Consejo de la Unión Europea

Bruselas, 22 de mayo de 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
A:	Delegaciones
N.º doc. prec.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Asunto:	Conclusiones del Consejo sobre la política de ciberdefensa de la UE

Adjunto se remite a las delegaciones las Conclusiones del Consejo sobre la política de ciberdefensa de la UE, adoptadas por el Consejo en su sesión del 22 de mayo de 2023.

Conclusiones del Consejo sobre la política de ciberdefensa de la UE

1. El Consejo acoge con satisfacción la ambiciosa Comunicación conjunta sobre la política de ciberdefensa de la UE, basada en el marco político de ciberdefensa de 2014 y su actualización de 2018, cuyo objetivo es seguir invirtiendo en unas fuerzas armadas modernas e interoperables, en tecnologías de vanguardia, en las más avanzadas capacidades de ciberdefensa y en reforzar las asociaciones para afrontar los retos comunes. En un momento en el que está aumentando la dependencia de las tecnologías digitales, el ciberespacio se ha convertido en un ámbito de competencia estratégica. Por tanto, resulta indispensable preservar la apertura, libertad, estabilidad y seguridad del ciberespacio. El recurso a ciberoperaciones que han permitido y acompañado la guerra de agresión no provocada e injustificada de Rusia contra Ucrania afecta a la estabilidad y la seguridad mundiales, representa un riesgo importante de escalada y se suma al ya significativo aumento de las actividades informáticas malintencionadas emprendidas en los últimos años al margen de los conflictos armados.

2. La guerra en Ucrania ha generado un nuevo contexto estratégico y ha confirmado la necesidad de que la UE, sus Estados miembros y sus socios refuercen aún más la resiliencia de la UE frente a las ciberamenazas y aumenten nuestra ciberseguridad y ciberdefensa comunes contra comportamientos malintencionados y actos de agresión en el ciberespacio. La Comunicación conjunta sobre la política de ciberdefensa de la UE pone de manifiesto nuestra determinación de proporcionar medidas inmediatas y a largo plazo para garantizar la libertad de acción en el ciberespacio y respuestas a los agentes de riesgo que intentan, entre otras cosas, invadir, perturbar o destruir las redes y sistemas información de la UE y sus socios. Como complemento de la Estrategia de Ciberseguridad de la UE y en consonancia con la Brújula Estratégica, la Comunicación conjunta representa un paso importante hacia un planteamiento de la UE que abarca todo el espectro en materia de resiliencia, respuesta, prevención de conflictos, cooperación y estabilidad en el ciberespacio. En este contexto, el Consejo subraya la necesidad de que la UE, sus Estados miembros y sus socios den respuestas adecuadas y coherentes, y aguarda con interés la revisión de las directrices de aplicación del conjunto de instrumentos de ciberdiplomacia de la UE, que será otro paso clave hacia la evolución de la posición de la UE en materia cibernética.

3. El Consejo hace hincapié en que los recientes ciberataques contra infraestructuras críticas europeas, la rápida evolución del panorama de las ciberamenazas y el ritmo acelerado de desarrollo tecnológico también demuestran la necesidad de aumentar la coordinación y la cooperación civil-militar, al tiempo que subraya que no existe jerarquía entre las comunidades civil y militar.

   La política de ciberdefensa de la UE le permite a esta y a sus Estados miembros reforzar su capacidad para proteger, detectar, defender y disuadir, haciendo un uso adecuado de toda la gama de opciones defensivas de que disponen las comunidades civil y militar para la seguridad y la defensa más amplias de la UE, de conformidad con el Derecho internacional, en particular el Derecho en materia de derechos humanos y el Derecho internacional humanitario.

4. Si bien la seguridad nacional, también en el ámbito cibernético, sigue siendo responsabilidad exclusiva de cada Estado miembro, como se señala en el artículo 4, apartado 2, del TUE, el Consejo destaca, no obstante, la necesidad de invertir sustancialmente de forma individual y colaborativa en una mayor resiliencia y el despliegue de todo el espectro de capacidades de ciberdefensa, así como de aprovechar los marcos de cooperación y los incentivos financieros de la UE. El Consejo hace hincapié en la necesidad de seguir reforzando las acciones de los Estados miembros y de las instituciones, órganos y organismos de la UE con el fin de proteger a la Unión, a nuestros ciudadanos, a las instituciones, órganos y organismos de la UE y a las misiones y operaciones de la política común de seguridad y defensa (PCSD) en el ciberespacio. Asimismo, subraya la importancia de impulsar la resiliencia de la UE en el ciberespacio mediante el desarrollo de capacidades de ciberdefensa y el refuerzo de la cooperación con un ecosistema privado de confianza.

I. **Acción común por una ciberdefensa reforzada**

5. El Consejo reitera que un proceso gradual, transparente e integrador resulta esencial para reforzar la confianza, lo cual es fundamental para profundizar en la creación de un marco de gestión de crisis de ciberseguridad de la UE, que deberá llevarse a cabo en consonancia con la hoja de ruta de gestión de crisis cibernéticas elaborada en el Consejo. El Consejo reitera la necesidad de seguir aumentando nuestra capacidad de protección, detección, defensa y prevención de los ciberataques mediante la mejora de la conciencia situacional, el desarrollo de capacidades y medios, la formación, los ejercicios y el refuerzo de la resiliencia, y respondiendo con firmeza a los ciberataques contra la UE, sus Estados miembros y las instituciones, órganos y organismos de la UE, así como las misiones y operaciones de la PCSD, utilizando todos los medios adecuados. Para ello, el Consejo anima al Alto Representante y a la Comisión a que reduzcan la complejidad en el ámbito cibernético, eviten duplicaciones innecesarias y garanticen la cooperación y las sinergias con las iniciativas existentes. Es necesario reforzar la cooperación y la coordinación entre los agentes de ciberdefensa dentro de la UE y de los Estados miembros, entre las comunidades cibernéticas militar y civil y entre un ecosistema público y un ecosistema privado de confianza. En este contexto, se anima a los Estados miembros a seguir explorando y reforzando los mecanismos nacionales de coordinación civil-militar, a facilitar el intercambio voluntario de información, a compartir las enseñanzas extraídas, a contribuir a la elaboración de normas interoperables y a llevar a cabo evaluaciones y supuestos de riesgo, así como a realizar ejercicios conjuntos, en particular a escala europea, respetando plenamente las disposiciones de la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad (SRI 2).

6. Reconociendo los esfuerzos por seguir aumentando la resiliencia de la Unión con la SRI 2 y la Directiva relativa a la resiliencia de las entidades críticas (Directiva REC), el Consejo reitera su recomendación sobre un enfoque coordinado a escala de la UE para reforzar la resiliencia de las infraestructuras críticas[1]. Pide medidas para seguir aumentando la resiliencia de las entidades críticas, de las infraestructuras, de los productos y de los servicios digitales, y señala que el paso más importante sigue siendo la correcta aplicación de la SRI 2; aunque se trata sobre todo de una responsabilidad civil, también contribuye a reforzar la ciberdefensa. En este contexto, se anima a las instituciones, órganos y organismos de la UE, así como a los Estados miembros, a que apoyen un mayor desarrollo y despliegue de mecanismos nuevos y existentes de coordinación de la UE, las evaluaciones, valoraciones y supuestos de riesgos, la puesta voluntaria en común de información y ejercicios, de manera que se añada valor y se eviten duplicaciones innecesarias con las iniciativas existentes.

7. Con la perspectiva de seguir reforzando la confianza, consolidar la cooperación y facilitar el intercambio oportuno de información sobre ciberincidentes importantes y a gran escala que afecten a los sistemas de defensa, el Consejo acoge con satisfacción la iniciativa de ahondar en el desarrollo de la Conferencia de Cibermandos de la UE que organizará cada Presidencia del Consejo de la UE, con el apoyo de la Agencia Europea de Defensa (AED) y la participación del Servicio Europeo de Acción Exterior (SEAE). El Consejo anima a todos los Estados miembros a participar en dichas reuniones. Para reforzar la resiliencia de la UE frente a los ciberincidentes a gran escala, el Consejo invita a la red de organizaciones de enlace de crisis cibernéticas (CyCLONe) y a la Conferencia de Cibermandos de la UE a determinar posibles maneras de cooperar y beneficiarse de una perspectiva militar y civil conjunta.

[1] Propuesta de Recomendación del Consejo sobre un enfoque coordinado de la Unión para reforzar la resiliencia de las infraestructuras críticas (COM/2022/551 final).

8. Con el objetivo de fomentar una respuesta más sólida y coordinada a escala de la UE, el Consejo acoge con satisfacción la creación de la red operativa de equipos militares de respuesta a emergencias informáticas de la UE (MICNET) y espera con interés que se alcance la capacidad operativa inicial para mediados de 2024, cuyo fin es mejorar el intercambio de información técnica sobre ciberincidentes que afecten a los sistemas de defensa entre los Estados miembros participantes. El Consejo anima a todos los Estados miembros a participar en MICNET para garantizar la eficacia de la red. Asimismo, el Consejo invita a los Estados miembros a aprovechar las enseñanzas extraídas de la red de equipos de respuesta a incidentes de seguridad informática (CSIRT) y anima encarecidamente a que se cree un mecanismo eficaz de cooperación y coordinación entre ambas redes en el momento oportuno, respetando plenamente los mecanismos de gobernanza y las circunscripciones de cada entidad.

9. A la luz del aumento de las actividades informáticas malintencionadas de agentes estatales y no estatales contra misiones y operaciones de la PCSD de la UE, el Consejo invita a la UE y a sus Estados miembros a reforzar sus capacidades para defender y proteger las misiones y operaciones de la PCSD. En este sentido, el Consejo acoge con satisfacción los objetivos de seguir avanzando en la protección de las redes y estructuras militares de la UE, en consonancia con la visión y estrategia militar de la UE en el ciberespacio como ámbito de operación[2], entre otras.

[2] EEAS(2021) 706 REV4.

10. El Consejo reitera las Conclusiones del Consejo de mayo de 2022[3] y la necesidad de invertir en nuestra asistencia mutua en virtud del artículo 42, apartado 7, del TUE, así como en la cláusula de solidaridad del artículo 222 del TFUE. El Consejo destaca la importancia de seguir profundizando en la interpretación común, de la UE y de sus Estados miembros, de la aplicación del artículo 42, apartado 7, en particular en situaciones complejas que impliquen un ciberataque, en consonancia con los principios pertinentes del Derecho internacional. Acoge con satisfacción la posibilidad de que la UE preste ayuda a petición expresa de los Estados miembros cuando se produzca un ciberataque, sin perjuicio del carácter específico de la política de seguridad y defensa de determinados Estados miembros.

11. El Consejo subraya los avances logrados en el proyecto Equipos de Respuesta Telemática Rápida y de Asistencia Mutua en el ámbito de la Ciberseguridad, de la Cooperación Estructurada Permanente (CEP), y su disposición a actuar, previa solicitud, como capacidad de respuesta a las necesidades de los Estados miembros y de la UE, en apoyo de las misiones y operaciones de la PCSD, y a prestar asistencia a los socios de la UE. El Consejo acoge con satisfacción que se sigan desarrollando las capacidades de los equipos de respuesta telemática rápida de la CEP, los equipos nacionales de ciberrespuesta y, cuando proceda, las capacidades adicionales de respuesta ante incidentes, como los futuros equipos de respuesta rápida contra amenazas híbridas previstos en la Brújula Estratégica, en particular fomentando su coordinación y cooperación a escala de la UE.

[3] Conclusiones del Consejo sobre la elaboración de la posición de la Unión Europea en materia cibernética, 23 de mayo de 2022 (9364/22).

12. El Consejo acoge con satisfacción la labor del proyecto Centro de Coordinación del Ámbito del Ciberespacio y de la Información (CIDCC), de la CEP, que tiene por objeto proporcionar capacidades militares destinadas a recopilar y analizar información pertinente para obtener un panorama operativo común del ciberespacio. Asimismo, el Consejo acoge con satisfacción la propuesta de integrar, a partir de 2025, la prueba de concepto —si resulta eficaz como centro de coordinación de la información— en un Centro de Coordinación de la Ciberdefensa de la UE, con lo que se reforzará la coordinación y la conciencia situacional, en particular de los mandos de las misiones y operaciones de la PCSD de la UE, así como el refuerzo de toda la arquitectura de mando y control de la UE. El Consejo pide al Alto Representante que presente un concepto y una hoja de ruta para la creación del Centro de Coordinación de la Ciberdefensa de la UE, extrayendo enseñanzas de entidades internacionales similares, determinando los recursos necesarios, evitando duplicaciones innecesarias y buscando la complementariedad con el marco más amplio de ciberseguridad de la UE.

13. El Consejo destaca la importancia de la cooperación en inteligencia estratégica en materia de ciberamenazas y actividades informáticas malintencionadas, e invita a los Estados miembros a que, a través de sus autoridades competentes, sigan contribuyendo al trabajo del Centro de Inteligencia y de Situación de la Unión Europea (INTCEN), de la Dirección de Información del EMUE y de los Estados miembros en el marco de la Capacidad Única de Análisis de Inteligencia (SIAC). El Consejo destaca además la importancia de reforzar nuestras capacidades de ciberinteligencia para aumentar nuestra ciberresiliencia, nuestras ciberrespuestas y prestar un apoyo eficaz a nuestras misiones y operaciones civiles y militares de la PCSD, así como a nuestras fuerzas armadas y a la capacidad de la SIAC en el ámbito cibernético, según las contribuciones voluntarias de inteligencia de los Estados miembros y sin perjuicio de sus competencias.

14. El Consejo toma nota del Centro de Análisis y Situación Cibernéticos de la Comisión Europea, cuyo objetivo es reforzar la conciencia situacional por parte de la Comisión. El Consejo destaca la importancia de establecer una cooperación mutuamente beneficiosa entre este centro y otras instituciones, órganos y organismos de la UE, en particular la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la UE (CERT-UE). El Consejo subraya la importancia de garantizar una estrecha colaboración con las redes de cooperación de la UE a la hora de desarrollar la conciencia situacional, así como de respetar la confidencialidad. El Consejo señala la necesidad de reforzar la conciencia situacional común a escala de la UE y de seguir elaborando el marco de gestión de crisis de ciberseguridad de la UE, evitando al mismo tiempo cualquier duplicación innecesaria de esfuerzos.

15. El Consejo recuerda que la educación, la formación y los ejercicios en materia cibernética son esenciales para garantizar la preparación y la eficacia, y acoge con satisfacción las actividades nacionales, así como las realizadas por la UE a través de la Escuela Europea de Seguridad y Defensa (EESD), la AED, la ENISA y los proyectos de la CEP en curso, como la Federación de Campos de Maniobras Virtuales y el Centro de la Unión Europea para el Mundo Académico y la Innovación en el ámbito del Ciberespacio (CAIH). Con vistas a seguir intensificando estos esfuerzos, el Consejo espera con interés la creación de CyDef-X, proyecto marco de la AED destinado a sincronizar y apoyar los ejercicios de ciberdefensa. El Consejo anima a la AED a estudiar, en estrecha cooperación con los Estados miembros y el SEAE, el modo en que CyDef-X puede seguir apoyando ejercicios como CYBER PHALANX, en particular en lo relativo a la asistencia mutua contemplada en el artículo 42, apartado 7, del TUE y a la cláusula de solidaridad prevista en el artículo 222 del TFUE, así como con la Comisión y la ENISA en lo que respecta a los ejercicios civiles. Además, el Consejo anima a que, en el marco de CyDef-X, se utilicen y se sigan desarrollando los entornos existentes de ensayo y ejercicios de ciberdefensa, como la Federación de Campos de Maniobras Virtuales. El Consejo subraya que, para garantizar un proceso de toma de decisiones ágil y eficiente en caso de crisis cibernética, es importante llevar a cabo ejercicios periódicos de simulación teórica en el nivel decisorio de los Estados miembros.

16. El Consejo señala la propuesta del Reglamento de Cibersolidaridad y la intención de reforzar las capacidades para detectar las amenazas e incidentes de ciberseguridad en la UE y darles respuesta. El Consejo subraya que las propuestas en este ámbito solo pueden ser eficaces si se ajustan a los marcos y necesidades de gestión de crisis de los Estados miembros. El Consejo subraya la importancia de poner a prueba las infraestructuras críticas para detectar posibles vulnerabilidades —cuando ello se considere beneficioso, como competencia nacional— teniendo en cuenta las evaluaciones de riesgos de que se dispone en el ámbito de la UE.

17. El Consejo señala la propuesta de la Comisión de crear un mecanismo de ciberemergencia, que podría propiciar la disponibilidad de servicios de ciberseguridad de proveedores privados de confianza destinados a ayudar, previa solicitud, a los Estados miembros en caso de ciberincidentes a gran escala, al tiempo que subraya la necesidad de ampliar el sector europeo de la ciberseguridad con el apoyo del Centro Europeo de Competencia en Ciberseguridad (CECC), pilar esencial para que este mecanismo sea operativo. El Consejo subraya el papel clave de cada Estado miembro en el seguimiento y la evaluación de sus necesidades nacionales.

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

18. El Consejo recuerda que anima a los Estados miembros a seguir desarrollando sus propias capacidades para llevar a cabo operaciones de ciberdefensa, en particular, medidas proactivas de protección, detención, defensa y disuasión frente a los ciberataques, cuando proceda. Considerando que la SRI 2 no se aplica a las entidades de la Administración pública que lleven a cabo sus actividades en el ámbito de la defensa, el Consejo invita a la AED a que, con el apoyo de la Comisión y del SEAE, según proceda, ayude a los Estados miembros a formular recomendaciones voluntarias no vinculantes inspiradas en la SRI 2 para aumentar la ciberseguridad en la comunidad de defensa, e invita a todos los Estados miembros a que participen activamente en este esfuerzo. Estas recomendaciones deben tener en cuenta los esfuerzos similares realizados en otros marcos.

19. Tal como se reconoce en la Brújula Estratégica, la capacidad de actuación de la UE depende de su habilidad para reducir sus dependencias estratégicas en sus capacidades de ciberdefensa y sus cadenas de suministro, así como de desarrollar y dominar tecnologías punteras de ciberdefensa. Esto incluye reforzar la base industrial y tecnológica de la defensa europea en toda la UE y su capacidad para cooperar con socios afines de todo el mundo, con arreglo a un principio de reciprocidad para garantizar beneficios mutuos. Por tanto, el Consejo pide a los sectores de la ciberseguridad y la ciberdefensa que cooperen estrechamente para crear sinergias con el objetivo de desarrollar y ofrecer todo el espectro de capacidades de ciberdefensa. El Consejo invita a la Comisión a que, en estrecha colaboración con el CECC siga apoyando, cuando proceda, el desarrollo de una base industrial y tecnológica europea fuerte, ágil, competitiva e innovadora en materia de ciberdefensa —que incluya a las pequeñas y medianas empresas (pymes)— mediante nuevas inversiones y acciones políticas.

20. Teniendo en cuenta la importancia de la interoperabilidad y el carácter común de las capacidades de ciberdefensa, en particular en lo que respecta al desarrollo colaborativo de las capacidades de ciberdefensa de nueva generación, el Consejo invita a la AED y al Estado Mayor de la UE a trabajar en un conjunto de requisitos de interoperabilidad de la ciberdefensa de la UE, que se basarían en los principios, procesos y normas existentes y establecidos, en particular, en el marco de la Organización del Tratado del Atlántico Norte (OTAN), y que serían compatibles con ellos. Asimismo, el Consejo invita a los Estados miembros a estudiar, en el marco del Comité Europeo de Normalización de la Defensa, si podrían necesitarse normas voluntarias específicas para los sistemas de defensa, en estrecha cooperación con todas las partes interesadas pertinentes, en particular las organizaciones europeas de normalización y la OTAN, según proceda.

21 El Consejo acoge con satisfacción los esfuerzos de la Comisión por presentar un plan para promover el uso de las normas existentes para los usos civiles de la ciberseguridad y la ciberdefensa, así como la elaboración de nuevas normas voluntarias. El Consejo hace hincapié en la necesidad de armonizar las normas de ciberseguridad y ciberdefensa, cuando proceda. El Consejo reconoce que estas normas voluntarias podrían ser útiles para los sectores de la ciberseguridad y la ciberdefensa de la UE e insta a una colaboración más estrecha entre los organismos de normalización civiles y de defensa.

22. El Consejo pide que se adopten rápidamente recomendaciones basadas en el inventariado de las herramientas existentes de comunicación segura en el ámbito cibernético, elaboradas por la Comisión y las instituciones pertinentes. En la medida de lo posible, las recomendaciones deben ajustarse a las iniciativas existentes en materia de intercambio de información y también deben tener en cuenta los riesgos que plantean las tecnologías emergentes y disruptivas para los actuales métodos de cifrado.

23. Además, el Consejo acoge con satisfacción el trabajo inicial realizado sobre la evaluación y los supuestos de riesgos que están elaborando la Comisión, el Alto Representante y el Grupo de Cooperación SRI, en relación, inicialmente, con los sectores de la energía y las telecomunicaciones, a petición del Consejo. El Consejo reconoce que también se están preparando evaluaciones específicas de los riesgos de ciberseguridad para las infraestructuras y redes de comunicaciones en la UE. El Consejo reitera que es de suma importancia llegar a un entendimiento común de las posibles repercusiones de los ciberincidentes entre los Estados miembros, pero también entre las instituciones, órganos y organismos de la UE. Así pues, el Consejo invita a los agentes mencionados a que velen por que las evaluaciones y los supuestos de riesgos y las recomendaciones posteriores se tengan en cuenta a la hora de definir y priorizar las medidas y el apoyo, a escala de la UE y, cuando proceda, a nivel nacional. Asimismo, el Consejo pide que todos los agentes pertinentes tengan en cuenta los supuestos de riesgo en los procesos de evaluación de riesgos, así como en la preparación de ciberejercicios.

III. **Inversión en capacidades de ciberdefensa**

24. El Consejo anima a los Estados miembros a aumentar sus inversiones para crear, mantener y desarrollar capacidades interoperables de ciberdefensa. El Consejo respalda la elaboración de un conjunto de compromisos voluntarios destinados a ahondar en el desarrollo de las capacidades nacionales de ciberdefensa, teniendo presentes los esfuerzos similares realizados en otros marcos.

25. El Consejo pide a los Estados miembros y a la AED que aprovechen la oportunidad que brinda la revisión del Plan de Desarrollo de Capacidades para fijar un nivel elevado de ambición en lo que respecta al desarrollo de la ciberdefensa colaborativa a escala de la UE. El Consejo anima además a los Estados miembros a basarse en el conjunto actualizado de prioridades y en sus compromisos de la CEP para aumentar su participación en proyectos colaborativos de la UE de desarrollo de capacidades de ciberdefensa, reconociendo el beneficio directo de dichos proyectos en el desarrollo de capacidades nacionales de ciberdefensa.

26. El Consejo acoge con satisfacción los esfuerzos de investigación en colaboración a escala de la UE para explorar las posibles aplicaciones de las tecnologías emergentes y disruptivas en los sistemas relacionados con la defensa, y señala asimismo la necesidad de garantizar que estos avances tecnológicos se incorporen rápidamente a las capacidades existentes y futuras. El Consejo anima a los Estados miembros y a la industria de la UE a aprovechar al máximo las oportunidades de investigación en colaboración a escala de la UE, por ejemplo en el marco de la AED y de proyectos en curso de la CEP, como el Centro de la Unión Europea para el Mundo Académico y la Innovación en el Ámbito del Ciberespacio (CAIH), el Fondo Europeo de Defensa y, cuando proceda, Horizonte Europa y el programa Europa Digital para proyectos de doble uso. Por otra parte, el Consejo acoge con satisfacción el aprovechamiento de los marcos específicos para apoyar la innovación en materia de defensa mediante la utilización de asimilaciones (*spin-ins*) procedentes del ámbito civil, en particular el Plan de Innovación de la UE en materia de Defensa y el Centro de Innovación en materia de Defensa. Además, el Consejo anima al CECC y a la AED a que elaboren un acuerdo de colaboración para facilitar el intercambio de información entre sus servicios sobre, respectivamente, las prioridades de la tecnología civil, de doble uso y de defensa, con vistas a crear sinergias y evitar duplicaciones.

27. El Consejo acoge con satisfacción la intención de la Comisión de elaborar una hoja de ruta tecnológica para las cibertecnologías críticas en cooperación con la AED y el CECC en consonancia con sus respectivos mandatos, con los Estados miembros y en consulta con las partes interesadas pertinentes, como la industria, que, al determinar las cibertecnologías críticas e inventariar los avances tecnológicos y las dependencias estratégicas, ofrezca maneras de reducir estas últimas, apoyando así la autonomía estratégica y la soberanía tecnológica de la UE, y preservando al mismo tiempo una economía abierta. El Consejo señala que la hoja de ruta tecnológica para las cibertecnologías críticas podrá fundamentar las prioridades estratégicas de los instrumentos de financiación de la UE, en consonancia con las respectivas modalidades establecidas para dichos instrumentos. El Consejo recuerda que la UE debe aplicar una política industrial europea ambiciosa y firme para crear un entorno empresarial sostenible, atractivo y competitivo, que también permita la expansión de las entidades europeas en el ámbito cibernético.

28. El Consejo agradece la intención de abordar el importante déficit de capacidades en materia de ciberseguridad atrayendo a nuevos profesionales —en particular a mujeres—, fomentando el perfeccionamiento y el reciclaje profesionales, invirtiendo en formaciones y ejercicios y organizándolos para crear una mano de obra diversa e inclusiva en el ámbito cibernético. Reconociendo los retos a los que se enfrenta la UE en relación con el capital humano en el ámbito de la ciberseguridad y la ciberdefensa, el Consejo acoge con satisfacción la iniciativa de la Academia de Cibercapacidades, que también puede beneficiar a la mano de obra de la ciberdefensa.

29. El Consejo invita a los Estados miembros a intercambiar información sobre las mejores prácticas para formar a profesionales cualificados en materia de ciberseguridad, aprovechando las sinergias entre las iniciativas militares, civiles y policiales, y pide a la EESD, con el apoyo y la experiencia de la AED y la ENISA, que estudie opciones para aumentar el intercambio de mejores prácticas y nuevas sinergias entre los ámbitos militar y civil en relación con la formación y el desarrollo de capacidades de defensa específicas del ámbito cibernético.

30. El Consejo subraya la importancia de contar con una interpretación común de la composición de la mano de obra en el ámbito de la ciberseguridad y de las competencias asociadas a fin de detectar y abordar las lagunas en el mercado laboral de dicho ámbito, así como la necesidad de fomentar la participación de todas las partes interesadas, en particular de los Estados miembros y de la industria. El Consejo reconoce que el establecimiento de indicadores de seguimiento del mercado de trabajo en el ámbito de la ciberseguridad ayudaría a determinar las necesidades en materia de capacidades en este sector y a orientar adecuadamente los fondos, además de contribuir al cumplimiento de las obligaciones relacionadas con las políticas, en particular las derivadas de la SRI 2. El Consejo acoge con satisfacción la propuesta de un marco de certificación de las capacidades de ciberdefensa e invita al Alto Representante, en su calidad de director de la EESD, a que lo elabore, en cooperación con el SEAE, la Comisión y los Estados miembros, aprovechando las iniciativas civiles.

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

31. El Consejo pide al Alto Representante y a la Comisión que refuercen e impulsen su cooperación y exploren asociaciones mutuamente beneficiosas y adaptadas en materia de políticas de ciberdefensa, en particular en el ámbito del desarrollo de capacidades de ciberdefensa a través del Fondo Europeo de Apoyo a la Paz (FEAP). A tal fin, debe añadirse la ciberdefensa como punto a los diálogos y consultas de la UE relativos al ámbito cibernético, así como a las consultas generales sobre seguridad y defensa con los socios; además, deben reforzarse los diálogos y la colaboración con el sector privado. El Consejo subraya que la colaboración internacional en materia de normas y certificación de la ciberseguridad supondría un valor añadido para la industria europea. Por tanto, acoge con satisfacción el compromiso de la Comisión de hacer de esta cuestión un punto esencial de los ciberdiálogos de la UE con terceros países y organizaciones internacionales.

32. El Consejo destaca la importancia de la cooperación internacional para prevenir o reducir los riesgos de conflicto en el ciberespacio, especialmente mediante la elaboración y la puesta en práctica de medidas de fomento de la confianza a escala regional e internacional, también en la esfera de las Naciones Unidas, y de continuar impulsando el uso de las medidas de fomento de la confianza existentes en el ámbito cibernético, como en la Organización para la Seguridad y la Cooperación en Europa (OSCE), incluso en tiempos de tensiones internacionales.

    La UE y sus Estados miembros hacen hincapié en que el Derecho internacional vigente es de aplicación al ciberespacio y destacan la importancia de proseguir los esfuerzos encaminados a defender y promover el marco de las Naciones Unidas sobre la conducta responsable de los Estados y trabajar en su aplicación, en particular mediante la creación del programa de acción para promover la conducta responsable de los Estados en el ciberespacio.

33. En consonancia con las Declaraciones conjuntas sobre la cooperación UE-OTAN, el Consejo invita al Alto Representante, también en su calidad de director de la AED, y a la Comisión a seguir reforzando, profundizando y ampliando la asociación en el ámbito cibernético con la OTAN, respetando plenamente los principios de inclusividad, reciprocidad, apertura mutua y transparencia, y con la autonomía decisoria de ambas organizaciones. Teniendo en cuenta la necesidad de garantizar esfuerzos complementarios y coordinados con la mayor implicación posible de los Estados miembros que no forman parte de la OTAN y evitar duplicaciones innecesarias, el Consejo pide que se establezcan vínculos a los niveles pertinentes entre la UE y la OTAN en el ámbito de la formación, la educación, la conciencia situacional, los ejercicios y las plataformas de I+D, y que se busquen posibles sinergias entre los respectivos compromisos voluntarios para el desarrollo de las capacidades nacionales de ciberdefensa y de los marcos de gestión de crisis, la protección de las infraestructuras críticas y el aumento de los intercambios de conciencia situacional, de respuestas coordinadas a las actividades cibernéticas malintencionadas y de esfuerzos de desarrollo de capacidades en terceros países. Esto incluye el acuerdo técnico entre la Capacidad de Respuesta ante Incidentes Informáticos de la OTAN (NCIRC) y el Equipo de Respuesta a Emergencias Informáticas - UE (CERT-UE), así como un diálogo político reforzado sobre cuestiones de ciberdefensa a todos los niveles.

V. **Conclusión**

34. Basándose en las Conclusiones del Consejo sobre la política de ciberdefensa de la UE, el Consejo pide al Alto Representante y a la Comisión que elaboren un plan de ejecución de la política antes del segundo trimestre de 2023, para su aprobación por los Estados miembros. Asimismo, el Consejo invita a los Estados miembros a que expongan voluntariamente su nivel de ambición y sus acciones en relación con la ciberdefensa en el contexto de la política de ciberdefensa de la UE y a que hagan pleno uso de las recomendaciones y compromisos voluntarios no vinculantes para intensificar sus esfuerzos nacionales y multinacionales en materia de ciberdefensa con el fin de maximizar el impacto a escala de la UE. Se invita al Alto Representante, a la Comisión y a los Estados miembros a que informen y debatan anualmente sobre los avances en la aplicación de los elementos de la Comunicación conjunta y su plan de ejecución a partir del segundo trimestre de 2024.