Consejo de la Unión Europea

Bruselas, 17 de febrero de 2022
(OR. en)

6316/22

LIMITE

COPS 68	PROCIV 16
POLMIL 33	ESPACE 11
EUMC 50	POLMAR 17
CIVCOM 21	MARE 17
CFSP/PESC 171	COMAR 15
CSDP/PSDC 70	COMPET 97
RELEX 196	IND 41
JAI 202	RECH 89
HYBRID 15	COTER 44
DISINFO 11	POLGEN 21
CYBER 53	

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2022) 61 final
Asunto:	COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES Hoja de ruta sobre tecnologías críticas para la seguridad y la defensa

Adjunto se remite a las Delegaciones el documento – COM(2022) 61 final.

Adj.: COM(2022) 61 final

COMISIÓN
EUROPEA

Estrasburgo, 15.2.2022
COM(2022) 61 final

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

Hoja de ruta sobre tecnologías críticas para la seguridad y la defensa

1. Introducción

Mantenerse a la vanguardia del desarrollo tecnológico es fundamental para garantizar la prosperidad, la seguridad y el modo de vida de Europa. Las nuevas tecnologías están transformando los sectores de la seguridad y la defensa a un ritmo más rápido que nunca y difuminando la línea divisoria entre el ámbito civil y el militar. En especial, las tecnologías digitales están afectando a los equilibrios de poder establecidos en el panorama de seguridad mundial. Por esta razón, es indispensable garantizar que los sectores de la seguridad y la defensa de Europa siguen siendo adecuados desde el punto de vista tecnológico.

Muchas de las tecnologías críticas para la seguridad y la defensa tienen cada vez más su origen en el ámbito civil y utilizan componentes críticos de doble uso. Para acelerar la innovación en todos los ámbitos, y fomentar la soberanía tecnológica en los sectores de la seguridad y la defensa, es necesario mejorar el intercambio entre las comunidades de investigación e innovación civiles y de defensa. La UE, con su larga experiencia en desarrollo tecnológico civil y sus nuevos instrumentos de cooperación en materia de defensa[1], está en condiciones de asumir un papel de liderazgo. Sin embargo, esto requerirá un uso más eficiente de los recursos y una voluntad de explorar las posibilidades que brinda el doble uso, respetando al mismo tiempo los valores fundamentales de la UE. También significa reducir las dependencias estratégicas y las vulnerabilidades de las cadenas de valor y suministro asociadas a estas tecnologías.

La fragmentación de las capacidades de seguridad y defensa de Europa ha dado lugar a ineficiencias económicas, reducido la capacidad operativa y provocado un aumento de las dependencias estratégicas. La profunda transformación en curso de las tecnologías de seguridad y defensa y los nuevos instrumentos de cooperación de la UE en materia de defensa brindan a la UE la oportunidad de evitar los errores del pasado, aprovechar sus capacidades existentes y preservar su prosperidad económica y su seguridad. **El futuro panorama tecnológico y de innovación en materia de seguridad y defensa en Europa debe desarrollarse desde el principio en marcos de cooperación de la UE.**

En su discurso sobre el estado de la Unión de 2021[2], la presidenta Von der Leyen reconoció que, si bien se habían iniciado los trabajos para desarrollar un ecosistema europeo de defensa, era necesaria una Unión Europea de la Defensa. La Brújula Estratégica sobre seguridad y defensa de la UE («Brújula Estratégica»), que los Estados miembros adoptarán en marzo de 2022, establecerá una visión estratégica común para la próxima década y definirá de qué manera la UE mejorará su capacidad para actuar y responder a los distintos desafíos y crisis; protegerá sus intereses y a sus ciudadanos; investirá e innovará para desarrollar conjuntamente las capacidades y tecnologías necesarias; y profundizará las asociaciones basadas en los valores e intereses de la UE.

---

[1] El Fondo Europeo de Defensa (FED), la revisión anual coordinada de la defensa (CARD) y la Cooperación Estructurada Permanente (CEP).

[2] Discurso sobre el estado de la Unión de 2021 pronunciado por la presidenta de la Comisión Von der Leyen.

Esta hoja de ruta sobre tecnologías críticas para la seguridad y la defensa responde a una petición del Consejo Europeo de 25 y 26 de febrero de 2021[3], en la que se solicitaba esbozar un camino para impulsar la investigación, el desarrollo tecnológico y la innovación (IDT+I) y reducir las dependencias estratégicas de la UE en tecnologías críticas y cadenas de valor para la seguridad y la defensa. La hoja de ruta se presentará en la cumbre informal de París los días 10 y 11 de marzo de 2022 y se incorporará a la Brújula Estratégica. Propone un itinerario a seguir para que la UE y los Estados miembros alcancen conjuntamente el objetivo antes mencionado, en particular mediante:

- la identificación de tecnologías esenciales para la seguridad y la defensa de la UE, y su promoción a través de los programas europeos (IDT+I);
- una mejor integración de las consideraciones de defensa en los programas europeos civiles de IDT+I y en las políticas industriales y comerciales, según proceda, mientras que los posibles usos civiles de las tecnologías también se tendrán más en cuenta en los programas de IDT+I en el ámbito de la defensa;
- la promoción desde el principio de un enfoque estratégico y coordinado a escala de la UE para las tecnologías críticas de seguridad y defensa, para hacer el mejor uso posible de los programas de IDT+I de la UE y de los Estados miembros, lograr sinergias entre las comunidades de IDT+I civiles y de la defensa y mitigar las dependencias estratégicas de fuentes externas; así como
- la coordinación, en la mayor medida posible, con otros socios afines, como los Estados Unidos y la Organización del Tratado del Atlántico Norte (OTAN), en condiciones mutuamente beneficiosas.

2. Tecnologías críticas y dependencias estratégicas para la seguridad y la defensa

La actualización del «Nuevo modelo de industria de 2020: Creación de un mercado único más sólido para la recuperación de Europa» («estrategia industrial actualizada»)[4] de mayo de 2021 confirma que el liderazgo tecnológico sigue siendo un motor esencial de la competitividad y la innovación de la UE, en particular para las denominadas «tecnologías críticas»[5]. También subraya la importancia de identificar y mitigar las dependencias estratégicas en los «ecosistemas sensibles», incluidos los de la «economía de proximidad y social y seguridad civil» y de la «industria aeroespacial y defensa», a fin de garantizar la resiliencia de la UE.

El plan de acción de la Comisión sobre las sinergias entre las industrias civil, de la defensa y espacial («plan de acción de sinergias»)[6], de febrero de 2021, reconoce la creciente importancia de las tecnologías disruptivas y facilitadoras originadas en el ámbito civil para la seguridad y la defensa futuras de Europa, y la necesidad de promover el enriquecimiento mutuo y las sinergias

---

3 Declaración de los miembros del Consejo Europeo, de 26 de febrero de 2021.

4 COM(2021) 350 final.

5 La Comisión, en el contexto de su trabajo sobre el Observatorio de Tecnologías Críticas, está consensuando una definición de «criticidad» para los ámbitos del espacio, la defensa y los sectores civiles conexos (incluida la seguridad).

6 COM(2021) 70 final.

entre las tecnologías civiles y de defensa. En él se exponen varias acciones clave para fomentar el intercambio de información y la cooperación entre las comunidades civiles y de defensa utilizando como punto de partida los programas e instrumentos de IDT+I de la UE.

2.1. Características específicas de los sectores de la seguridad y la defensa

La industria de la defensa de la UE tiene una estructura diversificada, que incluye tanto grandes multinacionales como actores de pequeño a mediano tamaño. La demanda procede casi exclusivamente de los gobiernos nacionales, quienes también controlan toda adquisición y exportación de productos y tecnologías relacionados con la defensa. Los diferentes requisitos nacionales y el gasto y la inversión públicos nacionales siguen fragmentando el mercado de la defensa de la UE, a veces amenazando con obstaculizar la interoperabilidad entre las fuerzas armadas nacionales de los Estados miembros. Por lo tanto, el sector de la defensa no sigue las normas y los modelos de negocio convencionales que rigen los mercados más tradicionales, por lo que tiene un margen limitado para influir en las inversiones conexas y las opciones de mercado. Por esta razón, la industria tiene dificultades para realizar importantes proyectos de IDT+I de defensa autofinanciados.

La industria de la seguridad de la UE se enfrenta a retos similares, ya que los mercados también son predominantemente nacionales, y están incluso más fragmentados. El abanico de clientes es variado (por ejemplo, fuerzas policiales, agencias de seguridad interior, agencias aduaneras, autoridades fronterizas, servicios de seguridad privada), las actividades se desarrollan a distintos niveles (local, regional, nacional), y la organización varía de un Estado miembro a otro. **La Comisión presentará en 2022 un estudio sobre el mercado de la seguridad de la UE que ofrecerá más información acerca de este complejo sector**. Además, en el primer semestre de 2022 los servicios de la Comisión harán un resumen de todas las propuestas existentes que buscan fomentar la adopción de enfoques orientados a las capacidades que puedan aplicarse a todos los sectores de la seguridad. Estas propuestas reforzarán la identificación temprana y prospectiva de las necesidades y soluciones para la seguridad y la aplicación de la ley.

El espacio y la ciberseguridad son «facilitadores» estratégicos para los sectores de la seguridad y la defensa. El sector espacial comparte muchas de sus características específicas, con reducidos volúmenes de mercado y una influencia limitada en el mercado privado de componentes. La resiliencia de los programas espaciales y de las cadenas de valor en el ámbito espacial es fundamental para los objetivos de seguridad y defensa de la UE. La ciberseguridad también desempeña un papel cada vez más importante en todas las capacidades de defensa, y requiere atención e inversión. El rápido aumento de los ciberataques dirigidos tanto a activos y redes civiles como de defensa y el papel cada vez más importante del sector civil en la ciberinnovación y la normalización requieren el establecimiento de vínculos más estrechos entre la ciberseguridad y la ciberdefensa. La contribución de la Comisión a la defensa europea en el contexto de la Brújula Estratégica («comunicación sobre defensa»), que forma parte de este paquete de defensa, esboza nuevas medidas para estos dos sectores.

2.2. Cartografía de tecnologías críticas y dependencias estratégicas para la seguridad y la defensa

La estrategia industrial actualizada ofrece una cartografía y un análisis amplios de las dependencias y capacidades estratégicas de la UE, sobre la base de una primera ronda de exámenes exhaustivos de los ecosistemas sensibles[7]. Si bien este trabajo ha proporcionado una base para la acción política en apoyo de una mejor resiliencia de la UE, también reconoce que es necesario seguir trabajando para mejorar nuestra comprensión de las dependencias estratégicas de la UE y de cómo pueden evolucionar para dar lugar a nuevas vulnerabilidades. Este proceso incluye una segunda ronda de exámenes exhaustivos de ecosistemas sensibles y un sistema de seguimiento a través del Observatorio de Tecnologías Críticas («el Observatorio») (véase la sección 2.3.).

Los servicios de la Comisión han empezado a trabajar en revisiones exhaustivas de los ámbitos de las tecnologías de seguridad y defensa, incluida la ciberseguridad, para apoyar la estrategia industrial actualizada y el desarrollo del Observatorio. Ya se han llevado a cabo dos estudios de casos preliminares sobre los sistemas autónomos y los semiconductores de las tecnologías de defensa, que se consideran representativos debido a su importancia transversal para las capacidades militares en distintos ámbitos (véase el recuadro 1). El objetivo era identificar patrones comunes entre estos ámbitos tecnológicos de defensa, sobre todo en lo que se refiere a las causas de las dependencias y los riesgos asociados, así como posibilidades tempranas para mitigarlos.

Los estudios de casos confirman que el sector de la defensa comparte en líneas generales las mismas dependencias y vulnerabilidades estratégicas que otros ecosistemas sensibles, especialmente en lo que se refiere a las lagunas tecnológicas, las materias primas (críticas), las capacidades, la baja inversión en IDT+I y las normativas extraterritoriales de países no pertenecientes a la UE. También revelan que las vulnerabilidades del sector se ven agravadas por el carácter estratégico y sensible de sus actividades (por ejemplo, los niveles más elevados de seguridad de la información y de seguridad del suministro) y su tamaño comparativamente marginal en el mercado.

Los estudios de casos muestran además que algunos de los competidores mundiales de la UE adoptan más medidas ofensivas y defensivas para promover las tecnologías críticas y abordar las dependencias estratégicas de lo que ha hecho hasta ahora la UE. Por ejemplo, vinculan de forma más sistemática las consideraciones de defensa nacional al desarrollo tecnológico civil, invierten intensamente en su capacidad industrial y de IDT+I autóctonas, atraen a inversores externos y, en algunas ocasiones, despliegan estrategias agresivas de adquisición en terceros países. Por otra parte, también protegen sus propios conocimientos e influencia aprovechando las interdependencias o utilizando reglamentaciones extraterritoriales estrictas para limitar el acceso de terceros países a las tecnologías.

A pesar de que la UE dispone de instrumentos propios para reforzar su capacidad industrial de conformidad con las normas de la UE, se ve obstaculizada por una demanda del mercado de defensa que sigue estando muy fragmentada, su histórica estricta separación entre la IDT+I civil y de defensa a nivel de la UE, y una infrainversión comparativa de los Estados miembros en la

[7] SWD(2021) 352 final.

base industrial y tecnológica de la defensa europea (BITDE). De hecho, el gasto colectivo de los Estados miembros en innovación en materia de defensa (2 500 millones EUR, es decir, el 1,2 % del gasto en defensa) sigue estando por debajo del objetivo del 2 % de la AED, que data de quince años atrás.

Si bien las fuerzas del mercado han llevado a una situación en la que ningún país puede alcanzar la plena soberanía tecnológica en ningún ámbito tecnológico, existe una carrera a nivel mundial para alcanzar el liderazgo tecnológico y hacerse con las ventajas económicas y militares asociadas. Si no se toman medidas, esta situación podría exacerbar las actuales dependencias estratégicas de la UE y generar otras nuevas. Es necesario un enfoque estructurado para que la UE se mantenga en la vanguardia de las tecnologías críticas, e identifique y mitigue las dependencias estratégicas en el ámbito de la seguridad y la defensa. Esta hoja de ruta tiene por objeto proporcionar un enfoque de este tipo, que se integrará en la Brújula Estratégica de la UE.

Recuadro 1: Estudio de casos — Sistemas autónomos y semiconductores para la defensa

El análisis de la Comisión sobre los sistemas autónomos de defensa, que presta especial atención a la inteligencia artificial (IA) y el aprendizaje automático, ha identificado las tecnologías críticas necesarias y cuatro ámbitos principales en los que la UE está a la zaga, a saber: capacidades, datos, *hardware* y ensayos. Las posibles medidas para abordar estos ámbitos se basarían en la actual estrategia de la UE en materia de IA[8] y en las iniciativas políticas conexas, así como en las estrategias nacionales de IA de los Estados miembros. Entre ellas encontramos actividades de IDT+I (por ejemplo, mayor disponibilidad de datos y formación en IA, vínculo con la iniciativa europea en materia de procesadores), infraestructuras (por ejemplo, capacidad de computación en la nube para fines de defensa, instalaciones de ensayo nacionales) y protección de los activos existentes (por ejemplo, el control de la inversión extranjera directa).

El análisis sobre los semiconductores para la defensa puso de relieve la omnipresencia de los semiconductores en los equipos de defensa y las dependencias existentes y futuras, causadas, en particular, por la falta de capacidades autóctonas de la UE (fundiciones) para los nodos más avanzados. En la propuesta de Ley Europea de Chips, adoptada el 8 de febrero de 2022[9], la Comisión ha incluido medidas de mitigación con el objetivo de crear un ecosistema europeo de chips de vanguardia para mejorar las capacidades de la UE en este ámbito, abordando así también las necesidades de defensa.

2.3. Observatorio de Tecnologías Críticas

La falta de previsión sobre la importancia futura de las tecnologías es en parte responsable de algunas de las actuales dependencias estratégicas de la UE con respecto a terceros países (por ejemplo, para los sistemas pilotados a distancia o los semiconductores). La UE necesita una visión más estructurada y una reflexión estratégica acerca de las tecnologías críticas para la seguridad y la defensa, con el fin de identificar los ámbitos prioritarios en los que impulsar la

[8] COM(2018) 237 final.
[9] COM(2022) 45 final.

investigación y la innovación, y reducir las dependencias estratégicas existentes y evitar la aparición de otras nuevas.

El Observatorio de Tecnologías Críticas, que la Comisión está creando en consonancia con el Plan de acción sobre las sinergias (acción 4), contribuirá a esta reflexión. En su metodología de trabajo tendrá en cuenta otras iniciativas similares[10] para evitar duplicaciones. De esta forma se conseguirá afinar la lista de tecnologías críticas del plan de acción de sinergias para reflejar la evolución del panorama tecnológico y las necesidades de capacidades.

El Observatorio identificará, supervisará y evaluará las tecnologías críticas para los sectores espacial, de la defensa y civiles relacionados, su aplicación potencial y las cadenas de valor y suministro conexas. También identificará, supervisará y analizará las lagunas tecnológicas existentes y previsibles, las causas profundas de las dependencias estratégicas y las vulnerabilidades.

Será esencial acordar con los Estados miembros un nivel significativo de detalle para debatir estas cuestiones a escala de la UE, y convenir en la necesidad de compartir los datos pertinentes entre los Estados miembros y con la Comisión. Se creará un mecanismo en el seno del Observatorio, en forma de grupo de expertos específico, para intercambiar y debatir con los Estados miembros en un entorno reservado. Se debatirá sobre la aparición de tecnologías nuevas y disruptivas para evitar nuevas dependencias para las industrias de la seguridad, la defensa y espacial. El Alto Representante y sus servicios estarán asociados a este proceso.

La Comisión, sobre la base de los datos del Observatorio, presentará a los Estados miembros un informe clasificado sobre las tecnologías críticas y los riesgos asociados a las dependencias estratégicas que afecten a la seguridad, el espacio y la defensa a finales de 2022 y, posteriormente, cada dos años. A partir de estos informes, elaborará hojas de ruta tecnológicas que incluirán medidas de mitigación para impulsar la IDT+I y reducir las dependencias estratégicas que afectan a la seguridad y la defensa.

Una vez que las actividades del Observatorio estén bien establecidas, el alcance de su trabajo podría ampliarse a otras industrias, como se indica en la estrategia industrial actualizada.

Camino a seguir:

- En 2022, la Comisión creará un grupo de expertos para facilitar el diálogo entre los Estados miembros sobre tecnologías críticas y cadenas de valor y de suministro. Formará parte del Observatorio de Tecnologías Críticas para la defensa, el espacio y las industrias civiles conexas. El objetivo sería:
  - consultar de forma periódica a las autoridades de los Estados miembros para preparar el informe clasificado;
  - garantizar un tratamiento adecuado de la información sensible y clasificada que pueda intercambiarse en el contexto del Observatorio relativa a las tecnologías críticas, informes

[10] Por ejemplo, el apoyo y las herramientas del proyecto sobre tecnologías avanzadas para la industria («ATI», por sus siglas en inglés), el seguimiento de tecnologías críticas para el espacio, el Programa Estratégico General de Investigación («OSRA», por sus siglas en inglés), los componentes tecnológicos conexos y las actividades estratégicas clave de la Agencia Europea de Defensa (AED).

conexos y hojas de ruta.

- A mediados de 2022, la Comisión presentará un estudio sobre el mercado de la seguridad de la UE, que servirá para comprender mejor las características específicas del mercado de la seguridad civil, para permitir la identificación de tecnologías críticas y dependencias estratégicas, y para respaldar el nuevo enfoque basado en las capacidades para la seguridad y otras actividades de IDT+I.
- A mediados de 2022, los servicios de la Comisión elaborarán un documento en el que se resumirán las propuestas para fomentar la adopción de enfoques basados en las capacidades que se aplicarán a todos los sectores de la seguridad.

3. Impulsar la IDT+I en tecnologías críticas para la seguridad y la defensa

Las hojas de ruta tecnológicas que preparará la Comisión sobre la base de las evaluaciones del Observatorio respaldarán toda una serie de actividades, desde la programación de IDT+I sobre tecnologías críticas hasta el desarrollo de iniciativas emblemáticas que contribuyan a reforzar la competitividad y la resiliencia de la UE en los sectores de la seguridad y la defensa. Para alcanzar estos objetivos, será necesario hacer un uso más eficiente de los recursos financieros disponibles a través de una mejor coordinación de los programas e instrumentos de IDT+I existentes a escala nacional y de la UE.

3.1. Superar la separación entre la IDT+I civil y de defensa de la UE

En el marco de su Plan de acción sobre las sinergias (acción 2), la Comisión se comprometió a mejorar, para 2022, la coordinación interna entre los programas e instrumentos de la UE (véase el recuadro 2), con el fin de liberar los enormes beneficios derivados de las sinergias entre la IDT+I civil y de defensa para el crecimiento económico, el mercado único y la seguridad de los ciudadanos europeos.

Si bien la ejecución de este objetivo también puede llevarse a cabo en 2023 (por ejemplo, mediante la mejora de la planificación y la sincronización, la orientación a las autoridades de gestión de los Estados miembros, etc.), algunos obstáculos serán más difíciles de abordar a corto y medio plazo y podría ser necesaria la participación de otras partes interesadas. Este es el caso, en particular, cuando las disposiciones legales de los actos de base de los programas e instrumentos de la UE establecen limitaciones prácticas. Por ejemplo, si bien las actividades de doble uso pueden financiarse con cargo al Mecanismo «Conectar Europa» (MCE) y a los Fondos Estructurales y de Inversión Europeos (Fondos EIE), las actividades realizadas en el marco de Horizonte Europa[11] se centran en aplicaciones civiles, y no existe un marco para el apoyo directo a estas actividades en los programas e instrumentos de IDT+I. Del mismo modo, la política de préstamos del Banco Europeo de Inversiones sigue imponiendo restricciones al sector de la defensa.

[11] El término «Horizonte Europa» en el presente documento hace referencia al programa específico por el que se ejecuta Horizonte Europa y el Instituto Europeo de Innovación y Tecnología, cuyas actividades se centran exclusivamente en las aplicaciones civiles.

Para facilitar los intercambios entre las comunidades civiles y de defensa, en particular en el ámbito de las tecnologías críticas, la Comisión preparará en 2023 un enfoque para fomentar que la IDT+I de doble uso a escala de la UE se aplique plenamente a medio y largo plazo en todos los programas e instrumentos de la UE. Este trabajo también se tendrá en cuenta en la evaluación intermedia de los programas sectoriales pertinentes, como los fondos en virtud del Reglamento sobre disposiciones comunes, incluidos los fondos para la preparación ante emergencias sanitarias.

Recuadro 2: Programas e instrumentos de la UE de apoyo a la IDT+I en tecnologías críticas pertinentes para la seguridad y la defensa y su despliegue de infraestructuras en el marco del Programa Financiero Plurianual (2021-2027)

- El FED dedica 8 000 millones EUR a la investigación y el desarrollo en materia de defensa. Entre el 4 y el 8 % del presupuesto de investigación y desarrollo del FED, es decir, hasta 100 millones EUR al año, se asignará a tecnologías disruptivas.
- Horizonte Europa, en el marco del pilar II «Desafíos mundiales y competitividad industrial europea», asigna 1 600 millones EUR a la investigación y la innovación en materia de seguridad civil en el marco del clúster «Seguridad civil para la sociedad», mientras que las tecnologías críticas reciben apoyo en el marco de los clústeres «Mundo digital, industria y espacio», «Clima, energía y movilidad» y «Alimentación, bioeconomía, recursos naturales, agricultura y medio ambiente». Las actividades complementarias se financian en el marco del pilar I «Ciencia excelente»; el Consejo Europeo de Innovación (CEI) y el Instituto Europeo de Innovación y Tecnología (EIT), en el marco del pilar III «Europa innovadora», así como las asociaciones europeas, que ponen en común y movilizan recursos para garantizar el liderazgo tecnológico de la UE y la autonomía estratégica abierta en ámbitos críticos.
- El programa Europa Digital fomentará las actividades de despliegue pertinentes para las tecnologías críticas en los ámbitos prioritarios de la ciberseguridad, la inteligencia artificial y la supercomputación.
- En 2022, el Centro de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros de Coordinación adoptarán una agenda estratégica sobre inversiones en ciberseguridad que alimentará Horizonte Europa y el programa Europa Digital. Podrán explorarse sinergias entre las tecnologías civiles y de defensa y las aplicaciones de doble uso a través de vínculos con el FED de conformidad con las normas aplicables.
- Los Fondos EIE (en particular el Fondo Europeo de Desarrollo Regional y el Fondo Social Europeo Plus) pueden utilizarse en apoyo de la BITDE.
- Otros programas, fondos e instrumentos pertinentes de la UE son el Programa Espacial, el MCE, el Programa InvestEU, el Mecanismo de Recuperación y Resiliencia (MRR), el Programa LIFE, las asociaciones público-privadas y los mecanismos de financiación combinada.

3.2. Vincular los programas e instrumentos nacionales y de la UE en apoyo de la IDT+I en las tecnologías críticas para la seguridad y la defensa

Aunque los programas e instrumentos de la UE proporcionan una financiación significativa a las actividades de IDT+I en materia de seguridad y defensa en la UE, la mayor parte de la

financiación para estas actividades sigue correspondiendo a los Estados miembros, y la fragmentación de los mercados de seguridad y defensa sigue siendo un problema grave. En consecuencia, para lograr la soberanía tecnológica en algunos ámbitos tecnológicos críticos y, en otros, la mitigación de las dependencias, será necesaria una coordinación a escala de la UE.

Se invita a los Estados miembros a comprometerse en la Brújula Estratégica a desarrollar, junto con la Comisión, un enfoque estratégico coordinado a escala de la UE para las tecnologías críticas pertinentes para la seguridad y la defensa desde el principio, respetando plenamente la variedad y complejidad de la gobernanza de los programas e instrumentos nacionales y de la UE. Este enfoque también tendría en cuenta otras estructuras de coordinación, como el nuevo Centro de Innovación de la UE en Seguridad Interior, presidido por el Comité Permanente de Cooperación Operativa en materia de Seguridad Interior (COSI), y el nuevo Centro de Innovación de la UE para la Defensa que creará la AED.

Se utilizarían los informes clasificados sobre tecnologías críticas y las hojas de ruta tecnológicas elaboradas por la Comisión como punto de partida para los debates entre las autoridades de los Estados miembros y la Comisión. El objetivo sería identificar, sobre la base de las hojas de ruta tecnológicas, los ámbitos que requieren la acción más urgente y, sucesivamente, movilizar los programas, instrumentos y políticas de la UE y de los Estados miembros para abordarlos de manera coordinada, de conformidad con las normas de la UE sobre ayudas estatales. De esta forma se garantizaría la concentración de las inversiones en los ámbitos más importantes para la seguridad de los ciudadanos de la UE. Las prioridades se actualizarían periódicamente para asegurarse de que siguen siendo pertinentes y que el gasto es eficiente.

La Comisión trabajará con los Estados miembros para determinar la mejor forma de facilitar este trabajo de coordinación (por ejemplo, a través del grupo de expertos del Observatorio).

3.3. Apoyo a la innovación y la iniciativa empresarial en materia de seguridad y defensa — Creación de un plan de innovación de la UE en materia de defensa

La UE debe aprovechar mejor todo el potencial de su comunidad de innovación en apoyo de la seguridad y la defensa. Para conseguirlo, será necesario brindar apoyo a los agentes no tradicionales, a las empresas emergentes y a las pequeñas y medianas empresas (pymes) innovadoras existentes en los dos sectores, para que superen los elevados obstáculos tecnológicos, administrativos, reglamentarios y de entrada en el mercado, cumplan las estrictas normas de seguridad y accedan a la financiación. A menudo, el mercado de la defensa se estructura en torno a un pequeño número de grandes operadores apoyados por un conjunto de pymes especializadas que tienen un acceso directo limitado a este mercado. Por esta razón, puede resultar difícil para las pymes innovadoras en el ámbito de la defensa acceder a la financiación, por lo que puede que sean más propensas a recurrir a inversores extranjeros, o ser objeto del interés de estos últimos. Lo mismo ocurre con las pymes innovadoras en el ámbito de la

seguridad, que se enfrentan a retos similares a la hora de contactar con posibles clientes o acceder a financiación adaptada[12].

La Comisión ha estado apoyando a las empresas emergentes y a las pymes innovadoras en el ámbito de la seguridad en el marco de Horizonte 2020, donde la financiación asignada y los índices globales de éxito en el marco del desafío social 7 «Seguridad civil para la sociedad» han sido superiores a la media de los pequeños innovadores. Si bien este apoyo continuará en el marco de Horizonte Europa, estas pymes y empresas emergentes seguirán necesitando un apoyo adaptado adicional para acelerar su camino hacia el mercado. Explorar nuevos instrumentos para la innovación de doble uso podría impulsar su capacidad de producción, competitividad y sostenibilidad.

La Comisión ha empezado a poner en marcha actividades similares en el marco del FED para desarrollar un conjunto de herramientas para la innovación en materia de defensa y doble uso, que abarque los niveles de madurez tecnológica[13] 1 a 9. Se está trabajando en los siguientes instrumentos que abarcan la defensa, las nuevas tecnologías y el doble uso:

a) *Innovación en materia de defensa a través del FED*: se están sopesando acciones específicas para apoyar mejor los proyectos sobre tecnologías disruptivas y soluciones de defensa innovadoras y orientadas al futuro, fomentando en particular la participación de pymes y laboratorios innovadores y las organizaciones de investigación y tecnología. Estas acciones pueden adoptar diversas formas, como, por ejemplo, asesoramiento empresarial (programa de trabajo 2021), desafíos tecnológicos (2022), hackatones o premios (2023 o sucesivos). También se basarán en la experiencia pertinente del Consejo Europeo de Innovación y podrán vincularse al nuevo CASSINI para la defensa.

b) *Un mecanismo de inversión combinada en defensa en el marco de InvestEU*: la creación de dicho mecanismo permitiría a la Comisión garantizar las inversiones realizadas por intermediarios financieros en toda la UE a favor de pymes innovadoras o de defensa estratégica. Esto aliviaría los problemas relacionados con el acceso limitado a la financiación de las pymes que desarrollan tecnologías prometedoras para la defensa europea, proporcionando al mismo tiempo capital de confianza y evitando adquisiciones hostiles por parte de entidades de terceros países. Permitir un mejor acceso a la financiación para las pymes y empresas de mediana capitalización innovadoras en el ámbito de la defensa respaldaría su crecimiento y, en último término, beneficiaría a la capacidad de innovación de la BITDE. La Comisión también estudiará la necesidad de nuevos instrumentos de apoyo a los principales agentes del mercado en la cadena de valor.

[12] Retos y oportunidades para las pymes y las empresas emergentes en I+i en materia de seguridad de la UE, CERIS, evento virtual en el marco del grupo temático «Refuerzo de la investigación e innovación en materia de seguridad», 30 de abril de 2021.

[13] Desde 2014, la UE ha adoptado de forma generalizada el uso de la escala de nivel de madurez tecnológica en el marco de los programas e instrumentos de IDT+I. La escala distingue nueve niveles de madurez tecnológica, que van desde la investigación fundamental con arreglo al nivel 1, hasta un producto final listo para entrar en el mercado en el nivel 9. Ya que la aplicación y, por tanto, el potencial de doble uso de una tecnología habitualmente se descubre en los niveles 5 o 6, se considera que en los niveles de 1 a 4 la tecnología es «neutra».

c) *CASSINI para la defensa*: esta iniciativa se inspiraría en la iniciativa CASSINI existente para apoyar a las pymes y a las empresas emergentes de la industria espacial. Les prestaría servicios como: desarrollo empresarial y redes (por ejemplo, establecimiento de contactos, aceleración empresarial), premios y concursos (incluidos hackatones, tutoría, etc.), que complementen el mecanismo de inversión combinada antes mencionado.

d) *Incubadora de innovación*: la Comisión creará en 2022 una incubadora de innovación para apoyar el desarrollo de nuevas tecnologías y dar forma a la innovación de doble uso en consonancia con el Plan de acción sobre las sinergias (acción 6), que podría desempeñar un papel importante a la hora de salvar la brecha entre los programas de IDT+I civil y los centrados en la defensa. Tras un análisis sistemático de los resultados de las fases iniciales de desarrollo tecnológico, la incubadora señalaría proyectos o tecnologías que ofrezcan posibles aplicaciones de seguridad, espaciales o de defensa para los servicios pertinentes de la Comisión y los Estados miembros, para su posible adopción. La Comisión evaluaría cómo podrían orientarse estos proyectos señalados hacia nuevas oportunidades de financiación, cuando proceda, como el régimen de financiación de transición del CEI o el FED.

e) *Apoyo a las redes de innovación*: las redes transfronterizas de innovación en materia de defensa podrían desempeñar el papel de intermediarios de la innovación y fomentar proyectos colaborativos para incorporar soluciones innovadoras. La búsqueda de tecnologías detectaría e identificaría soluciones y tecnologías nuevas e innovadoras con beneficios potenciales para las aplicaciones de defensa. A continuación, los centros de investigación y las instalaciones técnicas de ensayo comprobarían la pertinencia de estas tecnologías del ámbito civil e intercambiarían las mejores prácticas. La AED sería un socio clave de la Comisión para la ejecución de otra parte de la acción 6 en el marco del Plan de acción sobre las sinergias.

La Comisión determinará cómo vincular el conjunto de herramientas a los instrumentos de apoyo a la innovación en los ámbitos de la seguridad (por ejemplo, Horizonte Europa) o la ciberseguridad (por ejemplo, la red de centros nacionales de coordinación de la ciberseguridad en cooperación con los centros europeos de innovación digital).

Los puntos fuertes complementarios de la Comisión y de la EAD deben reunirse en un **«Plan de Innovación para la Defensa de la UE»**. En el marco de este plan, la Comisión, sobre la base de su experiencia en la ejecución del presupuesto de la UE en apoyo de la IDT+I en el ámbito civil, de la defensa y del doble uso, desempeñará un papel central en el fomento de la innovación para la BITDE. Habida cuenta de sus conocimientos especializados en materia de defensa, también a la hora de articular las tecnologías emergentes y disruptivas con los requisitos de capacidad militar, la EAD seguirá conectando y apoyando los esfuerzos de los Estados miembros a través de su Centro de Innovación en materia de Defensa. Gracias a esta estrecha cooperación, la Comisión y la AED acelerarán en sinergia la innovación en los ámbitos de la seguridad y la defensa a favor de la UE y de los Estados miembros.

3.4. Capacidades

La falta de cualificaciones y la escasez de mano de obra, especialmente de trabajadores cualificados con experiencia en ciencia, tecnología, ingeniería y matemáticas, son retos

importantes para la industria de la defensa y de la seguridad, que dependen en gran medida de ellos como muchas otras industrias de alta tecnología. Dado que las tecnologías y el panorama de amenazas evolucionan rápidamente, es importante que la industria tienda más la mano a los investigadores y emprendedores nuevos y jóvenes, incluidas las mujeres, adoptando un enfoque inclusivo y accesible de todos los talentos, las capacidades y la mano de obra disponible.

En noviembre de 2020, la Comisión puso en marcha el Pacto por las Capacidades, con una primera oleada de alianzas de capacidades en los tres ecosistemas industriales clave de la microelectrónica, la automoción y las industrias aeroespacial y de defensa. Los miembros del Pacto (industria, universidades y organizaciones de formación e interlocutores sociales) se comprometieron a garantizar una oferta continua y sostenible de capacidades en los ámbitos más necesarios mediante la mejora de las capacidades de 200 000 empleados y el reciclaje profesional de 300 000 personas, con una inversión pública y privada de 1 000 millones EUR de aquí a 2030.

Camino a seguir:

- La Comisión invita a los Estados miembros a comprometerse en la Brújula Estratégica para desarrollar desde el principio un enfoque estratégico coordinado a escala de la UE para las tecnologías críticas pertinentes para la seguridad y la defensa.
- En 2023, la Comisión revisará los instrumentos existentes y propondrá nuevas formas de fomentar la IDT+I de doble uso a escala de la UE.
- La Comisión apoyará la innovación y la iniciativa empresarial en tecnologías críticas para la seguridad y la defensa a través de las siguientes herramientas: a) acciones específicas del FED; b) un nuevo mecanismo de inversión combinada en defensa en el marco de InvestEU; c) una nueva iniciativa CASSINI para la defensa; d) una nueva incubadora de innovación sobre nuevas tecnologías e innovación de doble uso en 2022; y e) un mayor apoyo a las redes de innovación.
- La Comisión, junto con la AED y su Centro de Innovación en materia de Defensa, establecerá un Plan de Innovación en materia de Defensa de la UE para acelerar la innovación en seguridad y defensa a favor de la UE y de los Estados miembros.

4. Reducir las dependencias estratégicas en tecnologías críticas y cadenas de valor para la seguridad y la defensa

La UE dispone de varios instrumentos políticos, más allá de los programas e instrumentos de IDT+I, que pueden contribuir a reducir sus dependencias estratégicas en tecnologías críticas y cadenas de valor en los sectores de la seguridad y la defensa. Estos instrumentos contribuyen a reforzar la capacidad industrial, la competitividad, la soberanía tecnológica y la resiliencia de la UE, pero también sirven para proteger los avances y las capacidades tecnológicas actuales y futuras.

La Comisión, a partir del trabajo del Observatorio de Tecnologías Críticas y en el marco de la estrategia industrial actualizada, evaluará sistemáticamente las consideraciones de seguridad y defensa, según proceda, a la hora de aplicar y revisar los instrumentos industriales y comerciales

de la UE existentes, o de diseñar nuevos instrumentos para garantizar que son adecuados para su finalidad.

- *Alianzas industriales*: las alianzas industriales involucran a un amplio abanico de socios (por ejemplo, agentes públicos y privados, la sociedad civil) en una acción conjunta para alcanzar objetivos políticos clave de la UE en industrias o cadenas de valor específicas. Se basan en los principios de apertura, transparencia, diversidad e inclusividad, y funcionan respetando plenamente las normas de competencia. Las alianzas industriales pueden incluir, cuando proceda, líneas de trabajo específicas para reducir las dependencias estratégicas de los sectores de la seguridad y la defensa. Esto es lo que se está considerando en la Alianza europea para los datos industriales y la computación periférica y en la nube, y en la Alianza sobre tecnologías de procesadores y semiconductores.
- *Proyectos importantes de interés europeo común (PIICE)*: los Estados miembros dan inicio a los PIICE, que están sujetos a las normas de la UE sobre ayudas estatales. Están concebidos para sumar conocimientos, experiencia, recursos financieros y agentes económicos de toda la UE con el fin de superar las deficiencias del mercado o sistémicas y los retos sociales que los agentes privados no podrían abordar por sí solos, en particular en el ámbito de la innovación de vanguardia y de las infraestructuras clave. Los PIICE pueden tener en cuenta los aspectos de seguridad y defensa. Este podría ser el caso en el próximo segundo PIICE sobre microelectrónica anunciado en la Ley de Chips.
- *Programas de financiación de la UE*: la UE siempre ha tenido una política abierta de investigación e innovación. Se guía por el principio de autonomía estratégica abierta y tiene por objeto garantizar la igualdad de condiciones y la reciprocidad. El enfoque global de la UE en materia de investigación e innovación fomenta las asociaciones estratégicas con socios afines en consonancia con las obligaciones internacionales de la UE (por ejemplo, la OTAN, los Estados Unidos, Canadá, Japón, Corea del Sur, etc.)[14].

  Al mismo tiempo, Europa tiene que procurar preservar sus intereses estratégicos. Para el período 2021-2027, la Comisión ha aclarado y armonizado las normas de participación para los países no pertenecientes a la UE y la admisibilidad de las entidades en todos los programas e instrumentos de la UE. Se han establecido condiciones específicas de admisibilidad para las actividades sensibles en materia de seguridad para determinados programas (Horizonte Europa, PED, FED, Programa Espacial, MCE), mientras que para otros se han pulido aún más en los programas de trabajo pertinentes para proteger los intereses esenciales de seguridad de la UE. La revisión en curso del Reglamento Financiero de la Comisión también aportará más claridad acerca de cómo mantener el enfoque de autonomía estratégica abierta de la UE, es decir, cómo preservar plenamente los intereses esenciales de seguridad de la UE, respetando al mismo tiempo sus obligaciones internacionales.

[14] Cabe señalar, sin embargo, que los programas de investigación y desarrollo relacionados con la defensa de la mayoría de nuestros socios no están abiertos a las empresas de la UE.

– *Normas*: en el marco del Plan de acción sobre las sinergias, la Comisión promueve el uso de las normas híbridas existentes en materia civil y de defensa y el desarrollo de otras nuevas para finales de 2022 (acción 5), así como la consideración de la defensa en la política y las acciones de normalización de la Comisión. Si bien la estrategia de normalización[15] de la UE tiene por objeto garantizar el liderazgo de la UE en el establecimiento de normas civiles, será muy pertinente para el sector de la defensa, ya que casi el 80 % de las normas utilizadas en la defensa proceden de sectores civiles. La Comisión, junto con las partes interesadas (por ejemplo, la AED), estudiará la posibilidad de incluir requisitos de defensa en los futuros esfuerzos de normalización enfocados a mejorar su compatibilidad con las necesidades de defensa.

– *Control de la inversión extranjera directa*: la UE es uno de los entornos más abiertos del mundo para las inversiones extranjeras y uno de los principales destinos de la inversión extranjera directa (IED) del mundo. Sin embargo, hay algunas inversiones específicas que también pueden socavar los intereses esenciales de seguridad de la UE. Para prevenir estos riesgos, la UE ha establecido un marco para el control de las IED, que está en funcionamiento desde octubre de 2020. El primer informe anual sobre el control de las inversiones extranjeras directas confirma la importancia de un control eficaz de las IED a nivel de los Estados miembros y de una estrecha cooperación a escala de la UE, centrándose en los posibles riesgos para la seguridad o el orden público. Se anima a los Estados miembros a establecer mecanismos nacionales de control de las IED: dieciocho de ellos ya tienen uno, y otros seis están en preparación. La Comisión evaluará el Reglamento y presentará un informe al Parlamento Europeo y al Consejo a más tardar en octubre de 2023.

– *Infraestructuras críticas*: la aparición cada vez más rápida de tecnologías nuevas y disruptivas ha tenido un impacto significativo en la seguridad de los equipos, las infraestructuras, los servicios y las cadenas de valor y de suministro de los sectores estratégicos, incluidos los de la seguridad y la defensa. La UE y los Estados miembros deben tener más en cuenta estas vulnerabilidades en las evaluaciones de riesgos y el seguimiento pertinentes, así como en la aplicación de medidas de refuerzo de la resiliencia contra las amenazas a la seguridad, por ejemplo, de naturaleza híbrida o cibernética. Será necesaria una coordinación a nivel de la UE para garantizar que los Estados miembros mantengan un nivel de resiliencia a la altura de las exigencias futuras y unas normas de seguridad coherentes para evitar vulnerabilidades.

– *Uso inteligente y circular de materiales*: el nuevo Plan de Acción para la Economía Circular de marzo de 2020 es uno de los principales pilares del Pacto Verde Europeo, el nuevo programa de Europa en favor del crecimiento sostenible. La innovación y los nuevos modelos de negocio basados en una mayor eficiencia en el uso de los recursos, el desarrollo de nuevos materiales, la promoción de materias primas secundarias y una contratación pública más sostenible no solo preservarán el medio ambiente, sino que también garantizarán el acceso de la industria a los materiales. Las técnicas de fabricación aditiva, la contratación pública ecológica y el reciclado de materiales, si se ejecutan correctamente, también podrían

[15] COM(2022) 31 final.

contribuir a reforzar la resiliencia y la competitividad de las industrias de seguridad y defensa de la UE.

- *Seguridad de los datos*: la estrategia europea en materia de datos establece medidas para garantizar que las personas y las empresas puedan mantener el control de sus datos. La cuestión se abordará en la Ley de Datos que la Comisión adoptará a principios de 2022.

  Como parte del proyecto plurinacional sobre infraestructuras y servicios de datos comunes (que reúne a la Federación Europea de Computación en Nube y los espacios comunes europeos de datos), la Comisión está facilitando las inversiones —por ejemplo, el Programa Europa Digital (PED), el Mecanismo «Conectar Europa» (MCE), el fondo NextGenerationEU— en capacidades de la nube/periféricas que sean seguras, resilientes, eficientes desde el punto de vista energético y accesibles en tiempo real, y que ofrezcan un servicio de calidad en toda Europa. Garantizar la transferencia de tecnologías en la nube y periféricas entre las industrias civil (en particular la seguridad), de la defensa y espacial reforzaría la soberanía tecnológica. La Alianza europea para los datos industriales y la computación periférica y en la nube ofrece una posible plataforma para fomentar tales sinergias.

- *Política comercial*: la complejidad y vulnerabilidad de las cadenas de suministro mundiales no representa un problema solo para la UE. Hay países que dependen de la UE («dependencias inversas») y el comercio («interdependencia») puede contribuir a la estabilidad de las cadenas de valor mundiales. La UE también está dispuesta a actuar con firmeza y a defenderse contra las prácticas comerciales desleales, como el uso de subvenciones extranjeras distorsionadoras, al tiempo que actúa de conformidad con sus compromisos internacionales. La UE seguirá aprovechando al máximo los instrumentos comerciales y de competencia de que dispone, garantizando al mismo tiempo su correcto funcionamiento y actualización. La Comisión ha propuesto nuevos instrumentos, como el Reglamento sobre subvenciones extranjeras[16], que aborda las distorsiones en el mercado interior causadas por las subvenciones extranjeras.

En la Comunicación sobre defensa se enumeran otras medidas políticas pertinentes, como, por ejemplo, la introducción de una posible exención del impuesto sobre el valor añadido (IVA) o la facilitación de la transferencia de productos de defensa financiados por la UE.

Camino a seguir:

- La Comisión está estudiando la posibilidad de añadir líneas de trabajo en materia de defensa a iniciativas como la Alianza europea para los datos industriales y la computación periférica y en la nube y la Alianza industrial sobre tecnologías de procesadores y semiconductores.
- Junto con los Estados miembros, la Comisión identificará e informará en 2023 sobre la necesidad de evaluar el riesgo de las cadenas de suministro de infraestructuras críticas, en particular en el ámbito digital, para proteger mejor los intereses de seguridad y defensa de

[16] COM(2021) 223 final.

la UE.

- La Comisión anima a todos los demás Estados miembros a que establezcan un mecanismo nacional de control de las inversiones extranjeras directas.

5. Dimensión exterior

La cooperación con socios afines de todo el mundo es esencial para mejorar la resiliencia y la seguridad del suministro de la UE, reduciendo al mismo tiempo las dependencias estratégicas y aumentando los beneficios mutuos. En este contexto, el principio de reciprocidad desempeña un papel importante. Entre los socios tradicionales de la UE en los ámbitos de la tecnología, la seguridad y la defensa encontramos a los miembros del Espacio Económico Europeo (en particular Noruega), los países candidatos, los países vecinos y otros terceros países (como, por ejemplo, los Estados Unidos, Canadá, Japón y Corea del Sur), así como a las organizaciones internacionales (por ejemplo, la OTAN). Entre los intercambios recientes, cabe señalar:

5.1. Consejo UE-Estados Unidos de Comercio y Tecnología

El Consejo UE-Estados Unidos de Comercio y Tecnología (TTC) celebró su primera reunión el 29 de septiembre de 2021. En la declaración conjunta la UE y los Estados Unidos reafirmaron su compromiso de «centrarse en impulsar la resiliencia de las respectivas cadenas de suministro y de la seguridad del suministro en sectores clave para la transición ecológica y digital y para garantizar la protección de nuestros ciudadanos», así como su objetivo de «mejorar la transparencia de la oferta y la demanda; cartografiar las respectivas capacidades sectoriales existentes; intercambiar información sobre medidas políticas e investigación y prioridades de desarrollo; y cooperar en estrategias para fomentar la resiliencia y la diversificación de la cadena de suministro». Los trabajos en curso más pertinentes para la presente hoja de ruta son los que se están llevando a cabo en los grupos de trabajo sobre cadenas de suministro seguras (incluidos los semiconductores, con un procedimiento separado), seguridad de las tecnologías de la información y la comunicación, controles de las exportaciones y control de las inversiones. El diálogo sobre seguridad y defensa entablado recientemente entre la UE y los Estados Unidos también podría servir de foro de debate sobre estas cuestiones.

5.2. Cooperación con la OTAN

En la Cumbre de Bruselas de 2021, los dirigentes de la OTAN establecieron una ambiciosa agenda sobre tecnologías, en particular las tecnologías emergentes y disruptivas[17], que ha proporcionado mayor orientación para el trabajo llevado a cabo de conformidad con la estrategia de aplicación de la OTAN para las tecnologías emergentes y disruptivas, aprobada por los ministros de Defensa de la OTAN en febrero de 2021.

La Comisión y el Alto Representante supervisarán los avances de las correspondientes iniciativas de la OTAN en este ámbito mediante contactos regulares de trabajo con la OTAN, con vistas a una posible interacción mutuamente aceptable y beneficiosa con las iniciativas pertinentes de la

[17] La agenda incluía la decisión de poner en marcha el Acelerador de Innovación en Defensa para el Atlántico Norte («DIANA», por sus siglas en inglés) y un Fondo de Innovación de la OTAN.

UE con total transparencia para con los Estados miembros, al tiempo que se evita crear nuevas dependencias tecnológicas o de capacidades o el agravamiento de las existentes.

Camino a seguir:

- La Comisión y el Alto Representante analizarán cómo impulsar la resiliencia de la cadena de suministro y garantizar la protección de los ciudadanos en el contexto del Consejo UE-Estados Unidos de Comercio y Tecnología y del diálogo entre la UE y los Estados Unidos sobre seguridad y defensa recientemente iniciado.
- La Comisión y el Alto Representante estudiarán con la OTAN, en el marco de las declaraciones conjuntas sobre la cooperación UE-OTAN y con total transparencia para con los Estados miembros, cómo promover una interacción mutuamente aceptable y beneficiosa entre sus respectivas iniciativas pertinentes.

6. Conclusiones

Dado que la situación geopolítica mundial sigue siendo compleja y continúa la carrera en pro de nuevas tecnologías que sean pertinentes para la seguridad y la defensa, la UE y sus Estados miembros deben reforzar la cooperación en materia de tecnologías esenciales para la seguridad y la defensa a largo plazo de Europa, e incrementar los esfuerzos para reducir las dependencias estratégicas conexas.

Esta hoja de ruta propone colaborar estrechamente con los Estados miembros en la identificación de tecnologías críticas y cadenas de valor para la seguridad y la defensa, así como de las causas profundas de las dependencias estratégicas asociadas en el contexto del Observatorio de Tecnologías Críticas, con el fin de apoyar un enfoque estratégico coordinado a escala de la UE para las tecnologías críticas pertinentes para la seguridad y la defensa que aproveche al máximo los programas e instrumentos de IDT+I de la UE y nacionales.

Para aumentar la competitividad y la resiliencia de los sectores de la seguridad y la defensa, las conclusiones del Observatorio y los trabajos conexos en el marco de la estrategia industrial actualizada también contribuirán a garantizar que las consideraciones de seguridad y defensa se tengan más en cuenta en las políticas industriales y comerciales de la UE, según proceda y en consonancia con las normas de competencia y las obligaciones internacionales de la UE.

Las propuestas incluidas en esta hoja de ruta tienen por objeto contribuir a la dimensión de IDT+I de la próxima Brújula Estratégica de la UE, a través de la cual los Estados miembros fijarán objetivos ambiciosos a largo plazo para mejorar sustancialmente la seguridad y la defensa de Europa.