²⁴ La evaluación intermedia debe llevarse a cabo, a más tardar, cuatro años (2025) después del inicio del período de ejecución del Fondo, de conformidad con el artículo 29 del Reglamento por el que se establece el FED.

²⁵ Posición común 2008/944/PESC.

los criterios comunes para controlar la exportación de tecnología y equipos militares. También establece mecanismos de notificación de denegaciones y de consulta con vistas a aumentar la convergencia en la aplicación de sus políticas de exportación de productos relacionados con la defensa.

Sin embargo, dado que el desarrollo conjunto de capacidades de defensa se convertirá progresivamente en la norma en la UE, y no en la excepción, **los Estados miembros se beneficiarán de un intercambio de buenas prácticas más intenso, que gradualmente conducirá a un enfoque más convergente en cuanto a los controles de las exportaciones de armas.** Basándose en el trabajo ya realizado y reconociendo que las exportaciones son un factor clave para el éxito del modelo de negocio de la industria europea de la defensa, la Comisión apoya el avance gradual de los Estados miembros hacia una mayor racionalización y una mayor convergencia de las prácticas de control de las exportaciones de armas, especialmente en lo que respecta a las capacidades de defensa que desarrollan conjuntamente, en particular en el marco del FED.

En este contexto, **la Comisión acoge con satisfacción la reflexión iniciada en el Consejo**²⁶ sobre la exportación de capacidades desarrolladas en un marco de la UE y anima a los Estados miembros a proseguir estos debates para facilitar los procedimientos de control de las exportaciones para tales productos. Este proceso también podría basarse en la experiencia de los acuerdos bilaterales y multilaterales entre Estados miembros sobre capacidades desarrolladas conjuntamente.

Con el fin de no obstaculizar la cooperación, este trabajo debe facilitar la definición de procedimientos claros y fáciles de aplicar. Deben definirse medidas eficaces de control de las exportaciones que proporcionen a los productos financiados por el FED un acceso adecuado y competitivo a los mercados internacionales, preservando al mismo tiempo las decisiones soberanas de los Estados miembros, respetando plenamente sus obligaciones jurídicas pertinentes y teniendo en cuenta sus intereses de seguridad nacional. Para preservar el atractivo de los proyectos conjuntos de capacidades de defensa, **la Comisión invita a los Estados miembros a buscar un enfoque según el cual, en principio, no se impidan mutuamente exportar a un tercer país los equipos y tecnologías militares desarrollados en cooperación.** Esto podría aplicarse a las exportaciones previstas de equipos o tecnología que incorporen componentes de otro Estado miembro que superen un determinado umbral mínimo.

Camino a seguir

- La Comisión invita a los Estados miembros a explorar formas de racionalizar y de lograr, gradualmente, una mayor convergencia de sus prácticas de control de las exportaciones de armas, especialmente en el caso de las capacidades de defensa que se desarrollen conjuntamente, en particular en un marco de la UE, garantizando así que los productos financiados por el FED se beneficien de un acceso adecuado y competitivo a los mercados internacionales, sin perjuicio de las decisiones soberanas de los Estados

²⁶ Dentro del Subgrupo «Exportación de Armas Convencionales» (COARM) del Grupo «No Proliferación y Exportación de Armas».

6. Consolidar la dimensión de defensa del espacio a escala de la UE

El espacio es un ámbito estratégico para **la libertad de acción y la seguridad de la UE**. Al mismo tiempo, se trata de un entorno cada vez más congestionado y controvertido, caracterizado por una creciente competencia entre las potencias.

Estos retos deben abordarse con carácter de urgencia. La nueva estrategia espacial de la UE para la seguridad y la defensa, sometida actualmente a la consideración de los Estados miembros en el contexto de la Brújula Estratégica, debería contribuir a crear una interpretación común de los riesgos y amenazas relacionados con el espacio, a desarrollar respuestas adecuadas para reaccionar mejor y más rápidamente a las crisis, a reforzar nuestra resiliencia y a aprovechar plenamente los beneficios y oportunidades relacionados con el ámbito espacial. Sin perjuicio del contenido de la futura estrategia conjunta, se considerarán las siguientes acciones:

En primer lugar, los activos espaciales de la UE²⁷ deben protegerse mejor para aumentar la resiliencia de la UE en el espacio y desde el espacio.

En la Comunicación conjunta sobre la **gestión del tráfico espacial (GTE)**²⁸, la Comisión y el Alto Representante ofrecen orientaciones concretas sobre cómo aumentar la protección de los activos espaciales de la UE y promover un uso más sostenible del espacio. En particular, la Comisión reforzará sus **activos de vigilancia espacial** gracias a la mejora de los servicios de **vigilancia y seguimiento espacial (VSE)** y el desarrollo de tecnologías conexas, como la prevención automática de colisiones o la inteligencia artificial.

La Comisión también seguirá apoyando el desarrollo de proyectos relacionados con el **conocimiento del medio espacial (SSA) y las capacidades de alerta rápida para la defensa**. Estos proyectos contribuirán al establecimiento de capacidades avanzadas de mando y control espacial (SC2), de sensores SSA avanzados y de un sistema de alerta precoz contra las amenazas de misiles balísticos y las nuevas amenazas hipersónicas²⁹.

En segundo lugar, la Comisión reforzará la dimensión de seguridad y defensa en las infraestructuras espaciales de la UE existentes y futuras, en cooperación con el Alto Representante.

El **servicio público regulado (PRS) de Galileo**³⁰ ofrece un servicio de navegación reservado a los usuarios autorizados por los gobiernos para aplicaciones sensibles. Estas requieren un alto nivel de continuidad del servicio, utilizando señales potentes y cifradas, especialmente en el

²⁷ El Programa Espacial de la UE consta de cuatro componentes: Galileo/EGNOS para el posicionamiento, la navegación y la temporización, Copernicus para la observación de la Tierra, Govsatcom para la seguridad de las comunicaciones gubernamentales por satélite y SSA para el conocimiento del medio espacial.

²⁸ JOIN(2022) 4 final.

²⁹ Estos proyectos reciben el apoyo del FED y de sus programas precursores.

³⁰ Decisión n.º 1104/2011/UE del Parlamento Europeo y del Consejo, de 25 de octubre de 2011, relativa a las modalidades de acceso al servicio público regulado ofrecido por el sistema mundial de radionavegación por satélite resultante del programa Galileo, DO L 287 de 4.11.2011.

ámbito de la seguridad y la defensa. El PRS está concebido para ofrecer un servicio ilimitado e ininterrumpido en todo el mundo. Es una demostración clara de que una infraestructura común bajo control civil puede satisfacer las necesidades de defensa y seguridad.

La propuesta de Reglamento por el que se establece el **programa de conectividad segura de la Unión** para 2022-2027³¹, adoptado a la vez que la presente Comunicación dentro del paquete relativo al espacio, reforzará la resiliencia de la UE en cuanto a conectividad gracias a las comunicaciones gubernamentales seguras. Incluirá, desde el principio, requisitos de defensa en términos de resiliencia, mientras que la constelación de satélites en órbita terrestre baja (LEO) brindará la oportunidad de embarcar cargas útiles que contribuyan a otros componentes del programa espacial de la UE. El sistema se basará en Govsatcom y en las sinergias con el Fondo Europeo de Defensa.

La evolución de Copernicus también debe tener en cuenta, en la medida de lo posible, las exigencias en materia de defensa, prestando especial atención a los niveles requeridos de seguridad y rendimiento, y apoyándose en una gobernanza adecuada basada en la confianza.

Para impulsar el desarrollo de la dimensión de defensa de las infraestructuras espaciales de la UE existentes y futuras, la Comisión apoyará el desarrollo de **capacidades de defensa espacial a través del FED**. Hasta la fecha, se han asignado unos 130 millones EUR para financiar acciones relacionadas con el espacio en el marco del FED y de sus programas precursores.

Dado que la Comisión apoya el desarrollo de plataformas colaborativas para futuros retos en materia de defensa, también pretende mejorar su rendimiento haciendo el mejor uso posible de los activos espaciales europeos existentes y futuros. Por ejemplo, el proyecto **Galileo para la Defensa de la UE** (GEODE) está cofinanciado con 44 millones EUR³² y tiene por objeto desarrollar receptores de navegación militar normalizados europeos que sean compatibles con el PRS de Galileo. También se invertirán más de 22 millones EUR con el fin de mejorar los sensores y el mando y control (C2) para el conocimiento militar del medio espacial de la UE y desarrollar una capacidad de alerta precoz basada en el espacio.

En el marco del programa de trabajo del FED para 2021, este último dedicará 50 millones EUR tanto a la vigilancia de la **guerra de navegación en el espacio y en tierra (NAVWAR)**, como a las **tecnologías europeas de comunicaciones por satélite resilientes contra las interferencias**.

En tercer lugar, la Comisión trabajará para reducir las dependencias estratégicas conexas de la UE en materia de tecnologías críticas, por ejemplo en el ámbito de los chips, la informática cuántica y la IA. Para lograrlo, la Comisión maximizará las sinergias con las iniciativas relacionadas con el espacio ejecutadas en el marco de los actuales instrumentos dirigidos por la Comisión (incluidos el FED, Horizonte Europa³³, el Programa Espacial, el Consejo Europeo de Innovación e InvestEU) y aprovechará el Observatorio de Tecnologías

³¹ COM(2022) 57 final.

³² Con cargo al Programa Europeo de Desarrollo Industrial en materia de Defensa (PEDID).

³³ El término «Horizonte Europa» en el presente documento se refiere al programa específico por el que se ejecuta Horizonte Europa y el Instituto Europeo de Innovación y Tecnología; las actividades realizadas en el marco de los mismos se centran exclusivamente en las aplicaciones civiles.

Críticas. La Comisión reforzará, asimismo, la **resiliencia de las cadenas de suministro europeas conexas** para garantizar la integridad, la seguridad y el funcionamiento de las infraestructuras espaciales.

En cuarto lugar, la Comisión, en cooperación con el Alto Representante, en consonancia con sus respectivos mandatos, llevará a cabo la ampliación del actual mecanismo de respuesta a las amenazas de Galileo³⁴ a los sistemas y servicios de los demás componentes del Programa Espacial de la UE. Ello reforzará en mayor medida la gobernanza de la seguridad de las infraestructuras espaciales de la UE para responder mejor a las amenazas y promoverá la aplicación de una gobernanza adecuada por parte de los actores pertinentes. La Comisión y el Alto Representante mejorarán también el conocimiento del medio a escala de la UE gracias a un mejor uso de los datos espaciales, en estrecha cooperación con los Estados miembros y en el marco de una cooperación sistemática entre las agencias u organismos competentes que exploten las infraestructuras de la UE.

La Comisión y el Alto Representante contribuirán asimismo a los esfuerzos de los Estados miembros por seguir reforzando la asistencia mutua y los mecanismos de respuesta a las crisis, en particular mediante ejercicios e impulsando la capacidad de reacción frente a las amenazas, fomentando la interoperabilidad y apoyando una cultura estratégica común.

Camino a seguir

- Tras la adopción de la Brújula Estratégica, la Comisión y el Alto Representante propondrán una estrategia espacial conjunta de la UE para la seguridad y la defensa.
- Para finales de 2022, la Comisión estudiará la manera de reforzar en mayor medida la **protección de los activos espaciales de la UE**, en particular mediante servicios de Vigilancia y Seguimiento Espacial (VSE) adicionales, la mejora del rendimiento de la VSE de la UE y el pleno aprovechamiento del potencial de la industria de la UE.
- A partir de 2022, la Comisión promoverá un enfoque de **«doble uso desde la concepción»** para las infraestructuras espaciales de la UE, con vistas a ofrecer nuevos servicios resilientes que respondan a las necesidades de los gobiernos. En este contexto, la Comisión anima a los legisladores a que adopten rápidamente la propuesta de Reglamento por el que se establece el programa de conectividad segura de la Unión para 2022-2027.
- La Comisión intensificará su labor para reducir las dependencias tecnológicas estratégicas y aumentar la resiliencia de las cadenas de suministro relacionadas con las infraestructuras espaciales, en particular a través de los instrumentos de financiación de la

³⁴ Tal como se establece en el Reglamento (UE) 2021/696 sobre el Programa Espacial de la UE y en la Decisión (PESC) 2021/698 del Consejo, de 30 de abril de 2021, sobre la seguridad de los sistemas y servicios cuyo despliegue, funcionamiento y utilización en el marco del Programa Espacial de la Unión pueden afectar a la seguridad de la Unión.

UE y del Observatorio de Tecnologías Críticas.

- La Comisión establecerá una gobernanza adecuada para las infraestructuras espaciales de la UE, en estrecha cooperación con los Estados miembros, basándose en el modelo del PRS de Galileo. Evaluará la viabilidad de desarrollar e implantar un servicio Copernicus más resiliente y seguro para fines gubernamentales³⁵, teniendo en cuenta, en la medida de lo posible, las exigencias en materia de defensa.
- Para finales de 2022, la Comisión y el Alto Representante estudiarán la posibilidad de activar los mecanismos de solidaridad, asistencia mutua y respuesta a las crisis en caso de ataques procedentes del espacio o de amenazas a activos espaciales.

7. Reforzar la resiliencia europea

Europa necesita reforzar su resiliencia para prevenir futuras crisis, protegerse frente a ellas y resistir. Debido a los vínculos intrínsecos con las políticas nacionales de seguridad y defensa, la responsabilidad de hacer frente a estas amenazas recae principalmente en los Estados miembros. Aun así, algunas vulnerabilidades son comunes a todos los Estados miembros y algunas amenazas no entienden de fronteras, como aquellas cuyo objetivo son las redes o las infraestructuras transfronterizas, o en el caso del cambio climático.

El enfoque de la UE tiene por objeto integrar las dimensiones exterior e interior en un flujo continuo. Aúna consideraciones civiles y militares a escala nacional y de la UE para promover soluciones concretas, facilitando al mismo tiempo una mayor resiliencia y la continuidad de la eficacia operativa.

7.1. Luchar contra las amenazas híbridas

En 2020, la **Estrategia de la UE para una Unión de la Seguridad**³⁶ definió las amenazas híbridas como uno de los ámbitos prioritarios que deben abordarse para mejorar la seguridad de la UE. La Estrategia sienta las bases para un enfoque renovado ante estas amenazas en constante evolución que abarque todo el abanico de acciones, desde la detección precoz, el análisis, la sensibilización, el desarrollo de la resiliencia y la prevención, hasta la respuesta a las crisis y la gestión de sus consecuencias.

La cartografía de las medidas³⁷ **relacionadas con el refuerzo de la resiliencia y la lucha contra las amenazas híbridas incluye más de doscientos instrumentos y medidas a escala de la UE**, la mayoría de ellos dirigidos o apoyados por la Comisión. Las propuestas de la Comisión en diferentes ámbitos, incluida la Ley de Servicios Digitales³⁸, la propuesta de Directiva relativa

³⁵ Servicio de tipo PRS Copernicus.

³⁶ COM(2020) 605.

³⁷ SWD(2020) 152 final.

³⁸ COM(2020) 825 final.

a la resiliencia de las entidades críticas³⁹ y el Mecanismo de Protección Civil de la Unión revisado⁴⁰, contribuirán aún más a este número cada vez mayor de instrumentos de la UE disponibles para luchar contra las amenazas híbridas.

La resiliencia es uno de los principales pilares de la lucha contra las amenazas híbridas. En un documento de trabajo conjunto de los servicios de la Comisión de enero de 2022⁴¹ se identificaron 53 **líneas de base en materia de resiliencia**⁴² a escala de la UE. Esta identificación, anunciada en la Estrategia para una Unión de la Seguridad, constituye un primer paso crucial para seguir y medir objetivamente los avances en este ámbito.

En este contexto, los servicios de la Comisión, el Servicio Europeo de Acción Exterior (SEAE) y la Secretaría General del Consejo llevarán a cabo, en noviembre de 2022, el ejercicio «EU Integrated Resolve PACE», para hacer frente, entre otras cosas, a las amenazas híbridas, incluida su ciberdimensión. Este ejercicio se llevará a cabo bajo la responsabilidad general del Alto Representante, con la participación de los Estados miembros y las agencias de la UE, y en un formato paralelo y coordinado (PACE) con la OTAN.

La Comisión también se ha **adaptado al carácter rápidamente cambiante de las amenazas**. A raíz de la crisis en la frontera de la UE con Bielorrusia, propuso medidas para hacer frente a la **instrumentalización de la migración**, como la inclusión en una lista negra de los operadores de transporte implicados en el tráfico ilícito o la trata de personas en la UE⁴³.

La pandemia de COVID-19 ha puesto de manifiesto la necesidad de reforzar la acción coordinada a nivel de la UE para responder a las emergencias sanitarias. En un momento en que las amenazas químicas, biológicas, radiológicas y nucleares podrían poner en peligro la salud pública, la Autoridad Europea de Preparación y Respuesta ante Emergencias Sanitarias (HERA) es un elemento central para reforzar la preparación y la respuesta de la UE a las amenazas transfronterizas graves para la salud, al permitir la celeridad en la disponibilidad, el acceso y la distribución de las contramedidas necesarias. A partir de las lecciones extraídas de las primeras fases de la pandemia, se seguirá trabajando para mejorar la asistencia militar a las autoridades civiles a este respecto.

Camino a seguir

- De aquí a 2023, la Comisión, en cooperación con el Alto Representante y los Estados miembros, evaluará las líneas de base sectoriales en materia de resiliencia para detectar **lagunas y necesidades**, así como las medidas para subsanarlas.
- Tras la adopción de la Brújula Estratégica, la Comisión contribuirá al futuro conjunto de instrumentos híbridos de la UE garantizando que los Estados miembros tengan una visión

³⁹ COM(2020) 829 final.

⁴⁰ Reglamento (UE) 2021/836 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021.

⁴¹ SWD(2022) 21 final.

⁴² Criterios de referencia relativos al punto de partida de una situación, al objetivo que se desea alcanzar o a los requisitos mínimos recomendados.

⁴³ COM(2021) 753 final.

completa de los instrumentos y medidas internos existentes para luchar contra las amenazas híbridas que afectan a la UE y a sus Estados miembros. Se tendrán en cuenta las medidas incluidas en la cartografía de 2020 sobre la lucha contra las amenazas híbridas y las recientes propuestas de la Comisión y el Alto Representante en ámbitos como las infraestructuras críticas y la desinformación.

- Tras la adopción de la Brújula Estratégica, la Comisión estudiará la posibilidad de seleccionar expertos en los ámbitos políticos pertinentes, que podrían desplegarse como parte del equipo de respuesta rápida contra amenazas híbridas previa solicitud, en sinergia con los equipos de respuesta rápida de la unidad informática conjunta (JCU) propuestos.
- Paralelamente, los servicios de la Comisión y el SEAE revisarán conjuntamente el protocolo de actuación de la UE para contrarrestar las amenazas híbridas («EU Playbook»).
- Para finales de 2022, la Comisión, en cooperación con el Alto Representante, definirá una visión global de sus mecanismos de alerta rápida y, en particular, de la posibilidad de trazar una imagen más clara de la situación, en coordinación y complementariedad con otros mecanismos existentes en la UE. Esto reforzará la capacidad de la Unión para el seguimiento y la detección precoz, la prevención y la preparación, incluida la resiliencia, y la respuesta a las amenazas híbridas.
- Basándose en sus conocimientos especializados y en sus instrumentos, la Comisión contribuirá al esfuerzo de la UE por crear resiliencia en los países socios.

7.2. Reforzar la ciberseguridad y la ciberdefensa

La lucha contra las amenazas a la ciberseguridad es, hoy día, uno de los retos más complejos en materia de seguridad y defensa, especialmente si se tienen en cuenta su número e impacto crecientes, y las sofisticadas capacidades específicas que han conseguido desarrollar los actores estatales.

La UE debe proteger las redes y los sistemas de información críticos y desempeñar un papel de liderazgo a la hora de garantizar la seguridad, la estabilidad y la resiliencia, así como la libertad de la internet mundial. Hemos de impulsar la ciberseguridad y la ciberdefensa en Europa reforzando nuestra cooperación, invirtiendo más eficazmente en capacidades avanzadas y estableciendo normas adecuadas que permitan una mejor vinculación de todas las dimensiones del ciberespacio. Estos esfuerzos deben centrarse en la **protección** de los ciudadanos, las empresas y los intereses de la UE, en **la detección y la disuasión** de las actividades informáticas malintencionadas y en nuestra **defensa** frente a los ciberataques, lo que contribuirá a la seguridad y la estabilidad internacionales y consolidará el potencial de ciberdisuasión de la UE.

La Comisión y el Alto Representante ya han establecido medidas ambiciosas que contribuyen a estos objetivos en la Estrategia de Ciberseguridad de la UE de diciembre de 2020⁴⁴. Existen una serie de instrumentos importantes cuyo objetivo es aumentar la resiliencia de la UE, en particular, la **Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (SRI)**⁴⁵, el **Reglamento sobre la Ciberseguridad**⁴⁶, la **Directiva relativa a los ataques contra los sistemas de información**⁴⁷, la aplicación del **conjunto de instrumentos de la UE para la seguridad de las redes 5G**⁴⁸, la **Recomendación sobre un plan director para la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala**⁴⁹ y el **marco político de ciberdefensa de la UE [actualizaciones de 2018]**⁵⁰. Asimismo, la Comisión ha adoptado un acto delegado⁵¹ en virtud de la Directiva sobre equipos radioeléctricos⁵² por el que se establecen requisitos legales para las salvaguardias de ciberseguridad, que los fabricantes deberán tener en cuenta en el diseño y la producción de equipos radioeléctricos. Por último, publicó una recomendación relativa a una **unidad informática conjunta (JCU)**⁵³ y presentó una propuesta de **revisión de la Directiva SRI** en diciembre de 2020⁵⁴, que actualmente está siendo examinada por los colegisladores. En consonancia con este nivel de ambición, la Comisión presentará en breve propuestas para mejorar la ciberseguridad y la seguridad de la información de las instituciones, órganos y agencias de la UE.

El programa de trabajo plurianual 2021-2025 de Europa Digital y del Mecanismo «Conectar Europa» (MCE – Sector digital) apoyará el despliegue de una infraestructura de comunicación cuántica segura (Euro QCI). El MCE también apoyará otras infraestructuras de comunicación críticas, incluidas algunas redes troncales entre Estados miembros y con terceros países, en las que se aplicarán las normas de seguridad más estrictas.

Para complementar estos instrumentos y reducir aún más la superficie de ataque y la exposición al riesgo, debe reforzarse la seguridad y la normalización de los productos y servicios relacionados con las tecnologías de la información y la comunicación (TIC). Esto se aplica, en particular, a la seguridad de los componentes esenciales de *hardware* y *software*. Por consiguiente, la Comisión está preparando nuevas propuestas que establezcan requisitos horizontales de seguridad, que constituirán la piedra angular de la **Ley de Ciberresiliencia**

⁴⁴ JOIN(2020) 18 final.

⁴⁵ Directiva (UE) 2016/1148 sobre la seguridad de las redes y los sistemas de información (SRI).

⁴⁶ 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.

⁴⁷ Directiva 2013/40/UE (12.8.2013).

⁴⁸ COM(2020) 50 final.

⁴⁹ 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, C/2017/6100.

⁵⁰ 14413/18 (19.11.2018).

⁵¹ C(2021) 7672.

⁵² Directiva 2014/53/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos.

⁵³ C(2021) 4520 final.

⁵⁴ COM(2020) 823 final.

anunciada en el discurso sobre el estado de la Unión⁵⁵. En este contexto podría considerarse una dimensión de defensa, en particular en lo que se refiere al posible desarrollo de normas de ciberseguridad comunes o híbridas.

Para seguir mejorando las capacidades tecnológicas de la UE y de sus actores de ciberdefensa (principalmente las fuerzas de defensa de los Estados miembros), se buscará una mayor cooperación entre los actores pertinentes en la planificación de las inversiones en los ámbitos civiles y de la defensa para el desarrollo de las tecnologías pertinentes y su uso. El **Centro de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación (CCCN)**⁵⁶ adoptarán, en 2022, su agenda estratégica sobre ciberinversiones. La agenda podría abarcar posibles sinergias entre las tecnologías civiles y de defensa y las posibles aplicaciones de doble uso, buscando así sinergias con otros programas de la UE, como Horizonte Europa, el programa Europa Digital y el FED, de manera coordinada y respetando al mismo tiempo las normas de gobernanza pertinentes.

La Comisión ya ha destinado 38,6 millones EUR⁵⁷ a seis proyectos de ciberdefensa. Este presupuesto apoya, entre otras cosas, el desarrollo de una plataforma europea de conocimiento de la situación en materia de ciberseguridad y un proyecto sobre tecnologías para una comunicación segura y resiliente. El FED seguirá apoyando el desarrollo de ciber capacidades para la defensa. En 2021, se pusieron en marcha dos convocatorias específicas en el marco del FED que recibieron una dotación financiera de 33,5 millones EUR. Si bien todos los proyectos de capacidades de defensa entrañan una ciberdimensión, la ciberdefensa seguirá siendo una prioridad para el FED en los próximos años.

A fin de prepararse mejor frente a posibles incidentes y crisis a gran escala en la Unión, es esencial reforzar la coordinación para garantizar el conocimiento de la situación, determinar rápidamente las posibles necesidades y recursos de respuesta y armonizar una comunicación eficaz entre los actores pertinentes a escala de los Estados miembros y de la UE, a fin de atenuar los posibles efectos en la Unión.

Para intensificar la **detección de actividades informáticas malintencionadas y mejorar el conocimiento de la situación**, la Comisión está colaborando con los Estados miembros en la creación de **plataformas transfronterizas para compartir información sobre amenazas para la ciberseguridad (COS UE)**, reforzando al mismo tiempo las capacidades de los centros de operaciones de seguridad (COS) a escala nacional en toda la UE. El objetivo de estas plataformas transfronterizas (COS UE) es permitir el intercambio de datos sobre amenazas a la ciberseguridad procedentes de diversas fuentes, así como de herramientas y capacidades, a gran escala, en un entorno de confianza. Estarán equipadas con herramientas e infraestructuras ultraseguras de nueva generación. Esto debería permitir mejorar las capacidades de detección colectiva y de alertar con tiempo suficiente a las autoridades y a las entidades pertinentes. Estas acciones se beneficiarán del apoyo financiero del Programa Europa Digital, en particular a través

⁵⁵ Discurso sobre el estado de la Unión 2021 – Reforzar el alma de nuestra Unión – 15 de septiembre de 2021.

⁵⁶ PE/28/2021/INIT.

⁵⁷ A cargo del PEDID.

de la contratación pública conjunta para desarrollar y gestionar los COS de la UE, incluidas herramientas e infraestructuras avanzadas, y de una convocatoria de subvenciones para apoyar las capacidades de los COS en los Estados miembros. Como paso siguiente, también podría considerarse la promoción de la cooperación civil y militar a escala nacional en este ámbito, junto con los Estados miembros.

Debe incrementarse el grado de cooperación en materia de ciberseguridad entre los Estados miembros en lo que respecta a la respuesta a incidentes, en particular mediante la posible cooperación entre los **equipos de respuesta civil y de defensa**. La unidad informática conjunta tiene por objeto reunir a todas las comunidades de ciberseguridad pertinentes (es decir, diplomáticas, civiles, policiales y de defensa) para garantizar una respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala, así como ofrecer asistencia para la recuperación cuando se hayan sufrido estos ataques. Por lo tanto, el ejército podría cooperar y coordinarse estructuralmente con otras comunidades de ciberseguridad a través de esta unidad.

El **desarrollo de cibercapacidades** a través de la formación y los ejercicios conjuntos es también fundamental para una resiliencia eficaz frente a los ciberataques, al mejorar las cibercapacidades, desarrollar una interpretación compartida y crear una capacidad de respuesta común. Si los Estados miembros así lo deciden, podrían considerar la posibilidad de reforzar la cooperación militar y civil en materia de ciberformación y ejercicios conjuntos, sobre la base de los programas de educación, de formación y de ejercicios de ciberseguridad de la Escuela Europea de Seguridad y Defensa y de la AED.

Camino a seguir

- A más tardar, en el tercer trimestre de 2022, la Comisión propondrá la **Ley de Ciberresiliencia**, cuyo objetivo será aumentar la ciberseguridad de los productos y servicios conexos en el mercado interior.
- Con el fin de crear las nuevas plataformas «COS UE» para compartir información y herramientas relacionadas con las ciberamenazas, la Comisión publicará, a más tardar en el segundo trimestre de 2022, una convocatoria de manifestaciones de interés para seleccionar las entidades anfitrionas de los COS de la UE, acompañada de una hoja de ruta específica. Esto debería allanar el camino para crear una capacidad estratégica de la UE que permita detectar e intercambiar información sobre las ciberamenazas.
- La Comisión trabajará con los Estados miembros para intensificar la preparación ante ciberincidentes a gran escala mediante una coordinación más estrecha, incluida la determinación de posibles necesidades y recursos para gestionar la respuesta.
- En 2022, se propondrá una agenda estratégica para el Centro de Competencia en Ciberseguridad que trate, en particular, las tecnologías de doble uso y las sinergias civiles y militares que deban establecerse de forma coordinada con los actores pertinentes.
- La Comisión, junto con el Alto Representante, seguirá ayudando a los Estados miembros a establecer la JCU, en particular su mecanismo de asistencia mutua, y alentará la cooperación civil y militar para facilitar el intercambio de información y la coordinación

entre expertos en defensa y otras comunidades (es decir, civiles, policiales y diplomáticas).

- La Comisión pedirá a las organizaciones europeas de normalización que elaboren normas armonizadas en apoyo del acto delegado recientemente adoptado relacionado con la Directiva sobre equipos radioeléctricos en lo que respecta a la ciberseguridad y la privacidad.
- La Comisión colaborará con el Alto Representante para seguir desarrollando la política de ciberdefensa de la UE, que se presentará a los Estados miembros, a más tardar, a finales de 2022.
- La Comisión invita a los Estados miembros a considerar cursos de formación y ejercicios conjuntos en materia de ciberdefensa, en cooperación con los marcos existentes de formación y ejercicios civiles y de defensa.

7.3. Reforzar la movilidad militar

A través de la aplicación del Plan de Acción sobre Movilidad Militar, la UE ya está dando pasos importantes para mejorar la movilidad del personal, el material y los equipos militares dentro y fuera de la UE, mejorando así nuestra capacidad de responder rápidamente a una crisis o con vistas a actividades ordinarias, como los ejercicios. La movilidad militar es también un proyecto emblemático en el marco de la cooperación UE-OTAN.

Con un **presupuesto de la UE para 2021-2027 de 1 690 millones EUR** para apoyar las infraestructuras de transporte de doble uso, la movilidad militar es un componente clave del nuevo Mecanismo «Conectar Europa» (MCE)⁵⁸. El programa de trabajo 2021-2023 contempla un presupuesto anual específico de 330 millones EUR, y las primeras convocatorias de propuestas se pusieron en marcha en septiembre de 2021.

La movilidad militar es también uno de los temas del programa de trabajo del FED para 2021. El desarrollo de un sistema digital para un intercambio seguro y rápido de información relacionada con la movilidad militar es uno de los dos temas de la convocatoria de propuestas sobre sistemas logísticos y de soldado, con un presupuesto indicativo de 50 millones EUR para toda la convocatoria.

El 14 de diciembre de 2021, la Comisión propuso revisar el Reglamento sobre la red transeuropea de transporte (RTE-T). Entre otras medidas, la propuesta tiene por objeto reforzar las normas para la movilidad civil y militar y ampliar los mapas de la RTE-T a fin de incluir nuevas rutas importantes para la movilidad militar.

⁵⁸ Reglamento (UE) 2021/1153 del Parlamento Europeo y del Consejo, de 7 de julio de 2021, por el que se establece el Mecanismo «Conectar Europa» y se derogan los Reglamentos (UE) n.º 1316/2013 y (UE) n.º 283/2014.

La Comisión proseguirá sus esfuerzos para contribuir a la movilidad militar dentro y fuera de la UE, en particular considerándola en las propuestas e iniciativas legislativas pertinentes, especialmente en el ámbito de los procedimientos transfronterizos y de transporte.

Camino a seguir

- A más tardar, a finales de 2022, la Comisión, junto con el Alto Representante, propondrá una actualización del Plan de Acción sobre Movilidad Militar conjunto, que podría abarcar las necesidades detectadas en relación con la digitalización del transporte, la ciberresiliencia de las infraestructuras de transporte y la inteligencia artificial.

7.4. Abordar los retos del cambio climático para la defensa

El cambio climático y la pérdida de biodiversidad plantean nuevas amenazas para la seguridad. Si bien la prioridad sigue siendo el mantenimiento de la eficacia operativa, el sector de la defensa debe hacer frente al reto de adaptarse a los efectos del cambio climático en la seguridad, incluida la capacidad de actuar en condiciones climáticas más extremas, así como de contribuir a la mitigación en el marco de las políticas de la UE en materia de cambio climático, en particular el Pacto Verde Europeo. La mejora de la eficiencia energética, el aumento del uso de energías renovables cuando sea posible y la reducción de las emisiones en este sector deben convertirse en parte integrante de nuestros esfuerzos colectivos para lograr la neutralidad climática de aquí a 2050, así como la protección de la biodiversidad y una economía circular reforzada.

Los sistemas circulares pueden ofrecer ventajas importantes a las industrias de defensa y la contratación pública, aumentando la eficiencia de los recursos, incrementando la autonomía estratégica abierta para determinados materiales críticos y prolongando y optimizando la utilidad de los equipos de defensa⁵⁹. Se determinarán y apoyarán las oportunidades de mejorar el diseño para el desmontaje, la recogida de componentes, la reparación, la renovación y la remanufactura de equipos de defensa. Esto también se aplica a las oportunidades de mejorar los equipos de defensa para que puedan seguir operando en condiciones medioambientales cada vez más duras en los teatros operativos.

En este contexto, la Comisión se ha comprometido a aplicar la hoja de ruta conjunta de la UE sobre cambio climático y defensa de 2020⁶⁰, sobre la que los servicios de la Comisión presentarán un primer informe anual de situación junto con el SEAE y la AED en el primer semestre de 2022. El programa de trabajo del FED para 2021⁶¹ ya señala temas relacionados con la gestión energética y la eficiencia energética. Se han destinado 133 millones EUR a una convocatoria específica para apoyar la investigación y el desarrollo de tecnologías y productos de defensa que abordan estos temas. A medida que avancen los trabajos en la misma dirección en

⁵⁹ [IF CEED \(europa.eu\)Circular defence - News & insight - Cambridge Judge Business School](https://www.europa.eu/press-room/en/ifa-ceed-circular-defence-news-insight)

⁶⁰ 12741/20

⁶¹ El Reglamento del FED establece que el «Fondo contribuye a integrar las acciones por el clima en las políticas de la Unión, así como a alcanzar el objetivo general de destinar el 30 % de los gastos del presupuesto de la Unión a apoyar los objetivos climáticos».

el seno de la OTAN y de las Naciones Unidas, y por parte de Estados Unidos y otros socios, la UE intensificará sus diálogos interservicios sobre el nexo entre seguridad climática y defensa.

Camino a seguir

- En el primer semestre de 2022, los servicios de la Comisión, el SEAE y la AED presentarán el primer informe de situación sobre la aplicación de la hoja de ruta sobre cambio climático y defensa.
- En 2022, la Comisión evaluará las iniciativas relacionadas con el clima y la defensa ejecutadas en el marco de los instrumentos existentes dirigidos por la Comisión (incluidos el FED, Horizonte Europa, Horizonte 2020, el MCE y LIFE) con el fin de mejorar las posibles sinergias.
- Para finales de 2022, la Comisión establecerá un marco político, basado en los aspectos relacionados con el clima y la defensa de los instrumentos dirigidos por la Comisión, para contribuir a reducir la demanda de energía y a aumentar la resiliencia energética de las tecnologías críticas utilizadas por los actores civiles de seguridad y las fuerzas armadas, y desarrollará soluciones concretas resistentes al cambio climático en este contexto.
- A lo largo de 2022, la Comisión estudiará el potencial de mejorar el impacto de las directivas relacionadas con la energía en las infraestructuras militares (como oficinas, sedes, cuarteles, hospitales y academias), incluidas las opciones de contratación pública ecológica, como parte del Pacto Verde Europeo (es decir, la nueva acción de eficiencia energética «Oleada de renovación», la revisión de la Directiva de eficiencia energética y la Directiva relativa a la eficiencia energética de los edificios).
- A lo largo de 2022, la Comisión y el Alto Representante aumentarán e intensificarán los trabajos interservicios sobre el nexo entre seguridad climática y defensa con la OTAN, las Naciones Unidas y los socios bilaterales pertinentes, como Estados Unidos y Canadá.

8. Conclusiones

En un mundo más complejo, controvertido, competitivo y conectado que nunca, la UE debe redoblar sus esfuerzos para defender sus intereses y valores estratégicos. La próxima Brújula Estratégica de la UE sobre seguridad y defensa establecerá objetivos ambiciosos para la seguridad y la defensa de Europa a largo plazo, objetivos a los que contribuye activamente la presente Comunicación.

A tal fin, la Comisión ha señalado, en particular, los siguientes nuevos ámbitos donde seguir reforzando la competitividad del mercado de la defensa europeo:

- **estudiar la manera de estimular en mayor medida las inversiones de los Estados miembros en capacidades estratégicas clave y «catalizadores» críticos** que se desarrollen o se adquieran dentro de marcos de cooperación de la UE;

- **incentivar en mayor medida la adquisición conjunta de capacidades de defensa desarrolladas de manera colaborativa dentro de la UE**, en particular mediante una exención del IVA y un posible refuerzo de las bonificaciones del FED;
- **apelar a los Estados miembros para que continúen avanzando hacia prácticas de control de las exportaciones de armamento racionalizadas y más convergentes**, en particular, por lo que se refiere a las capacidades de defensa desarrolladas en un marco cooperativo de la UE.

La Comisión también aplicará las iniciativas ya puestas en marcha que son catalizadores clave para la defensa europea, como el **FED y la movilidad militar**, así como las que son esenciales para reforzar la resiliencia europea, en particular en el espacio, para luchar contra las amenazas híbridas, para reforzar la ciberseguridad y para abordar los retos del cambio climático relacionados con la defensa.

La Comisión sigue dispuesta a considerar medidas adicionales a la luz de los progresos realizados y de la evolución de las amenazas y los retos que la Unión afronte en el futuro.