



TEXTOS APROBADOS

P10_TA(2026)0303

Guerra híbrida y protección de la integridad territorial y las infraestructuras críticas de seguridad y defensa de la Unión

Resolución del Parlamento Europeo, de 16 de septiembre de 2026, sobre la guerra híbrida y la protección de la integridad territorial y las infraestructuras críticas de seguridad y defensa de la Unión (2026/2024(INI))

El Parlamento Europeo,

- Vistos la Carta de las Naciones Unidas y los principios fundamentales del Derecho internacional,
- Visto el título V del Tratado de la Unión Europea (TUE), y en particular su capítulo 2, sección 2, relativa a las disposiciones sobre la política común de seguridad y defensa,
- Visto el Tratado de Funcionamiento de la Unión Europea (TFUE),
- Vistos el artículo 42, apartado 7, y el artículo 222, del TUE,
- Vistas sus anteriores Resoluciones sobre Ucrania, Rusia y Bielorrusia, en particular las adoptadas desde la anexión de la península de Crimea por parte de Rusia en febrero de 2014 y la invasión a gran escala de Ucrania por parte de Rusia en febrero de 2022,
- Visto el marco jurídico internacional para la prevención y la lucha contra el terrorismo, incluida la Resolución 2341 del Consejo de Seguridad de las Naciones Unidas sobre la protección de las infraestructuras vitales contra los atentados terroristas, aprobada el 13 de febrero de 2017,
- Visto el Reglamento (UE) 2019/452 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, por el que se establece un marco para el control de las inversiones extranjeras directas en la Unión¹,
- Visto el documento titulado «Una Brújula Estratégica para la Seguridad y la Defensa - Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales», aprobado por el Consejo el 21 de marzo de 2022 y refrendado por el Consejo Europeo el 25 de marzo de 2022,
- Vistas las Conclusiones del Consejo, de 21 de junio de 2022, sobre un marco para una respuesta coordinada de la UE a las campañas híbridas,

¹ DO L 79 I de 21.3.2019, p. 1, ELI: <http://data.europa.eu/eli/reg/2019/452/oj>.

- Vista la Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo²,
- Visto el informe de evaluación final del Grupo de Trabajo UE-OTAN, de 29 de junio de 2023, sobre la resiliencia de las infraestructuras críticas,
- Visto el informe de Sauli Niinistö, de 30 de octubre de 2024, titulado «Safer Together – Strengthening Europe’s Civilian and Military Preparedness and Readiness» (Más seguros juntos: fortalecimiento de la respuesta y la preparación civil y militar de Europa) (informe Niinistö),
- Vista la Comunicación de la Comisión, de 11 de diciembre de 2024, sobre la lucha contra las amenazas híbridas derivadas de la instrumentalización de la migración y sobre el refuerzo de la seguridad en las fronteras exteriores de la UE (COM(2024)0570),
- Visto el Reglamento (UE) 2025/37 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se modifica el Reglamento (UE) 2019/881 en lo que se refiere a los servicios de seguridad gestionados³,
- Visto el Reglamento (UE) 2025/38 del Parlamento Europeo y del Consejo, de 19 de diciembre de 2024, por el que se establecen medidas destinadas a reforzar la solidaridad y las capacidades en la Unión a fin de detectar ciberamenazas e incidentes, prepararse y responder a ellos y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de Cbersolidaridad)⁴,
- Vista la Comunicación conjunta de la Comisión y de la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 21 de febrero de 2025, titulada «Plan de Acción de la UE sobre la seguridad de los cables» (JOIN(2025)0009),
- Vista su Resolución, de 12 de marzo de 2025, sobre el Libro Blanco sobre el futuro de la defensa europea⁵,
- Visto el Libro Blanco Conjunto de la Comisión y de la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 19 de marzo de 2025, titulado «Libro Blanco Conjunto “Preparación en materia de defensa europea 2030”» (JOIN(2025)0120),
- Vista la Comunicación conjunta de la Comisión y de la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad, de 26 de marzo de 2025, sobre la Estrategia de Preparación de la Unión Europea (JOIN(2025)0130),
- Vista la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, de 1 de abril de 2025, titulada «ProtectEU: una Estrategia Europea para la Seguridad Interior» (COM(2025)0148),
- Vista la Declaración de la Cumbre del Consejo del Atlántico Norte celebrada en La

² DO L 333 de 27.12.2022, p. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>.

³ DO L, 2025/37, 15.1.2025, ELI: <http://data.europa.eu/eli/reg/2025/37/oj>.

⁴ DO L, 2025/38, 15.1.2025, ELI: <http://data.europa.eu/eli/reg/2025/38/oj>.

⁵ DO C, C/2025/3151, 20.6.2025, ELI: <http://data.europa.eu/eli/C/2025/3151/oj>.

Haya, adoptada por los jefes de Estado o de Gobierno participantes en la reunión del Consejo del Atlántico Norte el 25 de junio de 2025,

- Vista su Resolución, de 9 de octubre de 2025, sobre una respuesta unida a las recientes violaciones del espacio aéreo y las infraestructuras críticas de los Estados miembros de la Unión por parte de Rusia⁶,
 - Visto el documento oficioso del ministro de Defensa italiano, de noviembre de 2025, titulado «Countering hybrid warfare: an active strategy» (Lucha contra la guerra híbrida: una estrategia activa),
 - Vista la propuesta de la Comisión, de 10 de diciembre de 2025, relativa a orientaciones sobre las infraestructuras energéticas transeuropeas (COM(2025)1006),
 - Vista su Resolución, de 18 de diciembre de 2025, sobre los ataques híbridos continuos de Bielorrusia contra Lituania⁷,
 - Vista la Comunicación de la Comisión, de 18 de febrero de 2026, titulada «Comunicación sobre las regiones orientales de la UE fronterizas con Rusia, Bielorrusia y Ucrania: unas regiones fuertes para una Europa segura» (COM(2026)0082),
 - Vista su Resolución, de 21 de enero de 2026, sobre la aplicación de la política común de seguridad y defensa: informe anual 2025⁸,
 - Vistas las Conclusiones del Consejo, de 16 de marzo de 2026, sobre el desarrollo de la capacidad de la Unión Europea para luchar contra las amenazas híbridas,
 - Visto el artículo 55 de su Reglamento interno,
 - Visto el informe de la Comisión de Seguridad y Defensa (A10-0212/2026),
 - Vista la Declaración de la Cumbre del Consejo del Atlántico Norte, adoptada por los jefes de Estado o de Gobierno participantes en la reunión del Consejo del Atlántico Norte celebrada en Ankara el 8 de julio de 2026,
- A. Considerando que la intensidad y el alcance de los ataques híbridos contra la Unión se han intensificado significativamente desde el inicio de la guerra de agresión de Rusia contra Ucrania, con incidentes relacionados reiteradamente con Estados autoritarios, en particular Rusia, Bielorrusia, China, Irán y Corea del Norte;
- B. Considerando que Rusia representa la principal y más importante amenaza para la seguridad de la Unión y sus Estados miembros; que Rusia ha violado repetidamente el principio de integridad territorial e independencia política establecido en el artículo 2, apartado 4, de la Carta de las Naciones Unidas; que los ataques híbridos representan una amenaza para la democracia en la Unión y sus Estados miembros;
- C. Considerando que la gravedad de estos ataques ha aumentado drásticamente y que estos representan una flagrante violación de la soberanía de los Estados miembros, la integridad territorial de la Unión y el Derecho internacional; que la guerra híbrida se ha

⁶ DO C, C/2026/1530, 15.4.2026, ELI: <http://data.europa.eu/eli/C/2026/1530/oj>.

⁷ DO C, C/2026/2161, 6.5.2026, ELI: <http://data.europa.eu/eli/C/2026/2161/oj>.

⁸ Textos Aprobados, P10_TA(2026)0013.

convertido en una característica estructural del entorno geopolítico actual;

- D. Considerando que los recientes ataques híbridos pueden incluir incursiones no autorizadas de drones, «globos de contrabando», violaciones del espacio aéreo, túneles clandestinos para la infiltración y el tráfico ilícito, sabotaje y espionaje dirigidos contra infraestructuras críticas de seguridad y defensa, sabotaje de cables submarinos e infraestructuras energéticas, interferencia intencionada del GPS y suplantación de señales de navegación, ciberataques, incendios provocados y tramas de asesinato, instrumentalización de la migración y la delincuencia organizada, captación de élites, inversión extranjera encubierta, coerción económica, exfiltración de datos y otros actos de subversión política y penetración económica, manipulación de información e injerencia por parte de agentes extranjeros e injerencia en los procesos políticos y electorales;
- E. Considerando que, en el verano de 2026, la Unión fue testigo de una intensificación de las actividades híbridas físicas y de los ataques en todo el territorio de la Unión; que esto incluyó un intento de ataque con drones con carga explosiva contra aeronaves de carga ucranianas en el aeropuerto de Leipzig/Halle (Alemania), un intento de ataque con un dron marítimo con carga explosiva contra un proyecto rumano de gas marítimo, una trama frustrada de sabotaje y espionaje dirigida por Rusia contra infraestructuras militares y aeronaves de carga ucranianas en Rumanía, un ataque incendiario contra un contratista de defensa en Estonia, el sabotaje deliberado y ataques incendiarios contra instalaciones de defensa y fabricación de drones en Polonia, la violación del espacio aéreo polaco por parte de un misil de crucero ruso y su estrellamiento en la región de Lublin, y una trama incendiaria en Eslovaquia contra un fabricante ucraniano de drones; que el ataque al aeropuerto de Leipzig/Halle, al ataque contra el proyecto rumano de gas marítimo y la trama de sabotaje contra infraestructuras militares y aviones de carga ucranianos en Rumanía han sido atribuidos públicamente a Rusia por las respectivas autoridades nacionales; que, tras el ataque contra el aeropuerto de Leipzig/Halle, las autoridades alemanas cerraron el consulado ruso en Bonn y la Casa Rusa en Berlín;
- F. Considerando que la soberanía y la integridad territorial de todos los Estados miembros son principios fundacionales de la Unión; que los agentes estatales hostiles, en particular Rusia, atacan la integridad territorial de la Unión en dos frentes: mediante ataques físicos directos contra los Estados miembros y mediante operaciones de influencia destinadas a socavar la unidad de la Unión, impulsando la retirada de Estados miembros de la Unión;
- G. Considerando que las amenazas híbridas afectan cada vez más a la Unión en su conjunto, incluidos los países y territorios de ultramar, como Groenlandia, pero que las regiones fronterizas exteriores de la Unión y las zonas marítimas de la Unión están especialmente expuestas a los ataques; que estos ataques también se dirigen contra países candidatos y vecinos de la Unión, en particular Ucrania, Moldavia, Armenia, Georgia y los Balcanes Occidentales; que la integridad territorial de la vecindad de la Unión es fundamental para garantizar la paz, la estabilidad y la seguridad en Europa y el resto del mundo;
- H. Considerando que la injerencia de terceros países en Groenlandia, en especial los discursos incendiarios y la realización de actos híbridos en territorio groenlandés, así como la formulación de amenazas explícitas contra la soberanía de Groenlandia por parte del Gobierno de los Estados Unidos, han suscitado preocupación en relación con la soberanía y la integridad territorial de Groenlandia;

- I. Considerando que Georgia es un ejemplo de injerencia híbrida rusa de éxito que ha dado lugar a que las autoridades lideradas por Sueño Georgiano y alineadas con el Kremlin reproduzcan el manual ruso de operaciones híbridas contra la propia sociedad civil y las instituciones democráticas de Georgia;
- J. Considerando que las actividades de sabotaje por parte de los servicios de inteligencia rusos se llevan a cabo cada vez más a través de intermediarios, grupos vulnerables de la sociedad, incluidos menores de edad, representantes y «agentes desechables», lo que complica la atribución y la respuesta; que las instituciones religiosas, incluida la Iglesia ortodoxa rusa y las redes vinculadas a los Hermanos Musulmanes, se han explotado para llevar a cabo operaciones de injerencia en la Unión, socavando los valores democráticos, el Estado de Derecho y la capacidad de la Unión para defenderse;
- K. Considerando que estos ataques no solo tienen por objeto crear caos y desestabilizar a los Estados miembros de la Unión, sino también socavar la integridad democrática, exacerbar las divisiones políticas y debilitar la cohesión social, manipular los procesos de toma de decisiones, sembrar el miedo y la desconfianza pública entre los ciudadanos de la Unión, debilitar la preparación en materia de defensa y el apoyo de la Unión a Ucrania, lo que genera efectos en cascada en toda la Unión;
- L. Considerando que la invocación del artículo 5 de la OTAN tras los atentados terroristas del 11 de septiembre demuestra que la defensa colectiva puede activarse no solo a raíz de acciones de un agente estatal, sino también por ataques en los que participen agentes no estatales y redes complejas que operan más allá de las fronteras nacionales; que este precedente pone de relieve la naturaleza cambiante de las amenazas para la seguridad y la necesidad de adaptar los mecanismos de respuesta colectiva en consecuencia, también mediante la mejora de las normas y procedimientos comunes de atribución;
- M. Considerando que se ha producido un aumento drástico de la guerra cognitiva junto con la manipulación de información e injerencia por parte de agentes extranjeros; que, según el cuarto informe anual del Servicio Europeo de Acción Exterior (SEAE) sobre amenazas en materia de manipulación de información e injerencia por parte de agentes extranjeros, se espera que las actividades de manipulación de información e injerencia por parte de Rusia se intensifiquen en 2026, con un presupuesto para los medios de comunicación controlados por el Estado que se prevé que alcance aproximadamente los 1 560 000 000 EUR, un 7 % más que en 2025, y que las regiones del mar Báltico y del Ártico figuren entre los principales objetivos;
- N. Considerando que las operaciones de manipulación de información e injerencia por parte de agentes extranjeros utilizan métodos cognitivo-psicológicos sofisticados, incluido el control reflexivo, una técnica arraigada en la teoría militar soviética que introduce aportaciones informativas específicas para limitar las opciones percibidas por el objetivo y orientar las decisiones hacia los objetivos estratégicos del influyente;
- O. Considerando que las estrategias de seguridad nacional de Rusia de 2015 y 2021 enmarcan la promoción de los denominados «valores tradicionales» y del «mundo ruso» como instrumentos de su estrategia más amplia de guerra híbrida y su influencia geopolítica; que Rusia ha desplegado estratégicamente relatos históricos, religiosos, culturales y basados en valores como parte de su estrategia de guerra híbrida para influir en el discurso público y en las dinámicas eclesásticas, debilitar la cohesión social y socavar la resiliencia democrática y la integración transatlántica;

- P. Considerando que el carácter transversal del ámbito cognitivo requiere que los indicadores cognitivos se integren plenamente en la visión operativa común que utilizan las estructuras cibernéticas, de inteligencia, policiales, militares y de infraestructuras críticas;
- Q. Considerando que el éxito de las operaciones militares modernas y la eficacia de las instituciones públicas dependen cada vez más del control del ciberespacio y del uso estratégico de los recursos digitales y sistemas de información;
- R. Considerando que la seguridad interior sigue siendo responsabilidad de los Estados miembros, si bien el carácter transfronterizo, interconectado y multidimensional de estos ataques híbridos requiere una cooperación reforzada, un intercambio sistemático de información y una acción coordinada a escala de la Unión, con el apoyo de una financiación adecuada y complementados con estrategias a largo plazo destinadas a reforzar la resiliencia de la sociedad y proteger la integridad institucional;
- S. Considerando que las agencias de la Unión que actúan en el ámbito de la Justicia y los Asuntos de Interior (JAI) tienen un papel clave que desempeñar, en cooperación con las autoridades nacionales, en el establecimiento y el mantenimiento de una conciencia situacional común de los riesgos relacionados con dichas amenazas y en la asistencia a los Estados miembros situados en primera línea en situaciones de crisis; que la Comisión ha incluido el refuerzo de la Agencia Europea de la Guardia de Fronteras y Costas (Frontex) en sus iniciativas emblemáticas para la legislatura 2024-2029, así como una revisión de los mandatos de la Agencia de la Unión Europea para la Cooperación Policial (Europol) y de la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust); que otras iniciativas, como la «guardia del flanco oriental», pueden contribuir a reforzar la protección de las fronteras exteriores y aumentar la resiliencia frente a las amenazas híbridas;
- T. Considerando que la aparición de sistemas avanzados de IA constituye una perturbación estructural de las arquitecturas de ciberseguridad existentes, lo que invalida los modelos de amenazas y los supuestos defensivos desarrollados en décadas anteriores; que los agentes estatales y no estatales hostiles ya están aprovechando las capacidades de IA para aumentar la rapidez, la escala y la precisión de las operaciones híbridas, incluidas las intrusiones cibernéticas, el envenenamiento de datos de IA, las campañas de desinformación y los ataques contra infraestructuras críticas; que los marcos de ciberresiliencia colectiva de la Unión deben adaptarse para afrontar estas nuevas vulnerabilidades;
- U. Considerando que, a pesar de los importantes esfuerzos realizados por los Estados miembros y del desarrollo de herramientas y mecanismos para contrarrestar las amenazas híbridas, la respuesta de la Unión a los ataques híbridos sigue presentando lagunas legislativas, la falta de un enfoque armonizado entre los Estados miembros, diferentes niveles de sensibilización y la ausencia de una estructura o entidad específica para supervisar dichos ataques; que, en consecuencia, y a pesar de la urgencia, los Estados miembros de la Unión aún no han desarrollado una respuesta plenamente coordinada y coherente a la guerra híbrida, tanto a nivel individual como europeo y, en caso necesario, con la OTAN;
- V. Considerando que el gasto nacional en defensa se beneficiaría de una mayor coordinación y puesta en común entre los Estados miembros o de una mayor inversión en proyectos colaborativos europeos; que los aumentos significativos del gasto en

defensa de los Estados miembros, en combinación con las iniciativas de defensa de la Unión, como SAFE y otras medidas en el marco de la preparación en materia de defensa europea para 2030, están empezando a abordar carencias persistentes en materia de capacidades, pero que se requiere una transformación más rápida en capacidades operativas concretas para proteger mejor a la Unión, a sus Estados miembros y a sus ciudadanos frente a las amenazas híbridas; que, en este ámbito, sigue habiendo potencial para las tecnologías de doble uso; que también se necesita una respuesta adicional en el ámbito de la seguridad interior;

- W. Considerando que la responsabilidad de la seguridad nacional recae principalmente en los Estados miembros y que cualquier medida e iniciativa coordinada o propuesta a nivel de la Unión debe formularse y aplicarse respetando plenamente las competencias exclusivas de los Estados miembros y ajustarse a los conjuntos de instrumentos de la Unión de ciberdiplomacia, contra las amenazas híbridas y contra la manipulación de información e injerencia por parte de agentes extranjeros;
- X. Considerando que la dependencia de la Unión respecto de agentes extranjeros y tecnologías de fabricación extranjera en infraestructuras y cadenas de suministro críticas, incluido el abastecimiento de materias primas procedentes de terceros países, constituye una de las vulnerabilidades más importantes de la Unión y un reto clave para la seguridad y la autonomía estratégica europeas;
- Y. Considerando que el actual entorno de seguridad al que se enfrenta la Unión se caracteriza por no ser ni un estado de paz ni un conflicto armado abierto, sino una guerra de fase cero en la que los adversarios utilizan instrumentos híbridos para aprovechar la brecha existente entre las estructuras de gobernanza de la Unión en tiempos de paz y la firmeza necesaria para disuadir y responder; que los marcos de política exterior y de seguridad de la Unión existentes, diseñados para una deliberación basada en el consenso, generan una latencia estructural que los adversarios aprovechan activamente; que esta situación intermedia exige una reevaluación fundamental de la arquitectura de toma de decisiones de la Unión en el ámbito de la seguridad y la defensa;
- Z. Considerando que la credibilidad de la disuasión se basa no solo en las capacidades materiales y la ventaja tecnológica de las fuerzas europeas y aliadas, sino también, de manera decisiva, en la voluntad política, la cohesión estratégica y una comprensión común de la amenaza; que la estrategia híbrida de Rusia está diseñada para socavar precisamente estas cualidades, mediante la ambigüedad, la división y la presión subumbral, con el fin de mermar la credibilidad de los compromisos de defensa colectiva antes de alcanzar cualquier tipo de umbral cinético;

Guerra híbrida: entre la guerra y la paz

1. Destaca que las operaciones híbridas son actos deliberados, combinados, basados en la inteligencia y coordinados por parte de Estados, también a través de agentes no estatales, intermediarios y representantes, que abarcan simultáneamente múltiples ámbitos; subraya que están concebidos para parecer incidentes aislados y mantenerse por debajo del umbral de conflicto armado, aunque pueden producir efectos comparables a las agresiones convencionales, lo que dificulta considerablemente la atribución y la respuesta efectiva; pide a la Unión y a los Estados miembros, por tanto, que reconozcan que la guerra híbrida puede constituir una forma de guerra, con independencia de si se emplea la fuerza convencional;

2. Subraya que el objetivo principal de la guerra híbrida es desestabilizar, dividir y socavar la Unión y sus Estados miembros aprovechando las vulnerabilidades sistémicas y debilitando su seguridad, resiliencia y fundamentos democráticos, así como su preparación en materia de defensa, perturbando la base industrial de la defensa y las infraestructuras críticas de la Unión, socavando el apoyo público y político a la defensa de la Unión y reforzando las fuerzas políticas favorables a los autores mediante la injerencia sistemática en los procesos democráticos;
3. Afirmar que Rusia, actuando directamente o a través de múltiples representantes, como Bielorrusia, es el agente estatal que representa la mayor amenaza híbrida contra la Unión y sus Estados miembros; observa que China, Irán, Corea del Norte y otros países han estado llevando a cabo campañas híbridas destinadas a socavar las democracias europeas y erosionar los intereses de seguridad de la Unión; subraya que la Unión debe adoptar un enfoque integral frente a las amenazas híbridas que aborde no solo las actividades rusas y bielorrusas, sino también el creciente papel estratégico de China, Irán y Corea del Norte a la hora de facilitar y amplificar las acciones hostiles contra los intereses y la seguridad europeos; observa con preocupación que los agentes no estatales, incluidos los grupos terroristas, las redes de delincuencia organizada, las redes oligárquicas y cleptocráticas, las instituciones religiosas y las redes profesionales, las empresas militares privadas, los movimientos extremistas y los operadores que ofrecen servicios de influencia por contrato, también pueden llevar a cabo o facilitar campañas híbridas contra las democracias europeas;
4. Pide a la Comisión y al Consejo que evalúen la adecuación de los marcos jurídicos vigentes de la Unión para hacer frente a las amenazas híbridas, colmar las lagunas detectadas y tratar las operaciones híbridas subumbral que no puedan abordarse únicamente mediante la aplicación de la ley como cuestiones de seguridad colectiva, requiriendo una respuesta combinada civil-militar;

Guerra de la información, seguridad cognitiva y resiliencia social

5. Subraya que la guerra de la información es uno de los elementos fundamentales de la guerra híbrida; expresa su preocupación por la creciente magnitud de la guerra cognitiva, junto con la manipulación de información e injerencia por parte de agentes extranjeros, cuyo objetivo es erosionar la confianza social en las instituciones democráticas, aumentar la polarización, socavar la toma de decisiones democráticas y el apoyo público a la seguridad y la defensa europeas, incluido el apoyo a Ucrania;
6. Destaca que los objetivos mencionados (véase el apartado 5) se persiguen principalmente a través de operaciones sofisticadas y coordinadas que abarcan múltiples ámbitos de la vida social y utilizan técnicas cognitivas y psicológicas estratégicas diseñadas para configurar los procesos de toma de decisiones, la percepción individual y colectiva, la formación de la identidad, las normas culturales, la memoria histórica, los marcos morales y los sistemas de creencias religiosas, aprovechando al mismo tiempo las infraestructuras tecnológicas, los ecosistemas mediáticos y las vulnerabilidades económicas y políticas; observa con preocupación que las operaciones de manipulación de información e injerencia por parte de agentes extranjeros emplean métodos cognitivo-psicológicos sofisticados, incluido el control reflexivo, que son difíciles de detectar, atribuir o contrarrestar a través de respuestas convencionales; destaca, por tanto, que el conjunto de herramientas de la Unión contra la manipulación de información e injerencia por parte de agentes extranjeros debe integrar explícitamente

contramedidas contra estas técnicas avanzadas de influencia con el fin de salvaguardar la integridad de la toma de decisiones de la Unión;

7. Advierte de que determinados incidentes cinéticos pueden desencadenar o diseñarse deliberadamente para encubrir operaciones inmediatas, sincronizadas y orquestadas de manipulación de información e injerencia por parte de agentes extranjeros, en las que agentes hostiles aprovechen la brecha existente antes de que se emitan declaraciones oficiales para moldear la percepción pública; pide que esta brecha de información se aborde debidamente mediante una mejor coordinación europea, en particular mejorando la coordinación entre el sector público y el privado en el ámbito de la información; destaca la necesidad de desarrollar herramientas comunes, como manuales de comunicación, que permitan una comunicación más rápida, coordinada y precisa antes de que los discursos hostiles saturen el espacio de información;
8. Expresa su preocupación por el uso por Rusia del revisionismo histórico, en particular en relación con la Segunda Guerra Mundial y el legado soviético, la manipulación de información e injerencia por parte de agentes extranjeros y la reinterpretación selectiva de acontecimientos históricos como herramientas de guerra híbrida destinadas a polarizar la opinión pública, socavar la cohesión social y la resiliencia democrática y deslegitimar la integridad territorial de Estados soberanos;
9. Subraya que la manipulación de información e injerencia por parte de agentes extranjeros va más allá de los medios de comunicación tradicionales y abarca los ámbitos educativo, cultural y religioso; destaca el uso estratégico de instituciones religiosas y redes confesionales, incluida la instrumentalización de la Iglesia ortodoxa rusa, para proyectar autoridad moral, difundir discursos patrocinados por el Estado y socavar gradualmente la resiliencia social y la cohesión democrática; pide a la Unión, además, que detecte las amenazas híbridas que explotan canales religiosos y que forme a funcionarios de la Unión en el diálogo interconfesional y la alfabetización religiosa, así como en la detección de la influencia financiera, la captura organizativa y la manipulación de información que socavan los valores democráticos y la cohesión social;
10. Condena el uso de plataformas en línea por parte de agentes hostiles para actividades híbridas; pide una aplicación más estricta de las normas vigentes de la Unión sobre la transparencia de los sistemas de recomendación, la publicidad política, el comportamiento no auténtico coordinado y la rápida difusión de contenidos manipulados o generados por IA vinculados a injerencias extranjeras hostiles;
11. Subraya que los agentes hostiles emplean técnicas híbridas cada vez más sofisticadas y adaptativas; destaca que las herramientas de IA, como las ultrafalsificaciones, la amplificación algorítmica y las redes de cuentas automatizadas, hacen que estas operaciones de influencia sean más rápidas, baratas y difíciles de detectar; considera que la respuesta de la Unión a la manipulación de información e injerencia por parte de agentes extranjeros basada en la IA debe tratar la IA como un vector de amenaza y como una capacidad de defensa crítica;
12. Observa que la respuesta de la Unión a la manipulación de información e injerencia por parte de agentes extranjeros sigue siendo reactiva y carente de capacidades suficientes de seguimiento, atribución y respuesta proactiva en tiempo real; insiste en que la manipulación de información e injerencia por parte de agentes extranjeros debe tratarse como una amenaza grave para la seguridad que requiere un enfoque operativo y una

mejor coordinación y cooperación entre Estados miembros a todos los niveles, que incluya la detección temprana, opciones de respuesta adecuadas y una mayor protección de los procesos democráticos, en particular durante los períodos electorales;

13. Acoge con satisfacción el trabajo del SEAE en el seguimiento, la detección y la respuesta a la manipulación de información e injerencia por parte de agentes extranjeros y subraya la importancia del sistema de alerta rápida de la Unión para dar respuestas conjuntas coordinadas a la desinformación; pide a la Comisión y a los Estados miembros que evalúen las recomendaciones de la Comisión Especial sobre el Escudo Europeo de la Democracia (EUDS) y se basen en ellas; pide que se siga reforzando el sistema de alerta rápida para abordar la manipulación de la información en tiempo real con responsabilidades operativas claras; pide mecanismos normalizados de inmunización antibullos y respuesta rápida en toda la Unión y con los países socios, incluidos canales de comunicación estructurados de alerta temprana; alienta el desarrollo de herramientas de comunicación estratégica proactivas capaces de alertar con antelación a la población sobre las previsiones en cuanto a tácticas de desinformación, patrones narrativos y contenidos inventados antes de acontecimientos críticos, como elecciones, negociaciones de suministro de energía o crisis de seguridad;
14. Pide asimismo a la Comisión, a la alta representante y a los Estados miembros que pongan en pleno funcionamiento el conjunto de instrumentos contra la manipulación de información e injerencia por parte de agentes extranjeros y hagan un uso coherente y coordinado de este, y que apliquen el manual de disuasión de la manipulación de información e injerencia por parte de agentes extranjeros, entre otras cosas mediante la atribución pública coordinada y, cuando proceda, el uso de medidas restrictivas, dirigidas no solo a incidentes concretos, sino también a los flujos financieros ilícitos, la infraestructura técnica y las redes de intermediarios y representantes que sustentan las operaciones de manipulación de información e injerencia por parte de agentes extranjeros;
15. Destaca que la opinión pública europea sigue siendo el principal objetivo de las operaciones híbridas rusas; recuerda que décadas de paz han creado condiciones de complacencia estratégica que explotan y agravan las operaciones de influencia del adversario; considera que los Gobiernos y las instituciones de la Unión comparten la responsabilidad de sensibilizar a la ciudadanía sobre la naturaleza y la proximidad de la amenaza híbrida, y que el hecho de no hacerlo socava la preparación y la disuasión desde dentro;
16. Pide a los Estados miembros que adopten enfoques que impliquen al Gobierno y a la sociedad en su conjunto, dando prioridad a la resiliencia y la preparación, como se subraya en el informe Niinistö; recuerda que las amenazas híbridas se dirigen contra la sociedad en su conjunto, ya que los agentes hostiles aprovechan las vulnerabilidades en ámbitos, servicios, comunidades y espacios de información interconectados; considera que la confianza y la cohesión social son fundamentales para la resiliencia de la sociedad; subraya, por tanto, que la resiliencia frente a las amenazas híbridas debe ir más allá de las medidas militares, técnicas e institucionales, reuniendo a las autoridades públicas, el sector privado, la sociedad civil —incluidas las comunidades locales y las circunscripciones a las que es difícil llegar—, el mundo académico y los medios de comunicación independientes para reforzar la confianza democrática, la sensibilización pública y la preparación de la sociedad, fomentando así una nueva cultura de seguridad europea;

17. Destaca la necesidad de reforzar la resiliencia pública frente a la manipulación de información e injerencia por parte de agentes extranjeros a través de la educación cívica, la alfabetización mediática, las comunicaciones estratégicas, el apoyo a los medios de comunicación independientes, incluido el periodismo de investigación, las redes de verificación de datos, como el Observatorio Europeo de los Medios de Comunicación Digitales, y las herramientas basadas en la IA para detectar y analizar campañas de desinformación a gran escala; pide una cooperación más estrecha con los medios de comunicación y los agentes audiovisuales para detectar, atribuir y responder a la manipulación de información e injerencia por parte de agentes extranjeros; pide que se incentive, también a través de iniciativas público-privadas, la detección, el análisis y la atribución de la manipulación de información e injerencia por parte de agentes extranjeros, mecanismos seguros de intercambio de datos y sistemas interoperables de alerta temprana;
18. Expresa su preocupación por las continuas denuncias de injerencias extranjeras en las elecciones europeas, en particular a través de ciberataques y desinformación basada en la IA; recuerda que la integridad y la resiliencia de los procesos electorales ocupan un lugar central para los fundamentos democráticos de la Unión y son un objetivo clave de las operaciones híbridas; subraya que la manipulación de información e injerencia por parte de agentes extranjeros tiende a intensificarse antes de las elecciones y que, por tanto, la vigilancia y la coordinación continuas son esenciales para salvaguardar la integridad electoral y la estabilidad democrática en toda la Unión y en los países socios, incluidos los países candidatos y candidatos potenciales; acoge con satisfacción la Comunicación conjunta titulada «Escudo Europeo de la Democracia: empoderar democracias sólidas y resilientes» y la creación del Centro Europeo para la Resiliencia Democrática, y pide una definición clara de sus tareas con el fin de evitar duplicaciones con las iniciativas existentes;
19. Pide que se reconozcan y aborden las vulnerabilidades cognitivas en el contexto de la guerra híbrida en la próxima estrategia de seguridad de la Unión y que la Comisión adopte nuevas medidas proporcionando una cartografía de las vulnerabilidades cognitivas y parámetros de referencia en materia de resiliencia;

Ciberseguridad

20. Destaca que los ciberataques se han convertido en un elemento central de las campañas híbridas, aprovechando la creciente digitalización de sectores críticos como la asistencia sanitaria, las finanzas y la energía, causando perturbaciones en cascada con consecuencias económicas y sociales potencialmente graves;
21. Observa que el ciberespacio se ha convertido en el quinto ámbito militar y en un elemento de apoyo central de las amenazas híbridas; subraya que la creciente dependencia de las plataformas militares, las infraestructuras críticas y los sistemas de mando, control, comunicaciones e inteligencia respecto de las tecnologías digitales hace que la ciberseguridad sea esencial para la superioridad operativa y la resiliencia en todos los ámbitos; destaca, por tanto, la necesidad de contar con cibercapacidades soberanas de detección, atribución respuesta e inteligencia, incluidas las capacidades ofensivas para neutralizar las amenazas y asegurar una disuasión creíble;
22. Subraya la convergencia entre la manipulación de información e injerencia por parte de agentes extranjeros y la ciberseguridad, y señala que los ciberataques suelen producirse en las primeras fases de las campañas de manipulación de información e injerencia por

parte de agentes extranjeros; pide que los mecanismos de lucha contra la manipulación de información e injerencia por parte de agentes extranjeros se vinculen sistemáticamente con las capacidades de ciberseguridad, a fin de detectar, atribuir y desarticular la infraestructura de manipulación coordinada en una fase temprana;

23. Advierte de los riesgos que plantean las ciberoperaciones convergentes, en las que agentes alineados con Estados adoptan activamente los perfiles operativos, las metodologías y las identidades de «hacktivistas» independientes o ciberdelincuentes con motivaciones comerciales para ocultar la atribución y adaptar la actividad cibernética a los acontecimientos geopolíticos, las elecciones o las operaciones cinéticas; destaca que las respuestas a las ciberamenazas híbridas deben distinguir claramente entre las formas legítimas de expresión política o disidencia civil y la ciberdelincuencia con motivaciones económicas y las operaciones de patrocinio estatal, a fin de proteger las libertades fundamentales, mejorando al mismo tiempo la atribución, la rendición de cuentas y la disuasión;
24. Advierte de que la expansión de la internet de las cosas aumenta el riesgo de que los ciberataques generen efectos físicos en infraestructuras críticas y servicios esenciales, y pide obligaciones de seguridad desde el diseño para garantizar que los dispositivos conectados no se conviertan en puntos de entrada para operaciones híbridas con consecuencias en el mundo real;
25. Advierte de que no existe una protección cibernética plena y de que se necesita un cambio de mentalidad hacia la ciberresiliencia; destaca que la ciberresiliencia de Europa debe reforzarse mediante ejercicios cibernéticos frecuentes y realistas; subraya que la ciberresiliencia no solo se refiere a los sistemas, sino también a la protección de datos, que son a la vez un objetivo y un elemento de apoyo de las amenazas híbridas; subraya asimismo la necesidad de reforzar la ciberresiliencia en todo el tejido económico europeo, incluidas las pequeñas y medianas empresas (pymes) y los proveedores de servicios digitales esenciales;
26. Insiste en el valor añadido de la Unión a la hora de ayudar a los Estados miembros a conectar las capacidades nacionales, desarrollar una conciencia situacional común y permitir respuestas más rápidas y coherentes a las amenazas híbridas; recomienda que la Comisión estudie propuestas relativas a un marco más unificado para apoyar a los Estados miembros en la planificación, la coordinación operativa y la ejecución de las ciberoperaciones; acoge con satisfacción la finalización del proyecto de la Cooperación Estructurada Permanente (CEP) sobre el Centro de Coordinación del Ámbito del Ciberespacio y de la Información (CIDCC) y el progreso realizado en su transición hacia un Centro de Coordinación de la Ciberdefensa de la UE de carácter permanente;
27. Pide una mayor armonización de las obligaciones de notificación de incidentes y los conceptos jurídicos clave en todos los marcos de ciberseguridad y resiliencia de la Unión, con el fin de reducir la fragmentación, mejorar la interoperabilidad y garantizar que el rápido restablecimiento de los servicios esenciales siga siendo una prioridad central en los escenarios de crisis híbrida;
28. Reconoce que la Reserva de Ciberseguridad de la UE, gestionada por la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en el marco del Reglamento de Ciberseguridad, es una capacidad estratégica de respuesta rápida en materia de ciberseguridad de la Unión; pide que su financiación se adapte a la demanda operativa y destaca su primer despliegue en Moldavia como un paso importante para reforzar la

- ciberresiliencia operativa de la Unión y el apoyo a los países socios; pide a las autoridades de ciberseguridad de los Estados miembros que fomenten la cooperación estructurada con los proveedores de confianza de la Reserva, a fin de hacer pleno uso de las capacidades disponibles de respuesta a incidentes cuando las amenazas híbridas se materialicen a través de ciberincidentes significativos o a gran escala;
29. Reafirma la importancia de los Equipos de Respuesta Telemática Rápida de la CEP, y pide que la Unión los dote de recursos adecuados, como capacidad permanente de ciberdefensa, desplegable a petición de los Estados miembros, los países socios y las misiones de la política común de seguridad y defensa (PCSD) que se enfrenten a ciberataques con implicaciones para la seguridad y la defensa;
 30. Reitera la importancia de hacer pleno uso del conjunto de instrumentos de ciberdiplomacia para la prevención y disuasión de las ciberamenazas y las actividades maliciosas en el ciberespacio, y responder ante ellas; toma nota de la puesta en marcha, en marzo de 2026, del primer Mecanismo Mundial permanente de las Naciones Unidas sobre ciberseguridad, y considera que la Unión debe centrarse en los ámbitos en los que existe un claro valor añadido europeo, al tiempo que refuerza la ciberdiplomacia europea;
 31. Destaca que la ciberresiliencia y las medidas defensivas son insuficientes para garantizar una disuasión creíble contra las amenazas híbridas, como se destaca en el Libro Blanco Conjunto «Preparación en materia de defensa europea 2030»; pide a la Comisión y a los Estados miembros que, en cooperación con la OTAN, examinen los requisitos previos jurídicos, procedimentales y operativos para unas contramedidas cibernéticas proporcionadas y conformes con la legislación; acoge con satisfacción los progresos realizados hacia la creación del Centro de Coordinación de la Ciberdefensa de la UE y pide su rápida puesta en funcionamiento y la aplicación de un mandato en consonancia con las Conclusiones del Consejo sobre la política de ciberdefensa de la UE, con el fin de lograr una ciberdefensa de la Unión más creíble y capaz;
 32. Advierte, a este respecto, de que la IA no es solo una herramienta utilizada en actividades cibernéticas híbridas, sino también una tecnología crítica que puede ser objeto de ataques, manipulaciones o vulneraciones mediante inyección de instrucciones, envenenamiento de datos de entrenamiento y ataques a las cadenas de suministro; destaca que, dada la creciente dependencia de los sistemas de IA comerciales y de doble uso en contextos civiles, de seguridad y de defensa, la Unión debe desarrollar una postura clara sobre la ciberseguridad, la resiliencia y la gobernanza de la IA de doble uso, incluidas salvaguardias para la integridad de los modelos, unas cadenas de suministro fiables y la supervisión en el límite entre las aplicaciones civiles, de defensa y de seguridad nacional;
 33. Destaca la necesidad de una mayor protección de las infraestructuras digitales públicas críticas y los registros de datos sensibles gestionados por el Estado, incluidas las infraestructuras electorales, ya que constituyen posibles objetivos de amenazas híbridas, dado su papel en la identidad digital, la administración pública, la gobernanza de datos, las comunicaciones seguras, el acceso a servicios esenciales y la integridad de los procesos democráticos;

Infraestructuras críticas

34. Condena los ataques híbridos dirigidos contra las infraestructuras críticas de la Unión, en particular las infraestructuras de energía, transporte, comunicaciones y satélites, incluidas las de movilidad militar, que son tanto elementos de apoyo críticos como medios estratégicos para la defensa colectiva, la resiliencia y la protección civil de la Unión; destaca que esta infraestructura crítica opera como un sistema interconectado que no puede protegerse de forma aislada, y que una mayor conectividad digital aumenta la vulnerabilidad; acoge con satisfacción la atención prestada a la protección y la resiliencia de las infraestructuras energéticas y de movilidad militar en la propuesta de Reglamento sobre movilidad militar (COM(2025)0847) presentada por la Comisión y en la propuesta de la Comisión relativa a orientaciones sobre las infraestructuras energéticas transeuropeas (COM(2025)1006); pide a la Comisión y a los Estados miembros que adopten todas las medidas necesarias para garantizar su protección;
35. Subraya que el ámbito espacial se ha convertido en un escenario cada vez más importante para la guerra híbrida, en el que agentes hostiles atacan los sistemas de comunicación, navegación y observación por satélite mediante ciberoperaciones, ataques físicos, interferencias intencionadas y suplantación o la explotación de dependencias estratégicas; destaca que la perturbación de los medios espaciales puede tener consecuencias significativas para la seguridad civil, las infraestructuras críticas, la movilidad militar y las capacidades de respuesta a las crisis de la Unión; pide, por tanto, una mayor resiliencia de los sistemas espaciales de la Unión, incluyendo un incremento de la conciencia situacional espacial, la protección de las infraestructuras terrestres, los requisitos de ciberseguridad, la seguridad de la cadena de suministro, los ejercicios periódicos y las capacidades de posicionamiento, navegación y temporización (PNT) alternativas o de respaldo; pide asimismo la integración del ámbito espacial en el marco más amplio de la Unión para luchar contra las amenazas híbridas;
36. Observa que los agentes hostiles, principalmente Rusia, utilizan cada vez más las infraestructuras energéticas, los mercados de la energía y las dependencias energéticas como arma para ejercer presión política; hace hincapié en la importancia estratégica de las infraestructuras energéticas críticas tanto para las necesidades de defensa como para las civiles; insta a la Comisión y a los Estados miembros de la Unión a que establezcan un marco jurídico y financiero de la Unión en el próximo marco financiero plurianual 2028-2034 que garantice una protección y una resiliencia suficientes de las infraestructuras energéticas críticas, dando prioridad a las propuestas de la Comisión relativas a orientaciones sobre las infraestructuras energéticas transeuropeas (COM(2025)1006) y al Mecanismo «Conectar Europa» (COM(2025)0547);
37. Condena las actividades de la flota clandestina rusa que aumentan el riesgo de accidentes marítimos, ocultan sabotajes vinculados al Estado y ponen en peligro infraestructuras críticas como los cables submarinos, las instalaciones energéticas en alta mar y las instalaciones portuarias; pide que se refuercen las medidas de seguimiento, inspección y ejecución en aguas europeas y que la Unión intensifique su respuesta a las amenazas híbridas en las zonas marítimas; anima a la Comisión a que estudie, basándose en la iniciativa de seguridad contra la proliferación como modelo, marcos jurídicos y operativos que permitan el abordaje de buques vinculados a flotas clandestinas, y pide al Grupo de Acción Financiera Internacional que siga examinando el papel de las estructuras de propiedad opacas, los registros de pabellón y las redes financieras asociadas a la hora de facilitar la elusión de las sanciones y los flujos financieros ilícitos;

38. Destaca que los cables submarinos constituyen una vulnerabilidad estratégica clave y son objeto de sabotaje híbrido, espionaje y operaciones de influencia debido a su exposición física y a su potencial de perturbación sistémica, ya que transportan la gran mayoría del tráfico de internet intercontinental; elogia la Recomendación de la Comisión de 2024 sobre unas infraestructuras de cables submarinos seguras y resilientes⁹ y la Comunicación conjunta de 2025 titulada «Plan de Acción de la UE sobre la seguridad de los cables» (JOIN(2025)0009) como primeros pasos importantes hacia el refuerzo de la seguridad y la resiliencia de la infraestructura de cables submarinos; pide, además, capacidades de conciencia situacional marítima, que integren datos de sensores de satélites, de superficie y submarinos, para detectar, vigilar y atribuir las amenazas físicas a las infraestructuras de cables submarinos y a las infraestructuras energéticas en alta mar en zonas marítimas estratégicas, como el mar Báltico, el mar del Norte, el mar Negro y las regiones del Ártico y el Mediterráneo; recomienda establecer disposiciones estrictas en materia de responsabilidad penal para disuadir de tales ataques, así como sistemas redundantes para garantizar la resiliencia; destaca, además, la necesidad de un enfoque global y multinivel que combine la innovación tecnológica, una mayor integración de la inteligencia, la mejora de las capacidades de atribución y el refuerzo de la cooperación entre la OTAN, los Estados miembros de la Unión y los agentes pertinentes del sector privado con el fin de garantizar una protección coherente de la infraestructura submarina;
39. Pide a la Comisión y a los Estados miembros que establezcan una interpretación coordinada, a escala de la Unión, de la Convención de las Naciones Unidas sobre el Derecho del Mar (CNUDM), con el fin de garantizar una actuación coherente y una tipificación penal y una disuasión efectivas respecto de las actividades híbridas, los actos de sabotaje y las violaciones de los derechos soberanos en las zonas marítimas de la Unión, en particular en el mar Báltico, al tiempo que recuerda el objetivo de la CNUDM de garantizar el uso pacífico de los mares; anima a la Comisión y a los Estados miembros a que se basen en el ejemplo australiano de establecer las denominadas «zonas de protección de cables», proporcionar garantías jurídicas y tipificar penalmente los daños a los cables submarinos más allá del límite del mar territorial de doce millas náuticas, junto con un seguimiento, una vigilancia y una respuesta activos en cooperación con los socios pertinentes de terceros países;
40. Pide a los Estados miembros y a la Agencia Europea de Defensa (AED) que impulsen los proyectos de la CEP Protección de Infraestructuras Críticas Submarinas (CSIP), Protección y Vigilancia Marítima y Portuaria (HARMSPRO), Sistema Integrado Multinivel de Defensa Antiaérea y Antimisiles (IMLAMD) y Defensa contra Sistemas de Aeronaves No Tripuladas (C-UAS) para impulsar las capacidades de vigilancia, detección y defensa frente a las amenazas aéreas y marítimas; pide a la Comisión que, en cooperación con la alta representante y en consulta con los Estados miembros, proponga un proyecto europeo de interés común en el ámbito de la defensa dedicado a la defensa integrada del entorno marítimo y del fondo marino;

⁹ Recomendación (UE) 2024/779 de la Comisión, de 26 de febrero de 2024, sobre unas infraestructuras de cables submarinos seguras y resilientes (DO L, 2024/779, 8.3.2024, ELI: <http://data.europa.eu/eli/reco/2024/779/oj>).

41. Acoge con satisfacción la adopción de la Directiva relativa a la resiliencia de las entidades críticas (Directiva REC)¹⁰ y la Directiva SRI 2¹¹ como pasos importantes para reforzar la resiliencia contra los ataques híbridos, pero subraya que los retrasos en su aplicación en todos los Estados miembros representan una vulnerabilidad común urgente, y pide su aplicación plena y oportuna; insta a la Comisión a que haga pleno uso de sus competencias de seguimiento y ejecución; pide a los Estados miembros que integren la resiliencia desde el diseño como requisito estándar en toda la legislación nueva y revisada;
42. Expresa su preocupación por que infraestructuras críticas en la Unión sean de propiedad extranjera, en particular de Rusia y China, lo que aumenta considerablemente el riesgo de espionaje, injerencia y dependencia estratégica; acoge con satisfacción el acuerdo político alcanzado entre el Parlamento y el Consejo sobre un mecanismo reforzado de control de las inversiones extranjeras directas (IED) de la Unión; pide a los Estados miembros que apliquen rápidamente este Reglamento, complementándolo, cuando sea posible, con un enfoque de «compra de productos europeos» en lo que respecta a las infraestructuras críticas y los equipos de defensa, con vistas a reforzar la autonomía estratégica de la Unión;
43. Reconoce que una parte significativa de las infraestructuras críticas relacionadas con los servicios públicos esenciales y las capacidades militares es de propiedad privada o está gestionada por el sector privado; pide marcos de cooperación público-privada permanentes y estructurados, en particular para el intercambio de información, la planificación de contingencias y la respuesta coordinada a las crisis; destaca que, cuando las infraestructuras privadas apoyen servicios esenciales y datos sensibles, las autoridades públicas deben garantizar un control reglamentario y operativo eficaz; pide que los requisitos de defensa se integren sistemáticamente en la planificación, el diseño y la financiación de infraestructuras civiles; insiste en que las infraestructuras financiadas por la Unión deben cumplir las normas de resiliencia pertinentes en materia de defensa como condición para el apoyo de la Unión; pide, además, que los desarrolladores de tecnologías de defensa y los proveedores de seguridad participen sistemáticamente en las fases iniciales de la evaluación de las amenazas para las infraestructuras críticas y la planificación de contingencias, garantizando que las capacidades tecnológicas disponibles se reflejen en los marcos de resiliencia nacionales y de la Unión; reconoce la contribución de las pymes, las empresas emergentes y los proveedores de tecnologías innovadoras a la resiliencia y la protección de las infraestructuras críticas, y pide una mayor participación de estos en los programas, los sistemas de contratación pública y las asociaciones público-privadas pertinentes de la Unión;

¹⁰ Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (DO L 333 de 27.12.2022, p. 164, ELI: <http://data.europa.eu/eli/dir/2022/2557/oj>).

¹¹ Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) n.º 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) (DO L 333 de 27.12.2022, p. 80, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>).

44. Pide a los Estados miembros que lleven a cabo regularmente ejercicios de preparación y resiliencia para infraestructuras críticas, también ejercicios comunes, y proporcionen urgentemente las capacidades prioritarias señaladas en el Libro Blanco Conjunto «Preparación en materia de defensa europea 2030», en particular por lo que respecta a la defensa aérea y antimisiles, los drones y sistemas antidrones, la movilidad militar, la ciberseguridad, la guerra electrónica y las capacidades marítimas;
45. Manifiesta su preocupación por la dependencia estructural de la Unión de terceros países de alto riesgo, en particular China, para el suministro de programas y equipos informáticos conectados a la red, como inversores solares, turbinas eólicas, vehículos conectados y dispositivos digitales de consumo, que pueden acceder, transmitir o controlar sistemas a distancia y, por tanto, constituyen una vulnerabilidad significativa; pide a la Comisión que amplíe sistemáticamente las evaluaciones de la seguridad de la cadena de suministro en todos los sectores de infraestructuras críticas y que acelere los esfuerzos para reducir las dependencias estratégicas; pide a los Estados miembros que hagan un seguimiento de estas evaluaciones, diversifiquen las cadenas de suministro y den prioridad a los proveedores europeos y afines en los sectores estratégicos cuando así lo exijan consideraciones de seguridad; acoge con satisfacción que la propuesta de revisión del Reglamento sobre la Ciberseguridad tenga por objeto proporcionar un marco para prohibir los componentes conectados a la red que procedan de proveedores de alto riesgo, y que la hoja de ruta estratégica para la digitalización y la IA en el sector energético, como parte del paquete europeo de medidas de soberanía tecnológica, prevea una revisión del marco de seguridad del suministro energético; pide que estas medidas se adopten rápidamente;
46. Destaca la importancia de diversificar las rutas de suministro por medio de redes de transporte seguras y resilientes con socios de confianza con el fin de reducir las dependencias estratégicas y reforzar la seguridad económica y la resiliencia de la cadena de suministro de la Unión;
47. Destaca que las tecnologías críticas y emergentes, incluida la inteligencia artificial, la infraestructura en la nube, los semiconductores avanzados, las tecnologías cuánticas, los sistemas cibernéticos, espaciales y autónomos y las comunicaciones seguras, forman parte de las infraestructuras críticas de seguridad de la Unión, dado su papel esencial en la preparación en materia de defensa, la resiliencia económica y la continuidad operativa; considera que una infraestructura digital de la Unión resiliente y competitiva, que incluya centros de datos locales seguros, una nube soberana de la Unión, computación periférica y redes de gigabit, constituye un pilar importante de la seguridad europea; destaca que la capacidad de la Unión para detectar campañas híbridas y resistir y responder a ellas depende de su capacidad para desarrollar, asegurar y ampliar estas tecnologías dentro de una base industrial y tecnológica europea resiliente respaldada por una inversión suficiente de la Unión, incluida la inversión en sistemas de intercambio de información seguros, interoperables y resilientes y centros de datos locales no sujetos a legislación extraterritorial;

Conciencia situacional

48. Destaca que la lucha eficaz contra las amenazas híbridas requiere prevención, anticipación temprana de las amenazas y un seguimiento continuo de las vulnerabilidades estratégicas para neutralizar las acciones hostiles antes de que tengan efectos sistémicos, así como una visión compartida de las amenazas, ya que los sectores contra los que van dirigidos los ataques no pueden responder eficazmente sobre la base

de informes de incidentes aislados; destaca a este respecto el potencial valor añadido único de la Unión a la hora de agregar datos transfronterizos para detectar patrones de campañas híbridas coordinadas que ningún Estado miembro puede identificar por sí solo, así como a la hora de coordinar el desarrollo de procedimientos de conciencia situacional y atribución comunes, y de marcos, metodologías, taxonomías, protocolos de interoperabilidad comunes entre órganos y estructuras nacionales y de la Unión pertinentes que apoyen la cooperación operativa entre los Estados miembros; pide que estas funciones se reconozcan formalmente como competencias de coordinación y apoyo de la Unión;

49. Señala que la Célula de Fusión de la UE contra las Amenazas Híbridas, dentro de la Capacidad Única de Análisis de Inteligencia (SIAC), sigue siendo el organismo central de la Unión con conocimientos especializados exclusivos de análisis de todas las fuentes sobre las amenazas híbridas, lo que proporciona una conciencia situacional basada en la inteligencia; reitera que la SIAC debe ser el centro único para la inteligencia en las instituciones de la Unión y subraya su estatuto especial dentro de la arquitectura de seguridad de la Unión; respalda el análisis de tendencias en el ámbito de las amenazas híbridas como herramienta clave para analizar amenazas híbridas y detectar patrones, así como su integración adecuada en los procesos de elaboración de políticas;
50. Recuerda la falta de avances en el cumplimiento del objetivo previsto en la Brújula Estratégica y en el documento conjunto del alto representante y los Estados miembros sobre el refuerzo de la capacidad analítica única de la UE en materia de inteligencia (EEAS(2024)2014) de reforzar la SIAC suministrando recursos adicionales para compilar, analizar e integrar información pertinente con el fin de producir inteligencia en los ámbitos de las ciberamenazas y las amenazas híbridas a la Unión y facilitar su suministro eficiente; pide a la Comisión, a la alta representante y a los Estados miembros que se comprometan firmemente con el refuerzo efectivo de la SIAC;
51. Insta a los Estados miembros a que aumenten el intercambio de inteligencia, también con el INTCEN y la Dirección de Inteligencia del Estado Mayor de la Unión Europea (EMUE), respetando al mismo tiempo la soberanía de los Estados miembros, el principio de la necesidad de conocer y la protección de la información nacional clasificada; destaca que las evaluaciones basadas en datos e inteligencia deben incorporarse sistemáticamente en la planificación, la gestión de crisis y la elaboración de políticas de la Unión;
52. Pide a las instituciones de la Unión que, en cooperación con los Estados miembros y el SEAE, estudien la posibilidad de crear un sistema seguro de intercambio de información, basado en la necesidad de conocer y la necesidad de compartir, en el que la Unión actuaría como facilitadora conectando a las autoridades públicas, los organismos pertinentes nacionales, de la Unión e internacionales, los operadores de infraestructuras críticas, las empresas privadas y las fuentes fiables de información sobre amenazas, con el fin de reforzar la conciencia situacional colectiva, garantizando al mismo tiempo la máxima protección de la información delicada; considera que dicho sistema incentivaría a los organismos participantes a compartir información, al permitirles beneficiarse de una visión más completa de las amenazas y de productos de inteligencia de mayor calidad, al tiempo que generaría progresivamente la confianza necesaria para un intercambio de información significativo;

53. Pide la creación de un «Libro Negro de agresión híbrida por parte de Rusia, China y otros países» con el fin de documentar públicamente todas las operaciones híbridas contra la Unión y sus Estados miembros de los últimos diez años; insiste en que el «Libro Negro» se debata en el Consejo y se presente al Parlamento anualmente con el fin de imponer costes adicionales a los Estados en cuestión;

De la fragmentación a una respuesta europea coordinada y decisiva

54. Subraya que la Unión solo puede responder eficazmente a la escalada de las amenazas híbridas y convencionales mediante una mayor integración y coordinación y un incremento de la preparación y capacidades europeas en materia de defensa, en particular mediante un mayor desarrollo de la base tecnológica e industrial de la defensa europea;
55. Considera que la Unión debe pasar de una estrategia reactiva a una proactiva, lo que incluye utilizar sus capacidades para perturbar las amenazas híbridas, disuadirlas y responder a ellas y aumentar de forma creíble el coste de las acciones hostiles; subraya que toda violación de la soberanía de los Estados miembros debe ser objeto de medidas de represalia efectivas, proporcionadas y coordinadas;
56. Destaca que, para contrarrestar y disuadir eficazmente las amenazas híbridas, se requiere una visión de las amenazas compartida y exhaustiva, que depende de marcos, metodologías, taxonomías y normas operativas comunes; destaca la necesidad de combinar medidas diplomáticas, jurídicas, económicas y restrictivas para prevenir, detectar, identificar y atribuir las operaciones híbridas y responder a estas, también mediante medidas asimétricas en todos los ámbitos pertinentes; pide a la Comisión, a la alta representante y al Consejo que elaboren un plan de acción transversal contra la guerra híbrida, que incluya una cooperación civil-militar reforzada, manuales operativos, protocolos de respuesta colaborativos y eficientes, incluidas opciones de represalia calibradas de la Unión proporcionadas a la gravedad de las actividades hostiles y cadenas de respuesta claras que sean interoperables con las de la OTAN y las complementen, preservando al mismo tiempo la capacidad de la Unión y de los Estados miembros para actuar con independencia en caso necesario; solicita la designación de un punto único de coordinación entre la Comisión y el SEAE con el fin de establecer un verdadero enfoque de toda la Unión frente a las amenazas híbridas;
57. Acoge con satisfacción las iniciativas en curso para reforzar la capacidad operativa, incluidos los equipos de respuesta rápida de la Unión contra amenazas híbridas y la puesta en marcha de la guardia del flanco oriental de la Unión y la iniciativa europea de defensa antidrones; pide que se avance rápidamente en sus despliegues; destaca la importancia estratégica de las agrupaciones regionales de defensa y seguridad y pide líneas de financiación específicas de la Unión para integrar sus conocimientos técnicos y capacidades en proyectos transfronterizos que mejoren la resiliencia europea;
58. Acoge con satisfacción el anuncio de la Comisión y la alta representante de una nueva estrategia mundial de seguridad de la Unión y pide que aborde de manera exhaustiva todo el espectro de las amenazas híbridas;
59. Insiste en la necesidad de avanzar urgentemente hacia una auténtica Unión Europea de Defensa, como pilar europeo más sólido de la OTAN, separable pero no independiente, que permita a la Unión y a sus Estados miembros actuar con independencia cuando sea necesario; pide que la cláusula de defensa mutua (artículo 42, apartado 7, del TUE) se

aplique en mayor medida en situaciones de agresión armada e híbrida grave; pide, además, un manual con arreglo al artículo 42, apartado 7, esto es, una guía operativa concisa pero exhaustiva para los Gobiernos nacionales y las instituciones de la Unión, en la que se explique lo que ocurre antes, durante y después de que un Estado miembro invoque el artículo; sugiere que el manual se ponga a prueba periódicamente en situaciones de crisis híbridas graves y mediante ejercicios intersectoriales exhaustivos;

60. Destaca que algunos de los ataques híbridos de Rusia contra la Unión y sus Estados miembros podrían constituir terrorismo patrocinado por el Estado; anima a los Estados miembros a que utilicen todos los instrumentos jurídicos disponibles para contrarrestarlos, incluida la cláusula de solidaridad (artículo 222 del TFUE), haciendo pleno uso de los mecanismos de cooperación y coordinación disponibles cuando se active la cláusula;
61. Acoge con satisfacción la labor realizada en el marco de los regímenes de sanciones existentes contra las actividades híbridas, en particular el régimen de sanciones establecido en octubre de 2024 contra las actividades desestabilizadoras de Rusia y el régimen de sanciones horizontales contra los ciberataques establecido en 2019; lamenta que el marco de sanciones de la Unión sea complejo y esté fragmentado en diferentes vectores de amenazas híbridas; pide que se sigan reforzando las medidas restrictivas de la Unión en respuesta a las amenazas híbridas, en particular el establecimiento inmediato de un marco horizontal de sanciones de la Unión, concebido específicamente para las amenazas híbridas con el fin de colmar las lagunas en los regímenes existentes y aumentar el efecto disuasorio, que coexista con el régimen de sanciones en materia híbrida contra Rusia para poner de relieve la participación activa de este país en operaciones híbridas a escala mundial, al tiempo que permita imponer sanciones de forma más rápida y sistemática a las entidades responsables de las campañas híbridas; solicita que se sigan reforzando los conjuntos de instrumentos de la Unión contra las amenazas híbridas, contra la manipulación de información e injerencia por parte de agentes extranjeros y de ciberdiplomacia, y que se utilicen de manera más eficaz;
62. Reitera la necesidad de garantizar la rendición de cuentas por las operaciones híbridas y por parte de los responsables, incluidos los representantes que actúan en nombre de agentes estatales, haciendo pleno uso de las herramientas existentes y específicas; pide a la Unión y a los Estados miembros que adopten medidas urgentes para detener y perturbar los flujos financieros que financian ataques contra la democracia, en particular movilizándolo a los reguladores bancarios, los investigadores penales y las autoridades responsables de las sanciones para rastrear y examinar las fuentes ilícitas de financiación, incluidas las criptomonedas; solicita a la Unión y a los Estados miembros que eliminen los incentivos financieros y algorítmicos que permiten que prospere la desinformación, en particular abordando los vínculos entre la financiación ilícita, los ingresos publicitarios, los modelos de negocio de las plataformas basados en la captación de atención y los contenidos manipuladores;
63. Considera que deben aplicarse y, en su caso, seguir desarrollándose todos los instrumentos de Derecho penal disponibles a escala de los Estados miembros y de la Unión para prevenir y combatir las conductas ilegales destinadas a socavar las instituciones y los procesos democráticos; destaca la necesidad de que las autoridades nacionales competentes estén dotadas de herramientas y canales de cooperación adecuados para prevenir, investigar, detectar y enjuiciar los delitos relacionados con la injerencia extranjera; considera que la corrupción y la intimidación de cargos electos y funcionarios públicos por parte de redes delictivas deben abordarse como parte de la

respuesta de la Unión a las amenazas híbridas, mediante una cooperación reforzada entre los organismos especializados de lucha contra la corrupción, las autoridades policiales y los organismos pertinentes de la Unión; pide a la Comisión que evalúe el valor añadido de establecer en el Derecho de la Unión normas mínimas sobre la definición y las sanciones del delito de participación consciente en actividades organizadas de injerencia en nombre de potencias extranjeras; observa que la próxima revisión de los mandatos de las agencias de Justicia y Asuntos de Interior de la Unión brinda la oportunidad de reforzar la capacidad de respuesta operativa de la Unión; pide a la Comisión que estudie la idea de convocar una plataforma o grupo de trabajo para que los Estados miembros coordinen voluntariamente las respuestas legislativas nacionales y compartan buenas prácticas;

Consideraciones geográficas

64. Condena enérgicamente la instrumentalización de la migración por parte de terceros países o agentes no estatales hostiles con el fin de desestabilizar a Estados miembros o ejercer presión sobre la Unión; toma nota de las disposiciones específicas sobre la instrumentalización de la migración recientemente incluidas en actos legislativos clave de la Unión; toma nota de la revisión anunciada por la Comisión del mandato de Frontex; subraya que esta revisión debe proporcionar la base jurídica, las capacidades analíticas y los recursos humanos, financieros y técnicos adecuados necesarios, lo que también ayudaría a reforzar la respuesta de la Unión a las amenazas híbridas;
65. Condena enérgicamente el ataque a la frontera meridional de la Unión en la ciudad de Ceuta, perpetrado los días 30 y 31 de julio de 2026, así como la posterior invasión de la ciudad, que constituye un ataque a la integridad territorial y la soberanía de un Estado miembro; lamenta el uso de los flujos migratorios irregulares como instrumento de guerra híbrida dirigido contra la estabilidad y la seguridad de un Estado miembro, por lo que pide una investigación independiente y exhaustiva para aclarar la responsabilidad de la planificación y la ejecución de los ataques y determinar los objetivos perseguidos;
66. Condena las incursiones sistemáticas de drones y las provocaciones transfronterizas por parte de Rusia dirigidas contra los Estados miembros a lo largo del flanco oriental de la Unión como una campaña calculada de intimidación contra la población civil; acoge con satisfacción la Comunicación de la Comisión sobre las regiones orientales de la Unión fronterizas con Rusia, Bielorrusia y Ucrania, y su reconocimiento explícito de que las regiones fronterizas orientales de la Unión se enfrentan a amenazas estructurales y sostenidas por parte de Rusia y Bielorrusia; pide a la Comisión que traduzca este reconocimiento en flujos de financiación específicos en el marco financiero plurianual 2028-2034, incluida financiación específica para mejorar las capacidades de protección integrada de las fronteras y modernizar las infraestructuras físicas y digitales de vigilancia de las fronteras —en consonancia con las normas de la OTAN— en las fronteras terrestres exteriores de la Unión; subraya que debe prestarse especial atención a los sistemas avanzados de detección, seguimiento y contramedidas contra los sistemas aéreos no tripulados para proteger las infraestructuras críticas, como los aeropuertos, las instalaciones energéticas y los centros de transporte, y apoyar a los Estados miembros en el despliegue de sistemas interoperables conciencia situacional del espacio aéreo, medidas de protección electrónica y capacidades de respuesta rápida a incidentes; destaca que las medidas deben ser proporcionadas y defensivas y estar orientadas a la protección civil, garantizando la continuidad de los servicios esenciales y la libertad de circulación dentro del espacio Schengen;

67. Destaca que las amenazas híbridas afectan cada vez más a la Unión en su conjunto, adoptando diferentes formas en las distintas regiones; destaca, a este respecto, la exposición de la región del mar Báltico, la región nórdico-báltica y la región del mar Negro a las amenazas contra la seguridad marítima y del espacio aéreo, así como a la instrumentalización de la migración, la vulnerabilidad de las regiones fronterizas mediterráneas y meridionales a las amenazas contra las infraestructuras marítimas, las redes energéticas, los corredores logísticos, las rutas de transporte estratégicas, las campañas de desinformación y la instrumentalización de los flujos migratorios, la exposición del sudeste de Europa a la coacción económica, las dependencias energéticas y la manipulación coordinada de la información vinculada a teatros vecinos, la vulnerabilidad específica de los principales espacios de información urbanos y digitales de toda la Unión a la guerra cognitiva, la polarización y las injerencias extranjeras; subraya la creciente importancia estratégica de la región del Ártico para la seguridad europea, incluida la protección de las infraestructuras críticas, la libertad de navegación, las comunicaciones por satélite y los corredores de transporte emergentes; pide a la Unión y a la OTAN que reflejen la geografía de las amenazas híbridas en sus estrategias, en particular en la próxima estrategia de seguridad de la Unión, manteniendo al mismo tiempo un enfoque de seguridad completo con respecto a la resiliencia, la preparación y la respuesta; destaca que la financiación para luchar contra las amenazas híbridas debe basarse en la exposición estratégica, las necesidades operativas y las vulnerabilidades demostradas, al mismo tiempo que se garantiza el apoyo a todas las regiones que se enfrentan a amenazas híbridas;

Coordinación y cooperación entre la Unión y la OTAN

68. Reafirma que la OTAN sigue siendo la piedra angular de la defensa colectiva de sus miembros; pide una mayor cooperación entre la Unión y la OTAN para reforzar la preparación, la resiliencia y la disuasión de Europa frente a las amenazas híbridas; destaca, a este respecto, la importancia de la protección de las infraestructuras críticas, la movilidad militar, la ciberresiliencia y la preparación; subraya la necesidad de un intercambio más sistemático de las lecciones aprendidas de la guerra en Ucrania en el ámbito híbrido;
69. Destaca que la acción de la Unión y de la OTAN en el ámbito híbrido debe ser complementaria, reforzarse mutuamente y coordinarse desde el punto de vista operativo, garantizando al mismo tiempo la capacidad de la Unión para actuar cuando sea necesario, en el contexto de la armonización de los requisitos mínimos de la Unión en materia de preparación con los requisitos básicos de la OTAN;
70. Observa que la estrategia híbrida revisada de la OTAN de 2025 supone un cambio de la resiliencia a la disuasión activa; acoge con satisfacción las opciones de respuesta militar acordadas previamente y la ampliación de las competencias del Comandante Supremo Aliado en Europa (SACEUR) para permitir una actuación más rápida al inicio de un ataque híbrido, reduciendo así los retrasos entre la detección de amenazas y la respuesta, al tiempo que se mantiene la supervisión política;
71. Acoge con satisfacción el Mecanismo de Seguimiento de las Amenazas Híbridas de la OTAN, una herramienta de agregación de inteligencia a través de la División Conjunta de Inteligencia y Seguridad de la OTAN, que proporciona a los aliados una visión consolidada de las amenazas, basada en los servicios nacionales de inteligencia; reconoce la cooperación continua entre la OTAN y la Unión en el ámbito de la inteligencia, y pide a la Comisión y al SEAE que establezcan una interfaz estructurada

dentro de la Célula de Fusión contra las Amenazas Híbridas con este mecanismo, de modo que la conciencia situacional de la Unión y la visión de amenazas híbridas de la OTAN se armonicen periódica y sistemáticamente;

72. Destaca el importante papel de las operaciones «Artic Sentry» (Centinela Ártica), «Baltic Sentry» (Centinela Báltica) y «Eastern Sentry» (Centinela Oriental) de la OTAN como instrumentos ágiles a la hora de responder a las amenazas híbridas dentro de plazos pertinentes desde el punto de vista operativo, en particular por lo que respecta a la protección de las infraestructuras marítimas críticas y las rutas de suministro y el seguimiento de las actividades híbridas en esas regiones; observa que su eficacia se ve limitada por el elevado coste de interceptar drones, las lagunas en la conciencia situacional y la fragmentación de los marcos reglamentarios de la lucha contra los drones entre los Estados miembros; pide que se acelere la aplicación del plan de acción de la Unión sobre seguridad de drones y defensa antidrones, incluida la provisión de una financiación específica para capacidades de defensa multinivel en los Estados miembros situados en primera línea para luchar contra los globos meteorológicos y los drones cinética y electrónicamente, y que se armonice sistemáticamente el plan de acción con los requisitos operativos de la OTAN, garantizando capacidades de defensa contra los drones armonizadas y dotadas de recursos adecuados en todos los Estados miembros; apoya, además, una mayor cooperación en el desarrollo y la implantación de tecnologías rentables de defensa contra los drones en toda la Unión;
73. Acoge con satisfacción el marco de ejercicios paralelos y coordinados entre la Unión y la OTAN como instrumento valioso para poner a prueba y mejorar la capacidad, la magnitud y el alcance de la respuesta conjunta, así como para la integración sistemática de las lecciones extraídas en las políticas, la planificación y las disposiciones institucionales de la Unión; pide la realización de ejercicios periódicos de la Unión y la OTAN que simulen situaciones de ataques híbridos, como el sabotaje contra infraestructuras de movilidad militar, ciberataques coordinados, campañas de manipulación de información e injerencia por parte de agentes extranjeros a gran escala, violaciones del espacio aéreo y ataques contra infraestructuras críticas;
74. Pide a la Comisión y al SEAE que, en estrecha coordinación con la OTAN y los Estados miembros, desarrollen una interpretación común de las amenazas híbridas y establezcan un mecanismo de respuesta coherente para la Unión y la OTAN;
75. Reconoce el valioso papel que desempeñan los centros de excelencia especializados, como el Centro de Excelencia para la Lucha contra las Amenazas Híbridas (Helsinki) y el Centro de Excelencia para la Ciberdefensa Cooperativa de la OTAN (Tallin), a la hora de reforzar la preparación, la resiliencia, la ciberdefensa y las capacidades de lucha contra las amenazas híbridas en toda Europa; celebra también la labor del Grupo de Trabajo UE-OTAN sobre la resiliencia de las infraestructuras críticas, en particular en lo que se refiere al refuerzo de la cooperación en materia de energía, transporte, infraestructuras digitales y conectividad submarina;
76. Pide a los Estados miembros que armonicen sus legislaciones para colmar las lagunas jurídicas que impiden al personal aliado participar en operaciones de respuesta a las amenazas híbridas por debajo del umbral; acoge con satisfacción las enmiendas recientemente adoptadas por Estonia a su Ley de organización de fuerzas de defensa como un paso concreto en esta dirección;

Países socios: cooperación y apoyo

77. Subraya que las operaciones híbridas rusas más allá de la Unión tienen por objeto cambiar la política exterior de terceros países en consonancia con los intereses de Moscú, socavar las relaciones de la Unión con sus socios y debilitar el apoyo internacional a Ucrania; reitera, por tanto, la importancia de una estrecha cooperación con los socios y organizaciones internacionales para mejorar la conciencia situacional y prevenir, disuadir y responder de manera más eficaz a las amenazas híbridas; reconoce el valor de profundizar el diálogo y las consultas sectoriales bilaterales con socios afines en materia de amenazas híbridas, especialmente dentro del marco de las asociaciones de seguridad y defensa;
78. Hace hincapié en que el refuerzo de la cooperación con Ucrania, Moldavia, Armenia y los socios de los Balcanes Occidentales es una necesidad estratégica, ya que se enfrentan a ataques continuos de Rusia y constituyen bases de prueba clave para las tácticas híbridas de Rusia, combinando la manipulación de información e injerencia por parte de agentes extranjeros, las operaciones cibernéticas, las redes de influencia encubiertas, la coacción energética y la influencia basada en la corrupción para socavar las instituciones democráticas, la cohesión social y las perspectivas de integración en la Unión y la OTAN; pide a los Estados miembros que adopten las lecciones aprendidas de estos países y que establezcan mecanismos estructurados para el intercambio sistemático de mejores prácticas y experiencias operativas, incluida la capacidad de Ucrania para mantener los servicios esenciales, la continuidad del gobierno, la protección de las infraestructuras críticas, la comunicación estratégica y el funcionamiento y la resiliencia de la sociedad bajo ataques continuos; reitera su firme apoyo a la adhesión progresiva de Ucrania a la Unión y su adhesión a la OTAN una vez que se hayan cumplido las condiciones pertinentes;
79. Destaca la importancia estratégica de mantener y profundizar el apoyo a la resiliencia híbrida de los países candidatos, candidatos potenciales y socios, que a menudo son los principales objetivos de las actividades híbridas de Rusia y cuya resiliencia contribuye directamente a la seguridad de la Unión; acoge con satisfacción la contribución activa de la Unión y de los Estados miembros al refuerzo de su resiliencia a través del Servicio de Instrumentos de Política Exterior, las comunicaciones estratégicas, los equipos de respuesta rápida contra amenazas híbridas, el estudio sobre los riesgos híbridos y las misiones de la PCSD en países socios como Ucrania, Moldavia, Armenia y Montenegro; solicita la organización de ejercicios periódicos conjuntos, escenarios de simulación y programas de formación destinados a mejorar la preparación, potenciar las capacidades de respuesta rápida y fomentar la interoperabilidad a la hora de hacer frente a las amenazas híbridas; observa con satisfacción la respuesta coordinada de la Unión y la OTAN en Moldavia, incluido el despliegue paralelo de un equipo de respuesta rápida de la Unión contra amenazas híbridas y un equipo de apoyo contra amenazas híbridas de la OTAN con mandatos complementarios; anima a los países candidatos y candidatos potenciales a que se adapten plenamente a la política exterior y de seguridad común (PESC) de la Unión, incluidas las medidas restrictivas, como aspecto esencial del proceso de integración en la Unión;
80. Elogia a las fuerzas proeuropeas de Moldavia y Armenia por su resiliencia democrática durante sus elecciones parlamentarias de 2025 y 2026 y en el período inmediatamente anterior a estas, lo que demuestra una fuerte resistencia a las continuas campañas de manipulación de información e injerencia por parte de Rusia durante años; subraya la efectividad del enfoque que implica a todo el Gobierno como modelo operativo, incluido su uso de medidas policiales contra redes que llevan a cabo operaciones híbridas en nombre de Rusia; pide a los Estados miembros y a la Comisión que, en

cooperación con el SEAE, desarrollen marcos a escala de la Unión que permitan respuestas de ejecución comparables; señala el importante papel que desempeñan las instituciones de la Unión, las instituciones estatales, la sociedad civil y los medios de comunicación independientes en la lucha contra la manipulación de información e injerencia por parte de agentes extranjeros, incluidas las campañas coordinadas de manipulación de la información a gran escala basadas en la IA que contribuyen al elevado nivel de concienciación pública sobre las amenazas híbridas;

81. Pide que se refuerce la cooperación en materia de amenazas híbridas con socios afines no pertenecientes a la Unión, en particular el Reino Unido y Noruega, como socios clave para la seguridad europea, así como con Canadá, Japón, la República de Corea, Australia, Nueva Zelanda, Taiwán y otros socios afines, también, cuando sea posible, mediante asociaciones en materia de seguridad y defensa, el intercambio de información y la cooperación en materia de ciberseguridad, seguridad marítima, espacio y resiliencia; destaca que los Estados del EEE/AELC y sus industrias de defensa deben incluirse plenamente en los marcos de resiliencia híbrida y los programas de desarrollo de capacidades de la Unión, reconociendo su contribución directa a la seguridad europea y su exposición común a las amenazas híbridas;
82. Lamenta que el reciente cambio en la política estadounidense haya debilitado el frente común de las democracias en un momento de intensificación de las amenazas híbridas; destaca que la unidad transatlántica sigue siendo esencial para combatirlas;
83. Destaca que las operaciones de influencia rusas en África, América Latina y el Caribe no son cuestiones periféricas para la seguridad europea, ya que pretenden socavar las asociaciones de la Unión, debilitar el apoyo a Ucrania y menoscabar la diplomacia europea, la asistencia en materia de seguridad y la cooperación al desarrollo; observa que, en África, estas operaciones se basan principalmente en los medios de comunicación estatales y en los frentes cultural y religioso, mientras que, en América Latina y el Caribe, Rusia ha creado un ecosistema de influencia en lengua española que complementa sus mensajes antieuropeos en otros lugares; pide a la Unión y a los Estados miembros que refuercen la comunicación estratégica, apoyen a los medios de comunicación locales independientes y fiables, impliquen a voces locales creíbles y refuercen la cooperación con los socios de ambas regiones para desenmascarar y contrarrestar las operaciones de información hostiles;
84. Subraya la importancia de la experiencia de los Estados del Golfo, Jordania y otros socios pertinentes a la hora de abordar las redes de influencia híbrida asociadas a los Hermanos Musulmanes, también mediante enfoques de gobernanza, regulación y resiliencia social, y pide un intercambio estructurado de buenas prácticas con estos socios a fin de reforzar la comprensión de la Unión de las amenazas híbridas, mejorar las respuestas políticas y potenciar la cooperación en la lucha contra la injerencia extranjera, respetando al mismo tiempo los derechos fundamentales y la diversidad de los sistemas jurídicos y políticos;
85. Toma nota de la amplia experiencia de Taiwán en su defensa contra los ataques híbridos y la manipulación de información e injerencia por parte de China; elogia el modelo de resiliencia integral de Taiwán, incluida la creación de un comité de resiliencia de defensa de toda la sociedad, la formación a gran escala en defensa civil, la cooperación con las organizaciones de la sociedad civil, las redes de resiliencia digital y las iniciativas de preparación de la población; subraya que la experiencia de Taiwán demuestra que la resiliencia social no es un aspecto secundario de la defensa, sino un

pilar central de la seguridad nacional, en particular cuando la presión híbrida se dirige contra las infraestructuras críticas, la confianza pública y la cohesión social; pide, a este respecto, intercambios periódicos entre la Unión y sus homólogos taiwaneses sobre cuestiones de seguridad pertinentes y una mayor cooperación en la lucha contra la manipulación de información e injerencia por parte de agentes extranjeros y la guerra cognitiva, la protección de las infraestructuras críticas y los cables submarinos y el refuerzo de la resiliencia de toda la sociedad entre la Unión y Taiwán; pide a la Unión que amplíe la cooperación comercial e industrial con Taiwán, en particular en lo que respecta a los componentes de alta tecnología y las tecnologías estratégicas fundamentales para la resiliencia y la seguridad de las infraestructuras esenciales y las cadenas de suministro, incluidos los semiconductores, los equipos de telecomunicaciones 5G/6G, los drones y los productos de doble uso; destaca asimismo la necesidad de proporcionar IRIS² (Infraestructura para la Resiliencia, la Interconectividad y la Seguridad por Satélite) a Taiwán y Ucrania;

◦

◦ ◦

86. Encarga a su presidenta que transmita la presente Resolución al Consejo, a la alta representante y a la Comisión.