COMISIÓN
EUROPEA

ALTA REPRESENTANTE
DE LA UNIÓN PARA
ASUNTOS EXTERIORES Y
POLÍTICA DE SEGURIDAD

Bruselas, 6.4.2016
JOIN(2016) 18 final

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO

Comunicación conjunta sobre la lucha contra las amenazas híbridas

Una respuesta de la Unión Europea

1. INTRODUCCIÓN

En los últimos años ha cambiado radicalmente el entorno de seguridad de la Unión Europea. Los principales desafíos para la paz y la estabilidad en la vecindad oriental y meridional de la UE siguen poniendo de manifiesto la necesidad, para la Unión, de adaptar y aumentar sus capacidades de proveedor de seguridad, haciendo hincapié en la estrecha relación existente entre seguridad exterior e interior. Muchos de los desafíos actuales para la paz, la seguridad y la prosperidad tienen sus raíces en la inestabilidad de la vecindad inmediata de la UE y en las formas cambiantes que adoptan las amenazas. En sus orientaciones políticas de 2014, el Presidente de la Comisión Europea, Jean-Claude Juncker, hizo hincapié en la necesidad de trabajar «por una Europa más fuerte en materia de seguridad y defensa» y de combinar los instrumentos europeos y nacionales con mayor eficacia que hasta la fecha. Así pues, a raíz de la petición del Consejo de Asuntos Exteriores de 18 de mayo de 2015, la Alta Representante, en estrecha cooperación con los servicios de la Comisión y la Agencia Europea de Defensa (AED), y previa consulta a los Estados miembros de la UE, emprendió la elaboración de este marco común con propuestas de actuación que contribuyan a luchar contra las amenazas híbridas y a reforzar la resiliencia de la UE y de sus Estados miembros, así como de los países socios[1]. En junio de 2015, el Consejo Europeo recordó la necesidad de movilizar los instrumentos de la UE para contribuir a la lucha contra las amenazas híbridas[2].

Si bien es cierto que las definiciones de las amenazas híbridas varían y deben seguir siendo flexibles para tener en cuenta su carácter evolutivo, el objeto de este concepto es subrayar la mezcla de actividades coercitivas y subversivas, de métodos convencionales y no convencionales (es decir, diplomáticos, militares, económicos y tecnológicos), que pueden ser utilizados de forma coordinada por agentes estatales o no estatales para lograr objetivos específicos, manteniéndose por debajo del umbral de una guerra declarada oficialmente. Suelen aprovecharse las vulnerabilidades del objetivo y generarse ambigüedad para obstaculizar los procesos decisorios. Las campañas de desinformación masiva, que recurren a los medios sociales para controlar el discurso político o para radicalizar, contratar y manipular a individuos que actúan por delegación, pueden constituir vectores de estas amenazas híbridas.

En la medida en que la lucha contra las amenazas híbridas constituye un asunto de defensa y seguridad nacional y de mantenimiento del orden público, la responsabilidad principal recae en los Estados miembros, ya que la mayor parte de los puntos vulnerables son específicos de cada país. Ahora bien, muchos Estados miembros de la UE se enfrentan a amenazas comunes, que también pueden centrarse en redes o infraestructuras transfronterizas. Esas amenazas pueden tratarse con mayor eficacia si media una respuesta coordinada a escala de la UE que recurra a sus políticas e instrumentos y se asiente en la solidaridad europea, la asistencia mutua y todas las posibilidades que ofrece el Tratado de Lisboa. Las políticas e instrumentos de la UE pueden desempeñar un papel fundamental (en gran parte ya lo hacen) a la hora de aportar un valor añadido para

[1] Conclusiones del Consejo sobre política común de seguridad y defensa (PCSD), mayo de 2015 [Consilium 8971/15].

[2] Conclusiones del Consejo Europeo, junio de 2015 [EUCO 22/15].

aumentar la concienciación, lo cual está ayudando a mejorar la resiliencia de los Estados miembros ante las amenazas comunes. La actuación exterior de la Unión que se propone en este marco se basa en los principios que establece el artículo 21 del Tratado de la Unión Europea (TUE), entre ellos la democracia, el Estado de Derecho, la universalidad e indivisibilidad de los derechos humanos y el respeto de los principios de la Carta de las Naciones Unidas y del Derecho internacional[3].

El objeto de esta Comunicación conjunta es facilitar un enfoque integral que permita a la UE, en coordinación con los Estados miembros, responder específicamente a las amenazas de naturaleza híbrida creando sinergias entre todos los instrumentos pertinentes y fomentando una cooperación estrecha entre todos los agentes implicados[4]. Las medidas se basan en estrategias y políticas sectoriales existentes que contribuirán al logro de una mayor seguridad. En particular, la Agenda Europea de Seguridad[5], la Estrategia global de la UE sobre política exterior y el Plan de Acción de Defensa Europeo, que serán adoptados en breve[6], la Estrategia de ciberseguridad de la UE[7], la Estrategia Europea de Seguridad Energética[8] y la Estrategia de Seguridad Marítima de la Unión Europea[9] constituyen herramientas que también pueden contribuir en la lucha contras las amenazas híbridas.

Dado que la OTAN está trabajando asimismo contra las amenazas híbridas y que el Consejo de Asuntos Exteriores propuso la intensificación de la cooperación y de la coordinación en este ámbito, algunas de las propuestas formuladas aspiran a mejorar la cooperación UE-OTAN en materia de lucha contra este tipo de amenazas.

La respuesta propuesta se centra en los siguientes elementos: aumentar la concienciación, reforzar la resiliencia, prevenir, responder a las crisis y recuperarse tras ellas.

2. RECONOCER LA NATURALEZA HÍBRIDA DE UNA AMENAZA

Las amenazas híbridas procuran aprovechar las vulnerabilidades de un país y suelen socavar los valores democráticos y las libertades fundamentales. Como primer paso, la Alta Representante y la Comisión colaborarán con los Estados miembros para mejorar la conciencia de la situación, controlando y evaluando los riesgos que pueden afectar a las vulnerabilidades de la UE. La Comisión está desarrollando métodos de evaluación de los riesgos de seguridad para contribuir a informar a los responsables de la toma de decisiones y para fomentar una formulación de políticas basada en los riesgos en ámbitos

[3] La Carta de los derechos fundamentales de la UE es vinculante para las instituciones y para los Estados miembros cuando aplican el Derecho de la Unión.

[4] Las posibles propuestas legislativas de la Comisión estarán sujetas a los requisitos para «Legislar mejor», en consonancia con las directrices correspondientes de la Comisión [SWD(2015) 111].

[5] COM(2015) 185 final.

[6] Está previsto que se presenten en 2016.

[7] Marco político de ciberdefensa de la UE (Consilium 15585/14] y Comunicación conjunta «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro», febrero de 2013 [JOIN(2013) 1].

[8] Comunicación conjunta «Estrategia Europea de la Seguridad Energética», mayo de 2014 [SWD(2014) 330].

[9] Comunicación conjunta «Un ámbito marítimo mundial abierto y seguro: elementos para una estrategia de seguridad marítima de la Unión Europea» - JOIN(2014) 9 final, de 6 de marzo de 2014.

que abarcan desde la seguridad de la aviación hasta la financiación del terrorismo, pasando por el blanqueo de dinero. Por otra parte, convendría que los Estados miembros realizasen un estudio a fin de identificar los ámbitos vulnerables ante las amenazas híbridas. Se trata de determinar indicadores de las amenazas híbridas, de incorporarlos a los mecanismos de alerta rápida y evaluación de riesgos existentes y de compartirlos, si procede.

***Medida n.º 1**: Se invita a los Estados miembros, con el apoyo, según proceda, de la Comisión y de la Alta Representante, a iniciar un estudio sobre los riesgos híbridos para determinar las principales vulnerabilidades, con unos indicadores específicos sobre los riesgos híbridos que puedan afectar a las redes y estructuras nacionales y paneuropeas.*

3. ORGANIZAR LA RESPUESTA DE LA UE: MEJORAR LA CONCIENCIACIÓN

3.1. Célula de fusión de la UE contra las amenazas híbridas

Resulta fundamental que la UE, en coordinación con sus Estados miembros, tenga un nivel suficiente de conocimiento de la situación para detectar cualquier cambio en el entorno de seguridad relacionado con actividades híbridas realizadas por agentes estatales o no estatales. Para luchar eficazmente contra las amenazas híbridas, es importante mejorar el intercambio de información y fomentar una puesta en común de los datos pertinentes entre sectores y entre la Unión Europea, sus Estados miembros y los países socios.

Una célula de fusión de la UE contra las amenazas híbridas ofrecerá un foco único para el análisis de las amenazas híbridas, en el seno del Centro de Análisis de Inteligencia de la UE (INTCEN) del Servicio Europeo de Acción Exterior (SEAE). Esta célula de fusión recibirá, analizará y compartirá información clasificada y de dominio público relacionada específicamente con los indicadores y las alertas en materia de amenazas híbridas; esa información procederá de las distintas partes interesadas dentro del SEAE (incluidas las delegaciones de la UE), la Comisión (con las agencias de la UE[10]) y los Estados miembros. En colaboración con organismos similares existentes en la UE[11] y a escala nacional, la célula de fusión analizará los aspectos externos de las amenazas híbridas que afecten a la UE y a su vecindad para analizar con rapidez los incidentes pertinentes y alimentar los procesos decisorios estratégicos de la UE, por ejemplo aportando datos para la evaluación de los riesgos de seguridad que se realiza a escala de la UE. Los resultados analíticos de la célula de fusión serán tramitados y utilizados con arreglo a las normas de la Unión Europea en materia de protección de datos e información clasificada[12]. La célula deberá estar en contacto con los organismos existentes a escala nacional y de la UE. Los Estados miembros deberán crear puntos de contacto nacionales conectados a la

[10] De conformidad con sus mandatos respectivos.

[11] Por ejemplo, el Centro Europeo de Ciberdelincuencia de Europol y el Centro de lucha contra el terrorismo de la UE, FRONTEX, el Equipo de Respuesta a Emergencias Informáticas de la UE (CERT-UE), etc.

[12] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

célula de fusión de la UE contra las amenazas híbridas. El personal interno y externo de la UE (incluidos los empleados en las delegaciones, operaciones y misiones de la UE) y en los Estados miembros también deberá recibir formación para reconocer los primeros síntomas de las amenazas híbridas.

***Medida n.º 2**: Creación de una célula de fusión de la UE contra las amenazas híbridas en el seno de la estructura de la INTCEN de la UE capaz de recibir y analizar información clasificada y de dominio público sobre las amenazas híbridas. Se invita a los Estados miembros a crear puntos de contacto nacionales sobre las amenazas híbridas para garantizar la cooperación y comunicación segura con la célula de fusión de la UE contra las amenazas híbridas*.

3.2. Comunicación estratégica

Los autores de las amenazas híbridas pueden propagar desinformación de forma sistemática, incluso a través de campañas en medios de comunicación social específicos, para intentar radicalizar a personas, desestabilizar la sociedad y controlar el discurso político. Para poder responder a las amenazas híbridas, es imprescindible utilizar una política adecuada de **comunicación estratégica**. Es importante proporcionar respuestas rápidas y concienciar a la opinión pública sobre las amenazas híbridas para reforzar la resiliencia de la sociedad.

La comunicación estratégica deberá hacer pleno uso de las herramientas de las redes sociales, así como de los medios de comunicación tradicionales, visuales, sonoros y en línea. El SEAE, basándose en la labor de los grupos de trabajo sobre comunicación estratégica para Oriente Próximo y los países árabes, deberá optimizar el recurso a lingüistas que dominen las lenguas exteriores a la UE pertinentes, así como a especialistas en medios sociales, que puedan controlar la información que se produce fuera de la UE y elaborar una comunicación puntual para reaccionar ante la desinformación. Además, los Estados miembros deberán desarrollar mecanismos de comunicación estratégica coordinada para respaldar la indicación de las fuentes y contrarrestar la desinformación a fin de sacar a la luz las amenazas híbridas.

***Medida n.º 3**: La Alta Representante explorará con los Estados miembros el modo de actualizar y coordinar la capacidad necesaria para conseguir comunicaciones estratégicas proactivas y optimizar el uso del seguimiento de los medios de comunicación y el recurso a expertos lingüísticos.*

3.3. Centro de excelencia para «la lucha contra las amenazas híbridas»

Basándose en la experiencia de algunos Estados miembros y de organizaciones asociadas[13], un instituto multinacional (o una red de institutos) podría actuar en calidad de centro de excelencia para abordar las amenazas híbridas. Ese centro podría dedicarse a investigar cómo se han aplicado las estrategias contra las amenazas híbridas y estimular

[13] Centros de excelencia de la OTAN.

el desarrollo de nuevos conceptos y tecnologías en el sector privado y la industria para ayudar a los Estados miembros a reforzar su resiliencia. La investigación podría contribuir a adaptar las políticas, las doctrinas y los conceptos nacionales y de la UE, y a garantizar que la toma de decisiones pueda tener en cuenta la complejidad y las ambigüedades asociadas a las amenazas híbridas. Dicho centro deberá elaborar programas para estimular la investigación y ejercicios para encontrar soluciones prácticas ante los desafíos que plantean las amenazas híbridas. La fortaleza de un centro de estas características radicará en los conocimientos que hayan adquirido sus participantes, plurinacionales e intersectoriales, del ámbito civil y militar, procedentes del sector privado y académico.

Este centro podría colaborar con los centros de excelencia de la UE[14] y la OTAN[15] para aprovechar la información sobre las amenazas híbridas que haya sido adquirida en materia de ciberdefensa, comunicación estratégica, cooperación civil y militar, energía y respuesta a las crisis.

***Medida n.º 4**: Se invita a los Estados miembros a crear un centro de excelencia «para la lucha contra las amenazas híbridas».*

4. ORGANIZAR LA RESPUESTA DE LA UE: REFORZAR LA RESILIENCIA

La resiliencia es la capacidad de soportar la presión y de recuperarse, sintiéndose reforzado por los retos superados. Para combatir eficazmente las amenazas híbridas, deben abordarse las posibles vulnerabilidades de las infraestructuras esenciales, de las cadenas de suministro y de la sociedad. Haciendo uso de los instrumentos y políticas de la UE, las infraestructuras a escala de la UE pueden volverse más resilientes.

4.1. Protección de las infraestructuras críticas

Es importante proteger las infraestructuras críticas (p. ej., las cadenas de suministro energético, el transporte, etc.), ya que un atentado no convencional perpetrado por los autores de las amenazas híbridas en un «objetivo blando» podría dar lugar a graves perturbaciones económicas o sociales. Para garantizar la protección de las infraestructuras críticas, el Programa Europeo de Protección de Infraestructuras Críticas (PEPIC)[16] establece un planteamiento sistémico y multirriesgos transsectorial, que examina las interdependencias, basado en la aplicación de las actividades relacionadas con la prevención, la preparación y la respuesta. La Directiva sobre las infraestructuras críticas europeas[17] establece un procedimiento de identificación y designación de infraestructuras críticas europeas (ICE) y un enfoque común para evaluar la necesidad de

[14] P. ej., el Instituto de Estudios de Seguridad de la UE (IES de la UE), los centros de excelencia temáticos de la UE en materia de QBRN.

[15] http://www.nato.int/cps/en/natohq/topics_68372.htm

[16] Comunicación de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas - COM(2006) 786 final de 12.12.2006.

[17] Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección (DO L 345 de 23.12.2008).

mejorar su protección. En particular, debe reanudarse la labor al amparo de la Directiva para reforzar la resiliencia de las infraestructuras críticas de la UE relacionadas con el transporte (p. ej. los principales aeropuertos y puertos mercantes). La Comisión estudiará la posibilidad de desarrollar herramientas comunes, incluidos indicadores, para mejorar la resiliencia de las infraestructuras críticas ante las amenazas híbridas en todos los sectores pertinentes.

***Medida n.º 5**: La Comisión, en cooperación con los Estados miembros y las partes interesadas, determinará herramientas comunes, incluidos indicadores, para mejorar la protección y la resiliencia de las infraestructuras críticas ante las amenazas híbridas en los sectores pertinentes.*

4.1.1. Redes energéticas

La producción y la distribución sin interrupciones de electricidad es fundamental para la UE: unos cortes de suministro importantes podrían ser perjudiciales. Un elemento esencial para la lucha contra las amenazas híbridas es seguir diversificando las fuentes de energía de la UE, así como sus proveedores y las rutas correspondientes, a fin de poder contar con un suministro energético seguro y resiliente. La Comisión también está llevando a cabo evaluaciones de riesgo y de seguridad («pruebas de resistencia») de las centrales eléctricas de la UE. Para garantizar la diversificación energética, se está intensificando la actividad en el contexto de la Estrategia Energética de la Unión: por ejemplo, el Corredor Meridional de Gas permitirá al gas de la región del Mar Caspio alcanzar Europa y crear en el norte de Europa centros líquidos de gas con múltiples proveedores. Este ejemplo debería seguirse en Europa Central y Oriental y en el Mediterráneo, región en la que se está creando una central de gas[18]. El mercado en desarrollo del gas natural licuado también contribuirá de forma positiva a la consecución de este objetivo.

En lo que se refiere a las instalaciones y los materiales nucleares, la Comisión apoya el desarrollo y la adopción de las normas de seguridad más estrictas, con lo que se reforzará su resiliencia. La Comisión está fomentando la coherencia en la transposición y la aplicación tanto de la Directiva sobre seguridad nuclear[19], que establece normas para prevenir los accidentes y atenuar sus consecuencias, como de las disposiciones de la Directiva relativa a las normas básicas de seguridad[20] sobre cooperación internacional en materia de preparación e intervención ante emergencias, especialmente entre los Estados miembros y con los países de la vecindad.

---

18 Sobre los avances registrados hasta la fecha, véase el Estado de la Unión de la Energía 2015 [COM(2015) 572 final].

19 Directiva 2009/71/Euratom del Consejo, de 25 de junio de 2009, por la que se establece un marco comunitario para la seguridad nuclear de las instalaciones nucleares, modificada por la Directiva 2014/87/Euratom del Consejo, de 8 de julio de 2014.

20 Directiva 2013/59/Euratom del Consejo, de 5 de diciembre de 2013, por la que se establecen normas de seguridad básicas para la protección contra los peligros derivados de la exposición a radiaciones ionizantes, y se derogan las Directivas 89/618/Euratom, 90/641/Euratom, 96/29/Euratom, 97/43/Euratom y 2003/122/Euratom.

***Medida n.º 6**: La Comisión, en cooperación con los Estados miembros, apoyará los esfuerzos por diversificar las fuentes de energía y promover normas de seguridad y protección para aumentar la resiliencia de las infraestructuras nucleares*

4.1.2 Transporte y protección de las cadenas de suministro

El transporte es esencial para el funcionamiento de la Unión. Los atentados híbridos contra las infraestructuras de transporte (como aeropuertos, infraestructuras viales, puertos y ferrocarriles) pueden tener graves consecuencias y provocar perturbaciones en las cadenas de desplazamiento y suministro. En su aplicación de la normativa sobre seguridad aérea y marítima[21], la Comisión realiza inspecciones periódicas[22] y, con sus actividades sobre la seguridad del transporte terrestre, procura tratar las amenazas híbridas emergentes. En este contexto, se está debatiendo un marco de la UE al amparo del Reglamento revisado sobre seguridad aérea[23], dentro de la estrategia de aviación para Europa[24]. Por otra parte, las amenazas para la seguridad marítima están siendo tratadas por la Estrategia de Seguridad Marítima de la Unión Europea y su plan de acción[25]. Este permite a la UE y a sus Estados miembros afrontar de forma global los retos para la seguridad marítima, incluida la lucha contra las amenazas híbridas, mediante una cooperación intersectorial de los actores civiles y militares a fin de proteger las infraestructuras marítimas críticas, las cadenas mundiales de suministro, el comercio marítimo y los recursos naturales y energéticos marítimos. La seguridad de la cadena internacional de suministro también figura en la estrategia de la UE para la gestión de los riesgos aduaneros y en su plan de acción[26].

***Medida n.º 7**: La Comisión realizará el seguimiento de las amenazas emergentes en el sector del transporte y actualizará la legislación según proceda. En la aplicación de la*

---

21 Reglamento (CE) n.º 300/2008 del Parlamento Europeo y del Consejo, de 11 de marzo de 2008, sobre normas comunes para la seguridad de la aviación civil y por el que se deroga el Reglamento (CE) n.º 2320/2002. Reglamento de Ejecución (UE) n.º 2015/1998 de la Comisión, de 5 de noviembre de 2015, por el que se establecen medidas detalladas para la aplicación de las normas básicas comunes de seguridad aérea; Directiva 2005/65/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, sobre mejora de la protección portuaria; Reglamento (CE) n.º 725/2004 del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, relativo a la mejora de la protección de los buques y las instalaciones portuarias.

22 Según la normativa de la UE, la Comisión tiene la obligación de realizar inspecciones para garantizar la aplicación correcta, por los Estados miembros, de los requisitos de seguridad aérea y marítima. Esto incluye inspecciones de la autoridad competente en el Estado miembro, así como inspecciones en los aeropuertos, los puertos, las compañías aéreas, los buques y las entidades que aplican las medidas de seguridad. Las inspecciones de la Comisión tienen por objeto garantizar que las normas de la UE se aplican plenamente en los Estados miembros.

23 Reglamento (UE) 2016/4 de la Comisión, de 5 de enero de 2016, por el que se modifica el Reglamento (CE) n.º 216/2008 del Parlamento Europeo y del Consejo en lo que se refiere a los requisitos esenciales de protección medioambiental; Reglamento (CE) n.º 216/2008, de 20 de febrero de 2008, sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia Europea de Seguridad Aérea.

24 Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Una estrategia de aviación para Europa, COM/2015/0598 final, de 7.12.2015.

25 En diciembre de 2014, el Consejo adoptó un plan de acción para aplicar la Estrategia de Seguridad Marítima de la Unión Europea: http://ec.europa.eu/maritimeaffairs/policy/maritime-security/doc/20141216-action-plan_en.pdf

26 Comunicación de la Comisión al Parlamento Europeo, al Consejo y al Comité Económico y Social Europeo sobre la estrategia y el plan de acción de la UE para la gestión de los riesgos aduaneros: afrontar los riesgos, reforzar la protección de la cadena de suministro y facilitar el comercio, COM(2014) 527 final.

Estrategia de Seguridad Marítima de la UE y de la estrategia de gestión de riesgos aduaneros de la UE junto con su plan de acción, la Comisión y la Alta Representante (en el marco de sus respectivas competencias), en colaboración con los Estados miembros, estudiará el modo de responder a las amenazas híbridas, especialmente en relación con las infraestructuras críticas de transporte.

4.1.3 Espacio

Las amenazas híbridas podrían golpear las infraestructuras espaciales con consecuencias multisectoriales. La UE ha diseñado un marco de ayuda a la vigilancia y seguimiento espacial[27] para agrupar en red los activos que poseen los Estados miembros a fin de prestar este tipo de servicios[28] a los usuarios identificados (Estados miembros, instituciones de la UE, propietarios y operadores de vehículos espaciales y autoridades de protección civil). En el contexto de la próxima Estrategia Espacial para Europa, la Comisión estudiará la posibilidad de seguir desarrollando ese marco a fin de controlar las amenazas híbridas para las infraestructuras espaciales.

Las comunicaciones por satélite son un recurso fundamental para la gestión de crisis, la respuesta a catástrofes, la policía y la vigilancia de fronteras y costas. Son la espina dorsal de las infraestructuras a gran escala, como el transporte, el espacio o los sistemas de aeronaves pilotadas a distancia. En consonancia con el llamamiento del Consejo Europeo para preparar la próxima generación de comunicaciones por satélite gubernamentales (GovSatCom), la Comisión, en cooperación con la Agencia de Defensa Europea, está examinando cómo unificar la demanda, en el contexto de la próxima Estrategia Espacial y del Plan de Acción de la Defensa Europea.

Muchas infraestructuras críticas dependen de información sobre la hora exacta para sincronizar sus redes (p. ej., la energía y las telecomunicaciones) o sus operaciones con una marca temporal (p. ej., los mercados financieros). El hecho de depender de la única señal de sincronización horaria del sistema global de navegación por satélite (GNSS) no ofrece la resiliencia necesaria para hacer frente a las amenazas híbridas. Galileo, el sistema global de navegación por satélite europeo, ofrecería un segundo generador de tiempos fiable.

<u>Medida n.º 8</u>: En el contexto de la próxima Estrategia Espacial y del Plan de Acción de la Defensa Europea, la Comisión propondrá que se aumente la resiliencia de las infraestructuras espaciales ante las amenazas híbridas, en particular mediante una posible ampliación del alcance de la vigilancia y seguimiento espacial para que abarque las amenazas híbridas, la preparación para la próxima generación de GovSatCom a escala europea y la introducción de Galileo en las infraestructuras críticas que dependen de la sincronización.

---

27 Véase la Decisión n.º 541/2014 del Parlamento Europeo y del Consejo.

28 Como un aviso anticolisión en órbita, alertas relativas a la destrucción o colisión y a la reentrada arriesgada de objetos espaciales en la atmósfera terrestre.

4.2. Capacidades de defensa

Es necesario reforzar las capacidades de defensa para reforzar la resiliencia de la UE ante las amenazas híbridas. Es importante determinar los ámbitos de capacidades clave, por ejemplo las capacidades en materia de vigilancia y reconocimiento. La Agencia Europea de Defensa podría actuar como catalizador para un desarrollo de las capacidades militares relacionadas con las amenazas híbridas (por ejemplo, acortando los ciclos de desarrollo de las capacidades de defensa, invirtiendo en tecnologías, sistemas y prototipos, abriendo el sector de la defensa a las tecnologías innovadoras comerciales). Las posibles medidas podrían ser examinadas en el contexto del próximo Plan de Acción de la Defensa Europea.

***Medida n.º 9**: La Alta Representante, apoyada en su caso por los Estados miembros, en colaboración con la Comisión, propondrá proyectos sobre la adaptación de las capacidades de defensa y sobre desarrollo que sean pertinentes para la UE, concretamente para luchar contra las amenazas híbridas contra uno o varios Estados miembros.*

4.3. Proteger la salud pública y la seguridad alimentaria

La salud de la población podría verse en peligro por la manipulación de enfermedades transmisibles o la contaminación de los alimentos, del suelo, del aire y del agua potable con sustancias químicas, biológicas, radiológicas y nucleares (QBRN). Además, la propagación intencionada de enfermedades animales o vegetales puede afectar gravemente a la seguridad alimentaria de la Unión y provocar repercusiones económicas y sociales graves en ámbitos cruciales de la cadena alimentaria de la UE. Las estructuras actuales de la UE para la seguridad sanitaria, la protección del medio ambiente y la seguridad alimentaria pueden utilizarse para responder a las amenazas híbridas que utilicen dichos métodos.

En virtud del Derecho de la UE sobre las amenazas transfronterizas para la salud[29], los mecanismos existentes coordinan la preparación frente a las amenazas transfronterizas graves para la salud, relacionando entre sí a los Estados miembros, a las agencias y a los comités científicos de la UE[30] a través del Sistema de Alerta Precoz y Respuesta. El Comité de Seguridad Sanitaria, que coordina la respuesta de los Estados miembros a las amenazas, puede actuar como punto de contacto sobre las vulnerabilidades de la salud pública[31], para inscribir las amenazas híbridas (en particular el bioterrorismo) en las directrices sobre la comunicación en caso de crisis, así como en los ejercicios de refuerzo de las capacidades en los Estados miembros (simulación de crisis). En el ámbito de la

[29] Decisión n.º 1082/2013/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud y por la que se deroga la Decisión n.º 2119/98/CE (DO L 293 de 5.11.2013, p. 1).

[30] Decisión C(2015) 5383 de la Comisión, de 7.8.2015, por la que se crean los comités científicos en el ámbito de la salud pública, la seguridad de los consumidores y el medio ambiente.

[31] En consonancia con la Decisión n.º 1082/2013/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud y por la que se deroga la Decisión n.º 2119/98/CE (DO L 293 de 5.11.2013, p. 1).

seguridad alimentaria, a través del Sistema de Alerta Rápida para los Productos Alimenticios y los Alimentos para Animales (RASFF) y el Sistema común de gestión del riesgo aduanero (CRMS), las autoridades competentes intercambian información sobre análisis de riesgos, a fin de controlar los riesgos para la salud que suponen los alimentos contaminados. En materia de sanidad animal y vegetal, la revisión del marco jurídico de la UE[32] añadirá nuevos elementos a la «caja de herramientas» existente[33] para estar mejor preparados ante las amenazas híbridas.

<u>Medida n.º 10</u>: La Comisión, en cooperación con los Estados miembros, mejorará la concienciación y la resiliencia ante las amenazas híbridas en los mecanismos existentes de preparación y coordinación, especialmente el Comité de Seguridad Sanitaria.

4.4. Ciberseguridad

La UE se beneficia en gran medida de una sociedad interconectada y digital. Los ciberataques podrían perturbar los servicios digitales de la UE y ese tipo de ataques podría ser utilizado por los autores de amenazas híbridas. Mejorar la resiliencia de los sistemas de información y comunicaciones en Europa es importante para respaldar el mercado único digital. La estrategia de ciberseguridad de la UE y la Agenda Europea de Seguridad proporcionan el marco estratégico general de las iniciativas de la UE sobre ciberseguridad y lucha contra la ciberdelincuencia. La UE ha participado de forma activa en la concienciación y el desarrollo de mecanismos de cooperación y respuesta concretos dentro de la Estrategia de Ciberseguridad. En particular, la propuesta de Directiva sobre seguridad de las redes y de la información (SRI)[34] aborda los riesgos de ciberseguridad para una amplia gama de proveedores de servicios esenciales en los ámbitos de la energía, el transporte, las finanzas y la sanidad. Estos proveedores, así como los proveedores de servicios digitales clave (p. ej., la computación en nube), deberán adoptar las medidas de seguridad oportunas y notificar los incidentes graves a las autoridades nacionales, indicando las posibles características híbridas. Una vez haya sido adoptada por los colegisladores, la transposición y la aplicación efectivas de la Directiva fomentará las capacidades de ciberseguridad en los Estados miembros, reforzando su cooperación al respecto mediante el intercambio de información y buenas prácticas sobre la lucha contra las amenazas híbridas. En particular, la Directiva prevé la creación de una red con los 28

---

32 Reglamento (UE) 2016/429 del Parlamento Europeo y del Consejo, de 9 de marzo de 2016, relativo a las enfermedades transmisibles de los animales y por el que se modifican o derogan algunos actos en materia de sanidad animal («Legislación sobre sanidad animal») (DO L 84 de 31.3.2016) En lo que se refiere al Reglamento del Parlamento Europeo y del Consejo relativo a las medidas de protección contra las plagas de los vegetales («Ley de sanidad vegetal»), el Parlamento Europeo y el Consejo alcanzaron el 16 de diciembre de 2015 un acuerdo político sobre el texto.

33 P. ej., los bancos de vacunas de la UE, un sistema complejo de información electrónica sobre enfermedades animales, una mayor obligación de adoptar medidas por parte de los laboratorios y otras entidades relacionados con agentes patógenos.

34 Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión [COM(2013) 48 final de 7.2.2013]. El Consejo de la UE y el Parlamento Europeo han alcanzado un acuerdo político sobre esta propuesta de Directiva y la Directiva debería adoptarse en breve con carácter oficial.

equipos de respuesta a incidentes de seguridad informática (CSIRT) nacionales y el CERT-UE[35] para mantener la cooperación operativa con carácter voluntario.

Para fomentar la cooperación público-privada y los planteamientos a escala de la UE en materia de ciberseguridad, la Comisión creó la plataforma SRI, que publica una guía de mejores prácticas sobre gestión de riesgos. Si bien es cierto que los Estados miembros determinan los requisitos y modalidades de seguridad para notificar los incidentes nacionales, la Comisión aboga por un alto grado de convergencia en los planteamientos de gestión de riesgos, basándose, en particular, en la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA).

***Medida n.º 11**: La Comisión anima a los Estados miembros a que establezcan y utilicen plenamente, con carácter prioritario, una Red entre los 28 CSIRT y el CERT de la UE, así como un marco para la cooperación estratégica. La Comisión, en coordinación con los Estados miembros, debe garantizar que las iniciativas sectoriales sobre las amenazas informáticas (p. ej., en el sector aéreo, energético, marítimo) sean coherentes con la capacidad intersectorial a que se refiere la Directiva SRI para compartir información, conocimientos técnicos y respuestas rápidas.*

4.4.1. Industria

Una mayor confianza en la computación en nube y en los macrodatos ha aumentado la vulnerabilidad ante las amenazas híbridas. La Estrategia para el Mercado Único Digital establece una asociación público-privada contractual (APPC) en materia de ciberseguridad[36], que se centrará en la investigación y la innovación y ayudará a la Unión a mantener un alto grado de capacidad tecnológica en este ámbito. La APPC generará confianza entre los distintos agentes del mercado y permitirá desarrollar sinergias entre la oferta y la demanda. Si bien es cierto que la APPC y las medidas complementarias se centrarán principalmente en el ámbito de los productos y servicios de ciberseguridad civil, los resultados de estas iniciativas deben permitir a los usuarios de las tecnologías protegerse mejor, también frente a las amenazas híbridas.

***Medida n.º 12**: La Comisión, en coordinación con los Estados miembros, colaborará con la industria en el contexto de una APPC para la ciberseguridad, a fin de desarrollar y ensayar tecnologías destinadas a proteger mejor a los usuarios y a las infraestructuras necesarias para luchar contra los aspectos cibernéticos de las amenazas híbridas.*

4.4.2. Energía

La aparición de hogares y aparatos inteligentes y el desarrollo de la red inteligente, que aumenta la digitalización del sistema energético, da lugar a un aumento de la

[35] Equipo de Respuesta a Emergencias Informáticas (CERT-UE) para las instituciones de la UE.
[36] Se pondrá en marcha a mediados de 2016.

vulnerabilidad ante los ciberataques. La Estrategia Europea de la Seguridad Energética[37] y la Estrategia Energética de la Unión[38] respaldan un planteamiento multirriesgo, en el que se incluye la resiliencia ante las amenazas híbridas. La red temática sobre protección de la infraestructura energética crítica fomenta la colaboración entre los operadores del sector energético (petróleo, gas y electricidad). La Comisión puso en marcha una plataforma en la web para analizar y compartir información sobre amenazas e incidentes[39]. También está desarrollando, junto con las partes interesadas[40], una estrategia global para el sector de la energía en materia de ciberseguridad en las operaciones de red inteligente a fin de reducir las vulnerabilidades. Si bien es cierto que los mercados de la electricidad están cada vez más integrados, las normas y los procedimientos para responder a situaciones de crisis siguen siendo nacionales. Debemos garantizar que los gobiernos cooperen entre sí para anticipar, prevenir y mitigar los riesgos y que todos los interesados actúen con arreglo a una serie de normas comunes.

***Medida n.º 13**: La Comisión ofrecerá asesoramiento a los propietarios de activos de red inteligente para mejorar la ciberseguridad de sus instalaciones. En el marco de la iniciativa sobre el diseño del mercado de la electricidad, la Comisión estudiará la posibilidad de proponer «planes de preparación ante el riesgo» y normas de procedimiento para el intercambio de información y de garantizar la solidaridad entre Estados miembros en tiempos de crisis, incluidas normas sobre cómo prevenir y mitigar los ataques cibernéticos.*

4.4.3. Garantizar la solidez de los sistemas financieros

La economía de la UE necesita un sistema financiero y de pagos seguro para funcionar. Es esencial proteger el sistema financiero y su infraestructura de los ciberataques, independientemente del motivo o de la naturaleza del agresor. Para hacer frente a las amenazas híbridas contra la industria de los servicios financieros de la UE, el sector debe comprender la amenaza, poner a prueba sus defensas y disponer de la tecnología necesaria para protegerse del ataque. En consecuencia, la puesta en común de información sobre las amenazas entre los participantes en los mercados financieros, las autoridades competentes, los proveedores de servicios esenciales o los consumidores es crucial, pero también ha de ser segura y cumplir los requisitos sobre protección de datos. En consonancia con la labor realizada en foros internacionales, incluidas las actividades del G-7 en este sector, la Comisión procurará identificar los factores que impiden una puesta en común adecuada de información sobre las amenazas y propondrá soluciones. Es importante garantizar que se realicen inspecciones periódicas y se perfeccionen los protocolos pertinentes para proteger a las empresas y a las infraestructuras afectadas, incluida la mejora continua de las tecnologías que refuerzan la seguridad.

---

37 Comunicación de la Comisión al Parlamento Europeo y al Consejo: Estrategia Europea de la Seguridad Energética - COM(2014) 0330 final.

38 Comunicación sobre la Estrategia Marco para una Unión de la Energía resiliente con una política climática prospectiva - COM(2015) 080 final.

39 Centro de la UE para el intercambio de información sobre incidentes y amenazas (ITIS, por sus siglas en inglés).

40 En forma de plataforma de expertos en materia de ciberseguridad para el sector de la energía (EECSP, por sus siglas en inglés).

<u>Medida n.º 14</u>: La Comisión, en cooperación con ENISA[41], los Estados miembros, las autoridades y entidades financieras pertinentes a escala nacional, internacional y europea, fomentará y facilitará la creación de redes y plataformas para la puesta en común de información sobre las amenazas y examinará los factores que dificultan el intercambio de este tipo de información.

4.4.4. Transporte

Los sistemas de transporte modernos (ferroviario, vial, aéreo, marítimo) dependen de sistemas de información vulnerables ante los ciberataques. Habida cuenta de su dimensión transfronteriza, la UE ha de desempeñar un papel especial al respecto. La Comisión, en coordinación con los Estados miembros, seguirá analizando las ciberamenazas y los riesgos vinculados a actos de interferencia ilícita con los sistemas de transporte. La Comisión está elaborando una hoja de ruta sobre ciberseguridad para la aviación en cooperación con la Agencia Europea de Seguridad Aérea (AESA)[42]. Las amenazas para la seguridad marítima también están siendo tratadas en el contexto de la Estrategia de Seguridad Marítima de la Unión Europea y su plan de acción.

<u>Medida n.º 15</u>: La Comisión y la Alta Representante (dentro de sus ámbitos de competencia respectivos), en coordinación con los Estados miembros, estudiarán el modo de responder a las amenazas híbridas, en particular las relativas a los ataques cibernéticos en el sector del transporte.

4.5. Luchar específicamente contra la financiación de las amenazas híbridas

Los autores de amenazas híbridas necesitan financiación para mantener sus actividades. La financiación puede utilizarse para prestar apoyo a grupos terroristas o para formas más sutiles de desestabilización, como la financiación de grupos de presión y de partidos políticos marginales. La UE ha intensificado sus esfuerzos para combatir la delincuencia y la financiación del terrorismo, según lo establecido en la Agenda Europea de Seguridad, especialmente con el plan de acción correspondiente[43]. En este contexto, concretamente, la revisión del marco europeo para combatir el blanqueo de dinero refuerza la lucha contra la financiación del terrorismo y el blanqueo de dinero, facilita el trabajo de las unidades de información financiera (UIF) para identificar y seguir las transferencias de dinero sospechosas e intercambiar información, garantizando a su vez la trazabilidad de las transferencias de fondos en la Unión Europea, por lo que podría contribuir asimismo a la lucha contra las amenazas híbridas. En el contexto de los instrumentos de la PESC, podría estudiarse la posibilidad de adoptar medidas restrictivas eficaces y adaptadas para luchar contra las amenazas híbridas.

---

41 Agencia de Seguridad de las Redes y de la Información de la Unión Europea

42 El nuevo Reglamento de la AESA está siendo objeto de debate entre el Parlamento Europeo y el Consejo tras la propuesta de la Comisión de diciembre de 2015. Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre normas comunes en el ámbito de la aviación civil y por el que se crea una Agencia de Seguridad Aérea de la Unión Europea, y se deroga el Reglamento (CE) n.º 216/2008 del Parlamento Europeo y del Consejo - COM(2015) 613 final, 2015/0277 (COD).

43 Comunicación de la Comisión al Parlamento Europeo y al Consejo - Plan de acción para intensificar la lucha contra la financiación del terrorismo [COM(2016) 50 final].

<u>Medida n.º 16</u>: La Comisión aprovechará la aplicación del plan de acción de lucha contra la financiación del terrorismo para contribuir asimismo a la lucha contra las amenazas híbridas.

4.6. Reforzar la resiliencia frente a la radicalización y el extremismo violento

Si bien es cierto que los actos de terrorismo y el extremismo violento no son en sí mismos de carácter híbrido, los autores de amenazas híbridas pueden orientar y contratar a miembros vulnerables de la sociedad, radicalizándolos por medio de los canales modernos de comunicación (redes sociales de internet, franquicias locales, etc.) y de propaganda.

Para hacer frente a los contenidos extremistas en internet, la Comisión está analizando, en el contexto de la Estrategia para el Mercado Único Digital, la necesidad de adoptar nuevas medidas, teniendo debidamente en cuenta su impacto sobre los derechos fundamentales de libertad de expresión e información. Esas medidas podrían incluir procedimientos estrictos de supresión de contenidos ilícitos, evitando que se retiren contenidos legales («notificación y acción»), y una mayor responsabilidad y diligencia debida de los intermediarios en la gestión de sus redes y sistemas. Todo ello vendría a completar el enfoque actual, de carácter voluntario, por el que las empresas de internet y de las redes sociales (especialmente al amparo del Foro de Internet de la UE), en cooperación con la Unidad de Notificación de Contenidos de Internet de Europol, retiran sin dilación la propaganda terrorista.

En el contexto de la Agenda Europea de Seguridad, se está luchando contra la radicalización mediante el intercambio de experiencias y el desarrollo de buenas prácticas, incluida la cooperación con terceros países. El Equipo Consultivo sobre Comunicaciones Estratégicas relativas a Siria se propone reforzar el desarrollo y la difusión de mensajes alternativos para contrarrestar la propaganda terrorista. La Red para la Sensibilización frente a la Radicalización apoya a los Estados miembros y a los profesionales que deben interactuar con individuos radicalizados (incluidos los combatientes terroristas extranjeros) o con individuos de los que se sospecha que son vulnerables a la radicalización. Esa Red propone actividades de formación y asesoramiento y ofrecerá apoyo a terceros países prioritarios, si se observa en ellos la voluntad de comprometerse. Además, la Comisión está fomentando la cooperación judicial entre los agentes de la justicia penal, incluido Eurojust, para luchar contra el terrorismo y la radicalización en todos los Estados miembros, lo cual incluye el tratamiento dado a los combatientes terroristas extranjeros y a los retornados.

A modo de complemento de los enfoques mencionados en su **acción exterior**, la UE contribuye a la lucha contra el extremismo violento, incluso mediante la colaboración y el acercamiento internacionales, la prevención (lucha contra la radicalización y la financiación del terrorismo), así como mediante medidas que permitan abordar los factores sociales, políticos y económicos subyacentes que constituyen el terreno abonado para el surgimiento de grupos terroristas.

<u>Medida n.º 17</u>: La Comisión está aplicando las medidas contra la radicalización que figuran en la Agenda Europea de Seguridad y analizando la necesidad de reforzar los procedimientos de supresión de contenidos ilegales, instando a los intermediarios a que apliquen la diligencia debida en la gestión de redes y sistemas.

4.7. Reforzar la cooperación con los terceros países

Tal como se subraya en la Agenda Europea de Seguridad, la UE ha hecho hincapié en el refuerzo de las capacidades de los ***países socios*** en materia de seguridad, por ejemplo aprovechando el nexo entre seguridad y desarrollo y ampliando la dimensión de seguridad de la Política Europea de Vecindad revisada[44]. Estas medidas pueden fomentar asimismo la resiliencia de los socios ante actividades híbridas.

La Comisión se propone intensificar el intercambio de información operativa y estratégica con los países de la ampliación, así como en el marco de la Asociación Oriental y la vecindad meridional, según proceda, para contribuir a luchar contra la delincuencia organizada, el terrorismo, la migración irregular y el tráfico de armas de pequeño calibre. En lo que se refiere a la lucha contra el terrorismo, la UE está consolidando la cooperación con los terceros países mediante el establecimiento de diálogos reforzados sobre cuestiones de seguridad y planes de acción.

Los instrumentos de financiación exterior de la UE procuran crear instituciones eficaces y responsables en los terceros países[45], lo cual constituye un requisito previo para responder de modo eficaz a las amenazas en materia de seguridad y mejorar su resiliencia. En este contexto, la reforma del sector de la seguridad y el desarrollo de capacidades en apoyo de la seguridad y el desarrollo[46] constituyen instrumentos fundamentales. En el marco del Instrumento en pro de la Estabilidad y la Paz[47], la Comisión ha desarrollado medidas destinadas a reforzar la resiliencia cibernética y la capacidad de los socios para detectar y responder a los ciberataques y a la ciberdelincuencia, lo cual permitirá hacer frente a las amenazas híbridas en los terceros países. La UE está financiando actividades de desarrollo de capacidades en los países socios para atenuar los riesgos de seguridad relacionados con los agentes QBRN[48].

---

44 Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «Revisión de la Política Europea de Vecindad» [JOIN(2015)0050 de 18.11.2015].

45 Ídem; Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «Estrategia de Ampliación de la UE», de 10.11.2015, COM(2015) 611 final. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «Incremento del impacto de la política de desarrollo de la UE: Programa para el cambio», COM(2011) 637 final, de 13.10.2011.

46 Comunicación conjunta «Desarrollo de capacidades en apoyo de la seguridad y el desarrollo - Capacitar a los socios para la prevención y la gestión de las crisis» [JOIN(2015) 17 final].

47 Reglamento (UE) n.º 230/2014 del Parlamento Europeo y del Consejo, de 11 de marzo de 2014, por el que se establece un instrumento en pro de la estabilidad y la paz (DO L 77 de 15.3.2014, p. 1).

48 Los ámbitos cubiertos incluyen el control de fronteras, la gestión de crisis, la primera intervención, el tráfico ilícito, el control de las exportaciones de productos de doble uso, el control y vigilancia de las enfermedades, el análisis forense nuclear, la recuperación tras un incidente y la protección de las instalaciones de alto riesgo. Pueden compartirse con terceros países las mejores prácticas derivadas de

Por último, teniendo en mente el enfoque integral de la gestión de crisis, los Estados miembros podrían recurrir a las herramientas y misiones de la Política Común de Seguridad y Defensa (PCSD), de forma independiente o como complemento de instrumentos de la UE que se hayan sido desplegados, a fin de ayudar a los socios en el refuerzo de sus capacidades. Podrían contemplarse las actividades siguientes: i) apoyo a la comunicación estratégica; ii) asesoramiento a los ministerios fundamentales expuestos a amenazas híbridas; iii) apoyo adicional para la gestión de fronteras en caso de emergencia. Podrían explorarse nuevas sinergias entre los instrumentos de la PCSD y los profesionales de la seguridad, las aduanas y la justicia, incluidas las agencias pertinentes de la UE[49], Interpol y la Fuerza de Gendarmería Europea, conforme a sus mandatos respectivos.

***Medida n.º 18**: La Alta Representante, en coordinación con la Comisión, iniciará una encuesta sobre los riesgos híbridos en las regiones vecinas.*

La Alta Representante, la Comisión y los Estados miembros utilizarán los instrumentos de que disponen, respectivamente, para ampliar las capacidades de los socios y reforzar su resiliencia ante las amenazas híbridas. Cabría la posibilidad de desplegar misiones de la PCSD, de forma independiente o como complemento de los instrumentos de la UE, para ayudar a los socios a reforzar sus capacidades.

5. PREVENIR, RESPONDER A LAS CRISIS Y RECUPERARSE TRAS ELLAS

Como ya se ha indicado en la sección 3.1, el objeto de la propuesta de célula de fusión de la UE contra las amenazas híbridas es analizar los indicadores pertinentes para prevenir las amenazas híbridas y responder a ellas e informar a los responsables políticos de la UE. Si bien es cierto que pueden atenuarse las deficiencias con políticas a largo plazo a escala nacional y de la UE, sigue siendo esencial, a corto plazo, reforzar la capacidad de los Estados miembros y de la Unión para prevenir las amenazas híbridas, responder a ellas y recuperarse, de forma rápida y coordinada.

Es fundamental responder con agilidad a las situaciones provocadas por las amenazas híbridas. A este respecto, podría constituir un mecanismo de respuesta eficaz que el Centro Europeo de Coordinación de la Repuesta a Emergencias[50] facilitase medidas y capacidades de protección civil a escala nacional para los aspectos de las amenazas híbridas que requieran una respuesta de protección civil. Esto podría lograrse en colaboración con otros mecanismos de respuesta de la UE y con los sistemas de alerta temprana, en particular con la Sala de Guardia del SEAE en cuanto a los aspectos de seguridad exterior y con el Centro de Análisis Estratégico y Respuesta en materia de seguridad interior.

---

los instrumentos desarrollados en el Plan de Acción QBRN de la UE, como el Centro europeo de formación en materia de seguridad nuclear y la participación de la UE en el grupo de trabajo internacional sobre vigilancia de fronteras.

49 EUROPOL, FRONTEX, CEPOL, EUROJUST.

50 http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en

La cláusula de solidaridad (artículo 222 del TFUE) permite una actuación de la Unión, así como entre los Estados miembros, si un Estado miembro es objeto de un atentado terrorista o víctima de una catástrofe natural o de origen humano. La intervención de la Unión para ayudar al Estado miembro afectado se realiza mediante la aplicación de la Decisión 2014/415/UE del Consejo[51]. Las modalidades de coordinación en el Consejo deben basarse en el Dispositivo Integrado de Respuesta Política a las Crisis[52] de la UE. De conformidad con esas modalidades, la Comisión y la Alta Representante (en sus ámbitos de competencia respectivos) deberán determinar los instrumentos pertinentes de la Unión y presentar al Consejo propuestas de decisiones sobre medidas excepcionales.

El artículo 222 del TFUE también se refiere a las situaciones de asistencia directa por uno o varios Estados miembros al Estado miembro que haya sufrido un atentado terrorista o una catástrofe. La Decisión 2014/415/UE del Consejo no se aplica en estas circunstancias. Ante la ambigüedad inherente a las actividades híbridas, la posible aplicabilidad en última instancia de la cláusula de solidaridad debe ser evaluada por la Comisión y la Alta Representante (en sus ámbitos de competencia respectivos) si un Estado miembro de la UE está sujeto a importantes amenazas híbridas.

A diferencia del artículo 222 del TFUE, si varias amenazas híbridas graves constituyen una agresión armada contra un Estado miembro de la UE, podría invocarse el artículo 42, apartado 7, del TUE para aportar una respuesta adecuada en el momento oportuno. La aparición de amenazas híbridas de gran alcance y gravedad puede requerir asimismo una mayor cooperación y coordinación con la OTAN.

A la hora de preparar sus fuerzas, se anima a los Estados miembros a tener en cuenta las posibles amenazas híbridas. Para estar en condiciones de tomar decisiones de forma rápida y eficaz en caso de atentado híbrido, los Estados miembros deben organizar ejercicios con carácter periódico, a nivel tanto operativo como político, a fin de poner a prueba la capacidad decisoria nacional y multinacional. El objetivo consistiría en establecer un protocolo operativo común entre los Estados miembros, la Comisión y la Alta Representante, perfilando procedimientos eficaces para seguir los casos de amenazas híbridas, desde la identificación inicial hasta el ataque final, y desglosando el papel de cada institución de la Unión y de cada participante en el proceso.

Como componente importante de la PCSD, el compromiso podría aportar: a) formación civil y militar, b) misiones de tutoría y asesoramiento para mejorar la seguridad y las capacidades de defensa del Estado amenazado, c) planes de emergencia para detectar las señales de amenazas híbridas y reforzar las capacidades de alerta rápida, d) apoyo a la gestión del control de fronteras, en caso de emergencia y e) apoyo en ámbitos especializados, como la atenuación de los riesgos QBRN y la evacuación de los no combatientes.

---

[51] Decisión 2014/415/EU del Consejo, de 24 de junio de 2014, relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad (DO L 192 de 1.7.2014).

[52] http://www.consilium.europa.eu/en/documents-publications/publications/2014/eu-ipcr/

***Medida n.º 19**: La Alta Representante y la Comisión, en coordinación con los Estados miembros, establecerán un protocolo operativo común y realizarán ejercicios periódicos para mejorar la capacidad decisoria estratégica en respuesta a la complejidad de las amenazas híbridas, basándose en los procedimientos del Dispositivo Integrado de Respuesta Política a las Crisis.*

***Medida n.º 20**: La Comisión y la Alta Representante, en sus ámbitos de competencia respectivos, examinarán la aplicabilidad y las implicaciones prácticas del artículo 222 del TFUE y del artículo 42, apartado 7, del TUE, en caso de que se produzca un atentado híbrido de gran alcance y gravedad.*

***Medida n.º 21**: La Alta Representante, en coordinación con los Estados miembros, integrará, aprovechará y coordinará las capacidades de acción militar en la lucha contra las amenazas híbridas, al amparo de la Política Común de Seguridad y Defensa.*

6. AUMENTAR LA COOPERACIÓN CON LA OTAN

Las amenazas híbridas representan un reto no solo para la UE sino también para otras grandes organizaciones socias como las Naciones Unidas (ONU), la Organización para la Seguridad y la Cooperación en Europa (OSCE) y, en particular, la OTAN. Una respuesta eficaz requiere diálogo y coordinación entre las organizaciones, tanto desde el punto de vista político como operativo. Una mayor interacción entre la UE y la OTAN reforzaría las capacidades de ambas organizaciones para prepararse y responder con eficacia a las amenazas híbridas, de forma complementaria y mediante un respaldo mutuo, basado en el principio de participación abierta, respetando la autonomía decisoria y las normas de protección de datos de cada organización.

Ambas organizaciones comparten valores y se enfrentan a retos similares. Tanto los Estados miembros de la UE como los aliados de la OTAN esperan de su organización que los apoye, que actúe con rapidez, con determinación y de forma coordinada en caso de crisis o, mejor aún, que eviten que esta ocurra. Se han establecido varios ámbitos en los que podría alcanzarse una cooperación y una coordinación mayores entre la UE y la OTAN, por ejemplo en cuanto se refiere al conocimiento de la situación, las comunicaciones estratégicas, la ciberseguridad y la prevención y gestión de crisis. Convendría consolidar el diálogo informal en curso entre la UE y la OTAN sobre las amenazas híbridas para sincronizar las actividades de ambas organizaciones al respecto.

Para desarrollar unas respuestas complementarias de la UE y la OTAN, es importante que ambas compartan la misma visión de la situación antes de la crisis y durante ella. Esto podría conseguirse mediante un intercambio periódico de los análisis y de las enseñanzas extraídas, así como mediante un contacto directo entre la célula de fusión de la UE contra las amenazas híbridas y la célula correspondiente de la OTAN. También es importante ampliar el conocimiento mutuo de los procedimientos de gestión de crisis respectivos para garantizar una reacción rápida y eficaz. Podría reforzarse la resiliencia garantizando la complementariedad en la fijación de valores de referencia para los elementos críticos de las infraestructuras respectivas y fomentando una estrecha

colaboración en la comunicación estratégica y la ciberdefensa. Unos ejercicios conjuntos con la plena participación de ambas partes, tanto a nivel técnico como político, contribuirían a reforzar la eficacia de la capacidad decisoria respectiva de ambas organizaciones. Explorar nuevas opciones en las actividades de formación ayudaría a desarrollar un nivel comparable de experiencia en áreas críticas.

***Medida n.º 22**: La Alta Representante, en coordinación con la Comisión, mantendrá el diálogo informal y mejorará la cooperación y la coordinación con la OTAN sobre el conocimiento de la situación, las comunicaciones estratégicas, la ciberseguridad y la «prevención y gestión de crisis» para luchar contra las amenazas híbridas, respetando los principios de plena participación y de autonomía en el proceso decisorio de cada organización.*

7. CONCLUSIONES

Esta Comunicación conjunta presenta medidas destinadas a contribuir a la lucha contra las amenazas híbridas y a reforzar la resiliencia a escala nacional y de la UE, así como de los socios. Dado que la atención se centra en **mejorar la concienciación**, se propone establecer mecanismos específicos para el intercambio de información con los Estados miembros y para coordinar la capacidad de la UE en materia de comunicaciones estratégicas. Se han elaborado medidas para **reforzar la resiliencia** en ámbitos como la ciberseguridad, las infraestructuras críticas, la protección del sistema financiero frente a usos ilícitos y los esfuerzos para luchar contra el extremismo violento y la radicalización. En cada uno de estos ámbitos, la aplicación de las estrategias acordadas por la UE y los Estados miembros, así como la plena aplicación por los Estados miembros de la normativa vigente, constituirán un primer paso fundamental. También se presentan algunas medidas más concretas para apuntalar los esfuerzos al respecto.

En lo que se refiere a la **prevención y respuesta a las amenazas híbridas y a la recuperación posterior**, se propone examinar la viabilidad de una aplicación de la cláusula de solidaridad del artículo 222 del TFUE (tal como se especifica en la Decisión correspondiente) y del artículo 42, apartado 7, del TUE, en caso de que se produzca un atentado híbrido de gran alcance y gravedad. La capacidad de toma de decisiones estratégicas podría reforzarse si se establece un protocolo operativo común.

Por último, se propone **reforzar la cooperación y la coordinación entre la UE y la OTAN** mediante esfuerzos comunes para hacer frente a las amenazas híbridas.

En la aplicación de este marco común, la Alta Representante y la Comisión se comprometen a movilizar los instrumentos de la UE pertinentes de que disponen respectivamente. Es importante para la UE obrar, junto con los Estados miembros, por reducir los posibles riesgos que supone la exposición a amenazas híbridas procedentes de agentes tanto estatales como no estatales.