COMISIÓN
EUROPEA

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

Bruselas, 13.6.2018
JOIN(2018) 14 final

INFORME CONJUNTO AL PARLAMENTO EUROPEO, AL CONSEJO EUROPEO Y AL CONSEJO

relativo a la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas de julio de 2017 a junio de 2018

INTRODUCCIÓN

Según la Comunicación conjunta sobre la lucha contra las amenazas híbridas[1], el conocimiento de la situación, la resiliencia y la respuesta están en el centro de la acción de la UE ante las amenazas híbridas. Para aumentar nuestra capacidad de resistir a los ataques y de recuperarnos de ellos resulta fundamental que desarrollemos nuestra competencia para detectar y entender de manera temprana las actividades híbridas maliciosas y mejoremos la resiliencia de las infraestructuras críticas de nuestras sociedades e instituciones (por ejemplo, en los ámbitos del transporte, las comunicaciones, la energía, el espacio y las finanzas). La lucha contra las amenazas híbridas requiere acciones tanto de los Estados miembros como de las instituciones europeas. El primer informe sobre la aplicación de las veintidós medidas definidas en la Comunicación conjunta se presentó al Consejo el 19 de julio de 2017[2]. Esta actualización de 2018 aporta una perspectiva general de los progresos realizados desde el verano del pasado año.

Se han conseguido avances notables en los cuatro ámbitos de acción prioritarios:

- mejorar el conocimiento de la situación,
- fomentar la resiliencia,
- reforzar la capacidad de los Estados miembros y de la Unión para prevenir las crisis y responder a ellas, así como para recuperarse de forma coordinada,
- mejorar la cooperación con la OTAN para garantizar la complementariedad de las medidas.

RECONOCER LA NATURALEZA HÍBRIDA DE LAS AMENAZAS

Acción 1: ***Realización por los Estados miembros de un estudio sobre los riesgos híbridos***

El Consejo ha creado un grupo de «Amigos de la Presidencia», encabezado por la Presidencia de turno, para impulsar los trabajos. En diciembre de 2017, los Estados miembros iniciaron un estudio para evaluar sus vulnerabilidades clave a las amenazas híbridas. Sobre la base de las respuestas de los Estados miembros, la Presidencia presentará un informe al Coreper, probablemente antes del final de junio de 2018.

Con vistas a la expiración de su mandato al final de junio de 2018, el grupo de «Amigos de la Presidencia» inició en su reunión de abril las deliberaciones sobre el futuro mandato. Estos debates se basaban en la propuesta de la Presidencia, que desea prorrogar el mandato actual hasta 2020 y ampliar las competencias del grupo. Con arreglo a este proyecto, el mandato incluiría tareas relacionadas con el análisis de opciones para reforzar la preparación y la resiliencia, la observación de los avances nacionales y la colaboración para coordinar las políticas de gestión de las amenazas híbridas, el apoyo a la labor del Consejo en la cooperación entre la UE y la OTAN en la lucha contra las amenazas híbridas y el intercambio de información, así como el desarrollo de una interpretación común de estas amenazas.

---

1 JOIN(2016) 18 final.

2 Informe conjunto al Parlamento Europeo y al Consejo relativo a la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas. Una respuesta de la Unión Europea, JOIN(2017) 30 final.

ORGANIZAR LA RESPUESTA DE LA UE: MEJORAR EL CONOCIMIENTO

Acción 2: ***Creación de una célula de fusión de la UE contra las amenazas híbridas***

La célula de fusión de la UE contra las amenazas híbridas, situada en el Centro de Inteligencia y de Situación de la Unión Europea e integrada en la Capacidad Única de Análisis de Inteligencia civil y militar de la UE, recurre a analistas y contribuciones tanto militares como civiles de los servicios de inteligencia y de seguridad de los Estados miembros. En julio de 2017 alcanzó su capacidad operativa plena, que se vio confirmada durante el ejercicio paralelo y coordinado con la OTAN de 2017 (PACE17). La célula de fusión de la UE contra las amenazas híbridas analiza la información confidencial y de fuente abierta relativa a amenazas híbridas que recibe de un amplio conjunto de partes interesadas. Los informes y análisis resultantes se ponen a disposición de las instituciones de la UE y de los Estados miembros, con el fin de que las decisiones se adopten con conocimiento de causa. Hasta la fecha, la célula de fusión de la UE contra las amenazas híbridas ha elaborado más de cien productos relativos a amenazas híbridas. El CERT-UE (equipo de respuesta a emergencias informáticas de las instituciones de la Unión Europea) contribuye a la labor de la célula de fusión de la UE contra las amenazas híbridas compartiendo información sobre las ciberamenazas existentes y emergentes. Sin embargo, los conocimientos específicos actuales en materia de amenazas químicas, biológicas, radiológicas y nucleares, ciberinteligencia y contrainteligencia son limitados.

A fin de completar esta labor, la célula de fusión de la UE contra las amenazas híbridas ha establecido una red de puntos de contacto nacionales. Hasta ahora, veintiséis de los veintiocho Estados miembros han declarado puntos de contacto, que se reúnen periódicamente para compartir sus conocimientos con la célula.

Por otra parte, existe una red conjunta equivalente del SEAE y la Comisión centrada en llevar a cabo diferentes acciones de resiliencia. Estas reuniones se celebran con periodicidad mensual y se centran en cuestiones temáticas como el transporte, las infraestructuras, la energía, la ciberseguridad y las actividades de inteligencia hostil.

A nivel estratégico, la célula de fusión de la UE contra las amenazas híbridas está desarrollando su relación con el Centro de Excelencia para la Lucha contra las Amenazas Híbridas de Helsinki mediante su participación en talleres y ejercicios, así como en debates rutinarios sobre temas relacionados con el desarrollo de competencias para la lucha contra las amenazas híbridas.

En el marco de la Declaración conjunta, el contacto con el personal de la rama dedicada al análisis de las amenazas híbridas de la OTAN es diario y continuo. En septiembre de 2017 se publicó una evaluación paralela, coordinada y de carácter innovador, sobre las amenazas híbridas, y los productos previstos para 2018 se centrarán en los retos derivados de las amenazas híbridas planteados por los vecinos del sur y del este.

Acción 3: ***Comunicaciones estratégicas***

El impulso que han cobrado las comunicaciones estratégicas en la UE va unido al desarrollo de las capacidades de diversos agentes. La Comunicación titulada «La lucha contra la desinformación en línea: un enfoque europeo»[3], de 26 de abril de 2018, reconoce la desinformación como una amenaza híbrida y establece diferentes acciones, como la creación de una red reforzada entre la Comisión, el Servicio Europeo de Acción Exterior y los Estados miembros. Las experiencias positivas del grupo de trabajo sobre comunicación estratégica para Oriente Próximo (Grupo de Trabajo East StratCom), creado en marzo de 2015 por mandato del Consejo Europeo, se han de respaldar y consolidar, como se propone en la

[3] COM(2018) 236 final.

Comunicación conjunta titulada «Enfrentarse a las amenazas híbridas: proteger a los europeos»[4].

La labor de East StratCom se centra en su mayor parte en apoyar a las delegaciones de la UE, principalmente en la región de la Asociación Oriental y Rusia, y, en cierta medida, en Asia Central, con el fin de mejorar la transmisión de mensajes positivos y ampliar el alcance a públicos nacionales o regionales. La Comisión respalda estas actividades con un programa regional plurianual de información y comunicación. El Grupo de Trabajo East StratCom también coordina periódicamente sus actividades con los Estados miembros y la OTAN. Además de llevar un seguimiento de la desinformación, realiza actividades para concienciar a los países de la Asociación Oriental y los Estados miembros del impacto de la desinformación rusa. Por otra parte, ha intensificado la formación del personal de los países de la Asociación Oriental con el fin de potenciar sus capacidades de comunicación estratégica y su resiliencia ante la desinformación. Para el futuro se prevé un aumento de la cooperación con la OTAN y los Centros de Excelencia de Riga y Helsinki, que incluirá una puesta en común de los análisis y la organización de seminarios de formación de periodistas de la región de la Asociación Oriental o Rusia.

A raíz de la nueva estrategia de la UE para los Balcanes Occidentales, se ha creado un Grupo de trabajo centrado en los Balcanes Occidentales para comunicar las políticas de la UE de manera más efectiva y a un público más amplio de la región, a la vez que se realizan actividades para concienciar de la desinformación y centradas en esta, orientadas a los Balcanes Occidentales. El Grupo de Trabajo y la Comisión han establecido una cooperación intensiva cuyo objetivo es desarrollar una comunicación y unos mensajes más estratégicos y orientados a la región, basándose en mejores prácticas y en un enfoque de campañas temáticas. Sin embargo, hay poca conciencia de las crecientes amenazas dirigidas específicamente a las instituciones. Es necesario construir una cultura de conciencia de la seguridad y desarrollar las capacidades de las instituciones de afrontar las amenazas híbridas.

El Grupo de Trabajo Sur, creado en 2017, adaptó su mandato para reflejar una transición del prisma de la lucha antiterrorista a un enfoque más matizado, con el fin de mejorar la comunicación con el mundo árabe y ampliar el alcance en este, en particular utilizando la lengua árabe. Dado que el Dáesh o Estado Islámico no es la única amenaza en términos de radicalización, el Grupo de Trabajo se aplica en mitigar la difusión de información errónea y una percepción equivocada de la UE. Para ello desarrolla, en estrecha cooperación con la Comisión, relatos positivos acerca de la Unión Europea y sus políticas, con el fin de mejorar el entendimiento de la Unión, comunicar de una manera más estratégica las actividades de la Unión en el mundo árabe y promover valores e intereses compartidos. La Comisión respalda estas actividades con un programa regional plurianual de información y comunicación.

<u>Acción 4:</u> ***Centro de Excelencia para la Lucha contra las Amenazas Híbridas***

El Centro de Excelencia para la Lucha contra las Amenazas Híbridas, creado en 2017, funciona como un núcleo de conocimientos especializados de apoyo a los esfuerzos individuales y colectivos de los países participantes por luchar contra las amenazas híbridas, mediante investigación, formación, educación y ejercicios. El Centro está abierto a la participación tanto de los Estados miembros como de los aliados de la OTAN. Recientemente se han unido al Centro Italia, los Países Bajos, Dinamarca y la República Checa, con lo que el número de miembros ya es de dieciséis. Tanto la UE como la OTAN participan en la junta directiva del Centro como observadores.

En 2018 el Centro ha acordado un presupuesto y un plan de trabajo, ha desarrollado un marco conceptual y ha creado tres comunidades de interés: influencia de las amenazas híbridas,

[4] Pendiente de referencia.

vulnerabilidades y resiliencia y estrategia y defensa. Se ha creado un subgrupo de agentes no estatales para observar cómo operan los diferentes grupos terroristas y sus representantes. El Centro ha publicado diversos análisis de amenazas híbridas y ha convocado varias reuniones de alto nivel para llegar a un entendimiento común de las amenazas híbridas, compartir mejores prácticas y buscar respuestas comunes en las comunidades de la UE y la OTAN.

ORGANIZAR LA RESPUESTA DE LA UE: REFORZAR LA RESILIENCIA

Para reforzar la resiliencia es necesario actuar en numerosos frentes políticos. Estas actuaciones no siempre son específicas del carácter híbrido de las amenazas, pero conjuntamente pueden garantizar que una UE más resiliente está mejor preparada para enfrentarse a estas. Así pues, cuando en la descripción de los avances conseguidos en cada una de las actuaciones descritas a continuación resulta pertinente, se hace referencia al marco político específico y a las actuaciones llevadas a cabo por la UE, y en particular a las que se integran en la labor orientada a la protección de la UE. El presente informe debe leerse conjuntamente con los informes mensuales de situación relativos a una Unión de la Seguridad genuina y efectiva, adoptados el mismo día[5].

Acción 5: ***Protección y resiliencia de las infraestructuras críticas***

La Comisión ha desarrollado un proyecto de manual de indicadores de vulnerabilidad y resiliencia ante las amenazas híbridas dirigidas a las infraestructuras críticas de la UE. Este texto se encuentra en proceso de validación mediante consultas con los Estados miembros. Su versión definitiva está prevista para noviembre de 2018. Por otra parte, los indicadores de vulnerabilidad se evaluarán durante el ejercicio paralelo y coordinado con la OTAN de 2018 (PACE18), y también los probarán los Estados miembros que han manifestado su interés al respecto. Se ha de prestar una atención especial al mayor desarrollo de los indicadores de detección para facilitar la alerta temprana al principio de los ataques híbridos a infraestructuras críticas. Las amenazas híbridas se tendrán también en cuenta en la próxima evaluación de la Directiva europea sobre la protección de las infraestructuras críticas. Por otra parte, la Comisión está reforzando el apoyo científico destinado a afrontar las características múltiples y transversales de las amenazas híbridas, centrándose especialmente en la identificación de las vulnerabilidades, la detección precoz y los indicadores tempranos, la resiliencia, la concienciación y los ejercicios.

Asimismo, a fin de proteger los activos clave de la Unión, la Comisión ha presentado una propuesta de Reglamento por el que se establece un marco para el control de las inversiones extranjeras directas en la Unión Europea que puedan afectar a la seguridad o al orden público[6]. La propuesta de la Comisión hace referencia a las inversiones directas de personas o empresas de terceros países que puedan, entre otras cosas, afectar a las infraestructuras críticas (lo que incluye la energía, los transportes, las comunicaciones, el almacenamiento de datos, la infraestructura espacial y otras instalaciones sensibles), las tecnologías críticas (lo que incluye la inteligencia artificial, la ciberseguridad y las tecnologías con aplicaciones que pueden tener doble uso), la seguridad del suministro de insumos críticos o las inversiones que dan acceso a información sensible o a la capacidad de control de la información sensible.

La segunda fase del Foro Consultivo de Energía Sostenible en el Sector de Defensa y Seguridad de la Agencia Europea de Defensa seguirá respaldando el desarrollo del documento conceptual elaborado por el Grupo de expertos en protección de las infraestructuras energéticas críticas y lo traducirá en un documento político orientativo a nivel de la UE. Este documento propone un marco de identificación de mejores prácticas para los ministerios de Defensa en el refuerzo de la protección y la resiliencia de todas las infraestructuras

[5] COM(2018) 470 final.
[6] COM(2017) 487 final.

energéticas críticas relacionadas con la defensa.

<u>Acción 6:</u> ***Mejora de la seguridad del suministro de energía y de la resiliencia de las infraestructuras nucleares***

A raíz del compromiso que adquirió en septiembre de 2017 (Comunicación conjunta «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE»[7]), la Comisión seguirá prestando apoyo al Centro Europeo de Puesta en Común y Análisis de la Información sobre Energía en materia de ciberseguridad.

A fin de evitar crisis de suministro de gas, los Estados miembros y la Comisión están aplicando el Reglamento relativo a la seguridad del suministro de gas adoptado el pasado año, y la Comisión está facilitando su aplicación y la cooperación entre los Estados miembros en los grupos de riesgo. Las evaluaciones comunes de riesgos se han de notificar a la Comisión a más tardar el 1 de octubre del 2018. La Comisión recibirá los planes de acción preventiva y los planes de emergencias a más tardar el 1 de marzo de 2019. Los Estados miembros deberían celebrar los acuerdos bilaterales de solidaridad a más tardar el 1 de diciembre de 2018.

Con el fin de colmar el vacío reglamentario existente en materia de preparación para afrontar situaciones de riesgo relacionadas con la electricidad, el Reglamento sobre preparación frente a riesgos, que se está negociando, impondrá normas sobre la evaluación de riesgos, así como la obligación de que los Estados miembros elaboren un plan de preparación para afrontar riesgos que incluya ciertos elementos preceptivos, sobre cómo gestionar situaciones de crisis y sobre cómo vigilar la seguridad del suministro. Los planes de preparación para afrontar riesgos deberían incluir acuerdos de cooperación regional y, en especial, disposiciones para la gestión de situaciones de crisis eléctricas simultáneas. La ejecución el Reglamento sobre preparación frente a riesgos implica la elaboración por los Estados miembros de los primeros planes de preparación frente a riesgos dos años después de su entrada en vigor. A continuación, los planes se deberán actualizar cada tres años. El futuro Reglamento sobre preparación frente a riesgos supondrá asimismo la realización de ejercicios regulares y conjuntos entre los Estados miembros para simular crisis eléctricas. La Comisión ha iniciado ya la preparación de esos ejercicios conjuntos con los Estados miembros interesados, el Centro Común de Investigación y el Grupo de Coordinación de la Electricidad.

Respecto de la resiliencia de las infraestructuras nucleares, próximamente se mejorará el intercambio de información entre los Estados miembros y la Comisión sobre las cuestiones de seguridad nuclear, y está previsto que se lleve a cabo un análisis que servirá para establecer iniciativas adicionales. Se realizará un análisis de la normativa sobre salvaguardias nucleares y con vistas a una posible orientación para ayudar a los Estados miembros a gestionar mejor las fuentes (radiactivas) selladas de actividad elevada. A largo plazo, la Comisión reforzará las actividades del ámbito nuclear en las que los Estados miembros tengan un interés común y en las que se considere que el intercambio de información y la colaboración suponen un beneficio. También estudiará medidas apropiadas para la ejecución efectiva en la UE de la Convención internacional sobre la protección física de los materiales nucleares y las instalaciones nucleares.

En relación con el sector de la defensa, el Foro Consultivo de Energía Sostenible en el Sector de Defensa y Seguridad elaboró la Hoja de ruta para la gestión de la energía sostenible en la defensa y la seguridad, con el fin de ayudar al sector de la defensa a mejorar la gestión de las infraestructuras. El Foro consultivo seguirá estudiando cómo conseguir que los recursos energéticos del sector de la defensa ganen efectividad y revisará diversas tecnologías de generación de proyectos que dicho sector podría explotar (por ejemplo, energía eólica, energía

[7] JOIN(2017) 450 final.

solar, redes eléctricas inteligentes, almacenamiento de energía, combustibles biológicos, biomasa y recuperación energética).

En este contexto, la Agencia Europea de Defensa siguió trabajando en su programa de energía y medio ambiente mediante el proyecto de investigación sobre campamentos inteligentes de agua azul, con el fin de estudiar las posibilidades de intervención tecnológica para la gestión sostenible del agua en los campamentos militares «internos» y por medio del contrato de investigación del demostrador técnico de campamentos inteligentes, que estudia si es viable integrar una amplia gama de tecnologías energéticas y medioambientales a mayor escala en un entorno militar, de manera que se tengan presentes diversas consideraciones de los ámbitos de la energía, el agua y los residuos, a la vez que se mejoran la rentabilidad y la efectividad militar de las misiones de la PCSD.

<u>Acción 7</u>: Protección de los transportes y de las cadenas de suministro

En todas las áreas del transporte, a saber, la aviación civil y los transportes marítimo y terrestre, la Comisión ha intensificado los debates con los Estados miembros, la industria y otras partes interesadas sobre las nuevas amenazas para la seguridad de carácter híbrido, con el fin de adquirir conocimientos y aprender de la experiencia.

En el contexto de las actividades de aplicación y la revisión del Plan de Acción de la Estrategia de Seguridad Marítima de la UE, la Comisión está analizando las tendencias en seguridad marítima, incluidas la piratería y las controversias marítimas, que podrían alterar las rutas marítimas y comerciales y afectar a los intereses de la UE. Dado que los Estados miembros de la UE y los del EEE controlan más del 40 % de la flota mercante mundial y que la UE es un importante bloque comercial, los ataques híbridos en las rutas marítimas comerciales tendrían efectos perturbadores considerables en las cadenas europeas de valor y suministro. El análisis del riesgo y el control de las amenazas emergentes en el ámbito marítimo podrían dar lugar a propuestas encaminadas a actualizar la legislación específica del transporte, cuando corresponda. Estos elementos constituyen asimismo la base de una labor continua de mejora del conocimiento marítimo, en particular en el contexto del desarrollo del entorno común de intercambio de información con fines de vigilancia del ámbito marítimo de la UE (CISE), en el que recientemente, a principios de 2018, se han concedido tres nuevos proyectos en el marco de una nueva convocatoria de propuestas para ayudar a los Estados miembros a mejorar la interoperabilidad informática entre las autoridades marítimas nacionales.

Con la adopción del paquete de la Guardia Europea de Fronteras y Costas[8] en septiembre de 2016, el Parlamento Europeo y el Consejo introdujeron un artículo común en los reglamentos de base de la Agencia Europea de la Guardia de Fronteras y Costas, la Agencia Europea de Control de la Pesca (AECP) y la Agencia Europea de Seguridad Marítima (AESM) que les confiaba la tarea de reforzar su cooperación, cada una de ellas en el marco de su mandato, tanto con las otras dos como con las autoridades nacionales que desempeñan funciones de guardia de costas[9], con el fin de aumentar el conocimiento de la situación marítima y respaldar una actuación coherente y rentable. En 2017 se publicó un estudio sobre este tema en el que se examinaban las afinidades y las maneras de cooperar y de aplicar la

[8] Reglamento (UE) 2016/1624 del Parlamento Europeo y del Consejo, sobre la Guardia Europea de Fronteras y Costas.

[9] Las funciones de guardacostas son: 1) la seguridad marítima y la gestión del tráfico de buques; 2) los siniestros de buques y el servicio de asistencia marítima; 3) la inspección y el control de la pesca; 4) el control fronterizo marítimo; 5) la protección medioambiental marítima; 6) la prevención y la represión del tráfico ilícito y el contrabando y la aplicación del derecho marítimo correspondiente; 7) la búsqueda y el salvamento marítimos; 8) el control y la vigilancia marítimos; 9) las actividades aduaneras marítimas; 10) la gestión de los accidentes y desastres marítimos, y 11) la seguridad marítima, de los buques y de las instalaciones portuarias.

interoperabilidad en el ámbito de la evaluación del riesgo entre las autoridades que desempeñan las funciones de guardacostas10.

Los temas relacionados con el transporte y las amenazas emergentes, incluidos, entre otras cosas, los puertos, son las ciberamenazas a la seguridad aérea, las interferencias intencionadas y la falsificación de direcciones en los GPS, las amenazas a los satélites y los problemas en la región boreal y el Ártico. El Centro de Excelencia para la Lucha contra las Amenazas Híbridas de Helsinki también contribuye a examinar estas amenazas híbridas relacionadas con el transporte, y recientemente ha iniciado un análisis que se aplicará en la protección portuaria.

Las aduanas de la UE desempeñan actualmente un papel clave en la protección de la frontera exterior y de la cadena de suministro, con lo que contribuyen a la seguridad de la Unión Europea. La Comisión está realizando una mejora notable del sistema de información anticipada sobre la carga y de gestión de los riesgos aduaneros a fin de cerciorarse de que las aduanas de la UE obtienen toda la información necesaria, la comparten de manera más efectiva entre los Estados miembros, aplican normas comunes y específicas de los Estados miembros en materia de riesgo y gestionan los envíos de riesgo de manera efectiva. Una de las prioridades fundamentales del Plan de acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares (QBRN)[11] es garantizar la seguridad fronteriza y la capacidad de detección de entradas ilegales de materiales QBRN. La adaptación de los sistemas de información sobre la carga es esencial para reforzar la supervisión y los controles basados en el riesgo de las cadenas de suministro internacionales para que no entren en la UE de forma ilícita materiales QBRN. El Decimoquinto informe sobre los progresos realizados hacia una Unión de seguridad efectiva y genuina ofrece más detalles de las medidas adoptadas por la UE para mejorar la preparación ante los riesgos QBRN y, en particular, de las actuaciones llevadas a cabo a escala de la UE en el marco del Plan de acción de la Comisión para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares.

A fin de eliminar los obstáculos que dificultan la movilidad militar en la UE, el 28 de marzo de 2018 el Alto Representante y la Comisión presentaron un plan de acción para explorar las posibilidades de uso civil militar de la red transeuropea, simplificar las formalidades aduaneras del transporte militar y hacer frente a las cuestiones normativas y procedimentales relativas al transporte de mercancías peligrosas con fines militares. La Comisión propuso un presupuesto de 6 500 millones de euros con cargo a la categoría de «Defensa» del marco financiero plurianual, que se ejecutaría por medio del Mecanismo «Conectar Europa» para apoyar la infraestructura de transportes a fin de adaptarla a las necesidades de la movilidad militar. El objetivo es un uso dual civil-militar de la infraestructura de transportes.

Acción 8: ***Desarrollo de la resiliencia de los activos espaciales***

La propuesta de la Comisión de creación de un Programa Espacial de la Unión[12] integra aspectos de seguridad, en particular Copernicus, las comunicaciones gubernamentales por satélite y el marco de apoyo a la vigilancia y el seguimiento espacial, que cubrirían los aspectos referentes a la resiliencia ante las amenazas híbridas, además de las medidas que ya se están aplicando en relación con Galileo y EGNOS.

10 https://publications.europa.eu/en/publication-detail/-/publication/217db2fc-15d6-11e7-808e-01aa75ed71a1/language-en.

11 COM(2017) 610 final de 18.10.2017.

12 COM(2018) 447 final de 6.6.2018.

La vigilancia y el seguimiento espacial[13] tienen por objetivo respaldar la disponibilidad a medio plazo de las infraestructuras, las instalaciones y los servicios espaciales nacionales y europeos. Comenzaron en julio de 2016 prestando servicios iniciales para evitar colisiones, fragmentaciones y reentradas incontroladas de objetos espaciales. Los centros nacionales de operaciones de vigilancia y seguimiento espacial y el Centro de Satélites de la UE han establecido medidas de seguridad que tienen en cuenta las recomendaciones del Consejo sobre los aspectos de seguridad de la política de datos de conocimiento del medio espacial[14].

En lo referente a Galileo, la Comisión está dando nuevos pasos a fin de garantizar una mejor protección del suministro de datos clave para el buen funcionamiento de las infraestructuras críticas que dependen de la navegación por satélite para la planificación temporal y la sincronización. Se está estudiando la posibilidad de usar Galileo para prestar servicios en infraestructuras críticas, como las redes de energía, las redes de telecomunicaciones y los mercados financieros. En este contexto, la propuesta de Reglamento por el que se establece un marco para el control de las inversiones extranjeras directas presentada por la Comisión señala los programas de los sistemas globales europeos de navegación por satélite (GNSS) Galileo y EGNOS como ejemplos de proyectos o programas de interés para la Unión que pueden ser pertinentes para el control de las inversiones extranjeras directas con arreglo al Reglamento propuesto[15].

La iniciativa de comunicaciones gubernamentales por satélite de la UE dará acceso garantizado y asegurado a las comunicaciones por satélite con las misiones, operaciones e infraestructuras clave de la Unión y los Estados miembros. Se trata de una importante herramienta de lucha contra las amenazas híbridas a diversas infraestructuras, incluidas las espaciales y las de transportes y energía.

<u>Acción 9</u>: ***Adaptación de las capacidades de defensa y sobre desarrollo que sean pertinentes para la UE***

El Fondo Europeo de Defensa, que se puso en marcha el 7 de junio de 2017, constituye un paso importante para incentivar los esfuerzos de los Estados miembros por aumentar y mantener la colaboración en materia de defensa en Europa, con el fin de dar una respuesta efectiva a los retos estratégicos. La ventanilla de capacidades del Fondo permitirá a la UE, en particular, completar la financiación nacional destinada a los proyectos de desarrollo de una defensa colaborativa. A este fin, en junio de 2017 la Comisión propuso un Reglamento sobre el Programa Europeo de Desarrollo Industrial en materia de Defensa con un presupuesto de 500 millones de euros para 2019-2020. El 22 de mayo de 2018, el Parlamento Europeo y el Consejo llegaron a un acuerdo provisional sobre el proyecto de Reglamento. Para el próximo marco financiero plurianual de la UE, la Comisión ha propuesto un Fondo Europeo de Defensa integrado dotado de un ambicioso presupuesto de 13 000 millones de euros, de los que 8 900 millones de euros se destinarían a proyectos colaborativos de desarrollo de las capacidades en materia de defensa. El impacto potencial de la lucha contra las amenazas híbridas en el desarrollo de las capacidades se integrará en el Plan de Desarrollo de Capacidades revisado, que los Estados miembros aprobarán en junio de 2018.

<u>Acción 10</u>: ***Mecanismos de preparación y coordinación en materia sanitaria***

La preparación en materia sanitaria es un componente muy importante de la preparación ante los riesgos QBRN. Así pues, la Comisión ha tomado medidas, en el marco de su Plan de acción, para impulsar la preparación ante los riesgos relacionados con la seguridad química,

---

13 Decisión n.º 541/2014/UE del Parlamento Europeo y del Consejo de 16 de abril de 2014 por la que se establece un marco de apoyo a la vigilancia y el seguimiento espacial.

14 Space Situational Awareness Data Policy (14698/12), 9.10.2012.

15 Véase el anexo del documento COM(2017) 487 final.

biológica, radiológica y nuclear. En particular, sus esfuerzos se han centrado en las iniciativas dirigidas a compartir de manera eficaz conocimientos especializados.

Por ello la Comisión creó Chimera, un ejercicio para comprobar la preparación y la planificación de la respuesta a las amenazas transfronterizas graves de los sectores sanitario, civil y de la protección y la seguridad en toda la UE y en terceros países. El ejercicio de simulación incluía la propagación de una enfermedad contagiosa combinada con ataques cibernéticos a estructuras críticas, incluidos hospitales, a fin de poner a prueba los mecanismos, sistemas y herramientas de comunicación existentes a escala nacional y de la UE para responder a una amenaza híbrida. El ejercicio, que abarcaba toda la UE, se desarrolló en Luxemburgo los días 30 y 31 de enero de 2018. Contribuyó a respaldar el desarrollo de las capacidades intersectoriales y a mejorar la interoperabilidad y la coordinación entre los sectores sanitario, de la protección civil y de la seguridad a escala de la UE y de los Estados miembros, así como la colaboración con socios internacionales. El ejercicio ayudó asimismo a definir las responsabilidades y funciones actuales de todas las partes interesadas en la gestión de crisis por amenazas híbridas. Se comprobó la interacción entre el sistema de alerta precoz y respuesta (SAPR), el sistema general y seguro de alerta rápida de la Comisión (ARGUS), el Sistema Común de Comunicación e Información de Emergencia (SCCIE) y el Dispositivo Integrado de Respuesta Política a las Crisis del Consejo (DIRPC). El Decimoquinto informe de situación relativo a una Unión de la Seguridad genuina y efectiva proporciona más detalles sobre las medidas adoptadas por la UE para potenciar la preparación ante los riesgos QBRN.

En abril de 2018, la Comisión publicó una comunicación y presentó una propuesta de recomendación del Consejo para reforzar la cooperación en la UE contra las enfermedades que se pueden evitar con vacunas, con miras a que se adoptasen antes del final de 2018. El objetivo es responder a la cuestión de la vacilación ante las vacunas, mejorar la sostenibilidad de los programas de vacunación y reforzar la efectividad de la investigación y el desarrollo en materia de vacunas.

Desde la perspectiva del Cuerpo Médico Europeo, la Organización Mundial de la Salud (OMS) seleccionó al equipo noruego de emergencias médicas, lo que implica el cumplimiento de unos estándares de calidad mínimos. En abril de 2018 se celebró la primera reunión regional de los equipos de emergencias médicas de la región europea de la OMS. Esta reunión estaba organizada por la Comisión, la Organización Mundial de la Salud y las autoridades sanitarias belgas, que ocupaban la presidencia del grupo regional.

En la actualidad se está colaborando estrechamente con la Sociedad Europea de Quemados y los Estados miembros en los preparativos de un mecanismo para gestionar las catástrofes que resulten en un número elevado de quemados. A principios de octubre de 2018, la Comisión y los Estados miembros se reunirán en un taller para ultimar esta labor.

<u>Acción 11</u>: ***Red de CSIRT (equipos de respuesta a incidentes de seguridad informática), CERT de la UE y Directiva SRI***

El CERT de la UE elabora, de manera periódica y según las necesidades, productos de evaluación de ciberamenazas relacionados con sectores críticos. La Comisión supervisa regularmente las iniciativas sectoriales relativas a las ciberamenazas correspondientes a los diferentes modos de transporte (aéreo, marítimo y terrestre) y se cerciora de su coherencia con las capacidades intersectoriales cubiertas por la Directiva sobre la seguridad de las redes y sistemas de información (Directiva SRI).

En septiembre de 2017, la Agencia Europea de Defensa y la Presidencia estonia del Consejo de la UE organizaron un ciberejercicio teórico de simulación estratégica para los ministros de Defensa llamado CYBRID17, con el fin de concienciar de la coordinación política necesaria en caso de incidentes de seguridad informática y de los efectos potenciales de las

cibercampañas ofensivas. Este ejercicio se centró en el conocimiento de la situación, los mecanismos de gestión de crisis y la comunicación estratégica. La Agencia Europea de Defensa trasladará los elementos de este ejercicio a la plataforma de educación, formación, evaluación y ejercicio en materia de cibernética de la Escuela Europea de Seguridad y Defensa que se creará en septiembre de 2018. Las presidencias de la UE están estudiando la posibilidad de realizar otros ejercicios de alto nivel similares.

Acción 12: ***APPC para la ciberseguridad***

La Comisión firmó un acuerdo público-privado sobre ciberseguridad con la Organización de Ciberseguridad Europea (ECSO) para estimular las capacidades de competitividad e innovación de la seguridad digital y la industria de la privacidad en Europa. La UE invertirá hasta 450 millones de euros en esta asociación para proteger a los usuarios y las infraestructuras de los ciberataques. Se espera que esta APPC genere inversiones por valor de 1 800 millones de euros para 2020.

Respecto de la ciberseguridad, la Comunicación conjunta «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE[16] establece medidas para dar un fuerte impulso a las estructuras y capacidades de ciberseguridad de la UE, como se determina en la Comunicación conjunta. Sin embargo, en la UE la ciberseguridad efectiva se ve obstaculizada por una inversión insuficiente y una falta de coordinación. La UE está intentando subsanarlas tal como se establece en la Comunicación conjunta.

Acción 13: ***Resiliencia del sector de la energía***

En junio de 2018 la Comisión establecerá, en el marco del Grupo de cooperación SRI, un eje de trabajo para tratar las particularidades del sector energético y asesorar a los Estados miembros en la aplicación de la Directiva sobre la seguridad de las redes y sistemas de información (Directiva SRI) a este sector. En paralelo, la Comisión está trabajando en un asesoramiento específico en materia de ciberseguridad que va más allá de la Directiva SRI en la detección de buenas prácticas en ciberseguridad en el sector energético y que se ocupa de los operadores que no están cubiertos por esta Directiva. La Comisión seguirá organizando eventos de puesta en común de información en cuestiones de ciberseguridad en el sector energético con el fin de concienciar, compartir mejores prácticas, potenciar la cooperación (más allá de las fronteras y entre gestores de redes de transporte y operadores de sistemas de distribución), adoptar medidas físicas, afrontar nuevos riesgos y dar respuesta a las necesidades de educación y de capacitación.

A largo plazo, la Comisión creará un Código de red para las normas sectoriales específicas de la ciberseguridad, como se propone en la refundición del Reglamento de electricidad[17], que actualmente se encuentra en el proceso legislativo.

Acción 14: ***Resiliencia del sector financiero: plataformas y redes para la puesta en común de la información***

El Plan de acción Fintech de la Comisión se centra en las barreras potenciales a la puesta en común de información sobre ciberamenazas entre los actores del mercado financiero y determina posibles soluciones para superarlas. Por otra parte, el CERT de la UE desempeña un papel importante en la puesta en común de información sobre incidentes.

16 JOIN(2017) 450 final.

17 Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al mercado interior de la electricidad (refundición), COM(2016) 861 final.

<u>Acción 15</u>: ***Resiliencia ante los ataques cibernéticos en el sector del transporte***

Para la Comisión, proteger las diferentes modalidades de transporte de los ciberataques es una cuestión de máxima prioridad. En la aviación civil se ha avanzado mucho en ciberseguridad, pero no se puede descartar que los sistemas sean vulnerables a fallos técnicos o a amenazas, como quedó patente con el reciente incidente informático de Eurocontrol, que afectó a la mitad de los vuelos de Europa. La Comisión coopera estrechamente con la Agencia Europea de Seguridad Aérea en esta área del transporte. El CERT de la UE ha firmado un Acuerdo de Nivel de Servicio con Eurocontrol y un Memorándum de acuerdo con la Agencia Europea de Seguridad Aérea para ayudar a estas entidades y a sus partes interesadas a afrontar las ciberamenazas.

En el transporte marítimo, la industria naviera publicó unas orientaciones en ciberseguridad que posteriormente fueron debatidas y adoptadas por la Organización Marítima Internacional con una perspectiva y un enfoque principalmente globales. La ciberseguridad de las instalaciones portuarias y puertos europeos sigue teniendo una alta prioridad política entre los Estados miembros, la industria y las partes interesadas, que la tienen presente y la debaten en el contexto del despliegue y el seguimiento de la Directiva sobre la seguridad de las redes y sistemas de información.

La Comisión tiene previsto desarrollar un instrumento interactivo de gestión de los conocimientos en ciberseguridad que recomendará a los gestores y profesionales de la seguridad del sector del transporte una serie de buenas prácticas para detectar, evaluar y mitigar los riesgos en ciberseguridad.

<u>Acción 16</u>: ***Lucha contra la financiación del terrorismo***

En el último año, la Comisión ha realizado esfuerzos notables para luchar contra la financiación del terrorismo que se han recogido en los informes periódicos de seguridad de la Unión. Muy recientemente, en su paquete de seguridad de abril de 2018[18], la Comisión adoptó medidas adicionales para intensificar la cooperación entre las autoridades responsables de la lucha contra los delitos graves y el terrorismo y facilitar su acceso a la información financiera y el uso de esta, con una propuesta de Directiva[19] para facilitar el uso de información financiera y de otros tipos para la prevención, detección, investigación o enjuiciamiento de determinados delitos. En el Decimoquinto informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva se incluyen más detalles sobre la reciente labor realizada a escala de la UE en la lucha contra la financiación del terrorismo.

A fin de armonizar las sanciones por delitos de blanqueo de capitales, la Comisión propuso legislación que se podría adoptar a mediados de 2018. Por otra parte, en mayo de este año se adoptó la Quinta Directiva sobre blanqueo de capitales, con vistas a reforzar diversas medidas, como reforzar el control de los terceros países de alto riesgo, controlar las plataformas virtuales de intercambio de divisas, adoptar disposiciones que garanticen la transparencia de los instrumentos de prepago, atribuir nuevas competencias a las unidades de inteligencia financiera y agilizar el acceso a la información sobre los titulares de cuentas bancarias y de pago, mediante registros centralizados o sistemas de recuperación de datos electrónicos para las unidades de inteligencia financiera.

<u>Acción 17</u>: ***Acciones contra la radicalización y análisis de la necesidad de reforzar los procedimientos de supresión de contenidos ilegales***

En los últimos años, la prevención de la radicalización violenta, tanto en línea como fuera de línea, ha sido prioritaria para la Comisión. Para impulsar la labor al nivel de la UE, la

[18] COM(2018) 211 final.
[19] COM(2018) 213 final.

Comisión estableció un Grupo de expertos de alto nivel en materia de radicalización encargado de formular recomendaciones sobre la coordinación, el alcance y el impacto de las políticas preventivas de la UE. El 18 de mayo de 2018, el Grupo de expertos de alto nivel en materia de radicalización presentó su informe final, que incluye una recomendación de crear un mecanismo de cooperación de la UE.

Con vistas a abordar los contenidos ilegales en línea, a resultas de la adopción de la Recomendación de la Comisión de 1 de marzo de 2018, los esfuerzos se están centrando en reducir la accesibilidad a esos contenidos en línea. La Comisión ha puesto en marcha una evaluación del impacto para determinar si los esfuerzos que se están realizando son suficientes o si se necesitan medidas adicionales para garantizar la detección y la eliminación rápida y proactiva de los contenidos ilícitos en línea, incluidas posibles medidas legislativas que complementen el actual marco regulador. La labor que la Comisión ha llevado a cabo en este ámbito se expone con más detalle en el Decimoquinto informe sobre los progresos realizados hacia una Unión de seguridad efectiva y genuina.

El Código de conducta para luchar contra la difusión en línea de los discursos de odio adoptado con Facebook, Twitter, Google (YouTube) y Microsoft está dando resultados rápidos y positivos. El Código de conducta garantizaba un avance significativo de las empresas en la revisión rápida y la eliminación los discursos de odio notificados considerados ilegales. El tercer ejercicio de control de la Comisión sobre la aplicación del Código, publicado en enero de 2018, reveló que se retira una media del 70 % del contenido de incitación al odio y que las revisiones de estos contenidos se realizan en un plazo de veinticuatro horas, como se indica en el documento. El Código se ha convertido en una norma del sector y la reciente decisión de Instagram y Google+ de sumarse a su aplicación resulta alentadora. En marzo de 2018 la Comisión propuso también medidas adicionales para las plataformas en línea, como la detección automática, la transparencia y la información de retorno a los usuarios, además de salvaguardias para proteger la libertad de expresión[20].

Más allá de las acciones ya adoptadas contra la radicalización y el discurso de incitación al odio en línea, se han de tomar medidas para prevenir y mitigar las amenazas facilitadas por la informática en las elecciones.

<u>Acción 18</u>: Refuerzo de la cooperación con las regiones vecinas y terceros países

La Unión Europea se ha ido centrando más en el desarrollo de las capacidades y la resiliencia de los países socios en el sector de la seguridad, en particular desarrollando la dimensión de la seguridad de la política europea de vecindad revisada. Con el fin de mejorar las capacidades de los socios en la lucha contra las amenazas híbridas, se están poniendo en marcha unas encuestas con las que se pretende detectar las vulnerabilidades críticas y brindar apoyo específico. El SEAE, en coordinación con la Comisión, ha realizado una encuesta en Moldavia. En 2018, Jordania y Georgia han solicitado formalmente a la UE encuestas de vulnerabilidad. El primer paso consistirá en adaptar el cuestionario a sus necesidades concretas. En Ucrania se ha iniciado una labor complementaria sobre el desarrollo de las capacidades en materia de ciberseguridad, en particular para las infraestructuras críticas, mediante misiones de asistencia técnica, y a principios de 2018 la Comisión puso en marcha un nuevo programa global dirigido a aumentar la resiliencia cibernética de los terceros países de África y Asia.

La UE sigue debatiendo planes y programas de desarrollo de las capacidades en materia de seguridad nuclear con el Organismo Internacional de Energía Atómica y el Gobierno de los Estados Unidos en el seno del Grupo de trabajo sobre vigilancia en las fronteras. El Centro Europeo de Formación en Seguridad Nuclear (CEFSN) ofrece formación sobre prevención y

[20] COM(2018) 1177 final.

detección en seguridad nuclear y gestión de accidentes nucleares. El Plan de acción de la Comisión para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares contiene medidas específicas de cooperación con los principales socios internacionales, entre las que se incluyen actuaciones en el contexto de la lucha contra el terrorismo y diálogos sobre seguridad con los terceros países pertinentes.

La iniciativa de los centros de excelencia QBRN, que está financiada por la UE y cubre a casi todos los países socios vecinos[21], sigue adelante para mejorar las capacidades nacionales y regionales de los países socios en materia de prevención, preparación y gestión de estas amenazas, incluidas aquellas que afectan a las estructuras de «seguridad dura».

En los países vecinos del este y el sur de Europa se organizan cursos y ejercicios de protección civil en el marco de los programas regionales de prevención, preparación y respuesta ante catástrofes de origen natural o humano (PPRD). La tercera fase del PPRD Sur comenzó en 2018 y la segunda fase del PPRD Este terminará en noviembre de 2018, si bien es posible que se prorrogue. Será necesario garantizar vínculos estrechos con los centros de excelencia QBRN y los programas PPRD Sur y Este.

PREVENIR, RESPONDER A LAS CRISIS Y RECUPERARSE TRAS ELLAS

Aunque las consecuencias pueden atenuarse con políticas a largo plazo a escala nacional y de la UE, a corto plazo sigue siendo esencial 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. En el último año se ha avanzado mucho en este ámbito, y actualmente existe un protocolo de actuación en la UE que establece el proceso de gestión de las crisis en caso de atentado híbrido. En el futuro se seguirá adelante con el seguimiento y los ejercicios periódicos.

<u>Acción 19</u>: ***Protocolo operativo común y ejercicios para mejorar la capacidad decisoria estratégica en respuesta a amenazas híbridas complejas***

En junio de 2016 se elaboró el documento de trabajo conjunto en el que se establecía el protocolo operativo de la UE. En dicho protocolo se sentaban las bases de la gestión de crisis paninstitucional. Durante el EUPACE17 el protocolo se probó en un escenario híbrido y demostró su gran valor como herramienta para facilitar la interconexión entre servicios. Por otra parte, proporcionó los puntos de contacto para la interacción entre los diferentes niveles de respuesta: político, estratégico, operativo y técnico, así como entre los tres principales mecanismos de la UE de gestión de crisis (externas), ARGUS (la plataforma informática interna de la UE para la puesta en común de información) y la plataforma integrada de respuesta política a las crisis del Consejo. El protocolo también demostró su utilidad durante los ejercicios paralelos con la OTAN en el CMX 17. El próximo ejercicio de la serie PACE18 se desarrollará en noviembre de 2018. La experiencia adquirida se tendrá en cuenta para actualizar el protocolo.

En septiembre y octubre de 2017, la UE celebró el primer ejercicio paralelo y coordinado con la OTAN (PACE17), en el que se evaluaron la preparación y la interacción entre ambas organizaciones en caso de crisis híbrida a gran escala. En la fase preparatoria se realizaron intercambios intensivos de personal en los cuatro ámbitos de procedimiento de los protocolos de actuación conjunta para contrarrestar las amenazas híbridas: alerta rápida y conocimiento de la situación, comunicaciones estratégicas, ciberdefensa y prevención de crisis y respuesta a estas. El grado de interacción entre el personal de la UE y el de la OTAN durante el EUPACE17 no tiene precedentes. Además, era la primera vez que la OTAN participaba en

[21] Con centros de excelencia QBRN en Rabat, Argel, Amán y Tiflis.

una mesa redonda de gestión política integrada de crisis bajo la Presidencia del Consejo. En los debates del Consejo del Atlántico Norte participaron altos funcionarios de la UE. El proceso de adquisición de experiencia se centró en aspectos como la interacción entre los mecanismos de gestión de crisis de la UE y la OTAN y los retos relacionados con el intercambio de información confidencial entre el personal de ambas entidades, y en particular en la necesidad de comunicaciones seguras, con el objetivo principal de garantizar en el futuro un intercambio ágil y seguro que respete plenamente la necesidad de control de la fuente.

En la actualidad se está planificando el ejercicio paralelo y coordinado de 2018, que estará dirigido por la UE.

<u>Acción 20</u>: ***Examen de la aplicabilidad y las implicaciones prácticas del artículo 222 del TFUE y del artículo 42, apartado 7, del TUE en caso de atentado híbrido de gran alcance y gravedad***

La aplicabilidad de la cláusula de solidaridad de la UE y su mecanismo de asistencia mutua, así como la interacción entre ambas entidades y los mecanismos de gestión de la OTAN en los que se incluye la defensa colectiva establecida en el artículo 5, se siguen debatiendo y comprobando en los ejercicios de simulación de amenazas híbridas. El Centro de Excelencia para la Lucha contra las Amenazas Híbridas de Helsinki está interesado y preparado para seguir investigando y realizando ejercicios, con lo que ayudará a desarrollar un planteamiento común entre los Estados miembros y los Aliados.

<u>Acción 21</u>: ***Integración, aprovechamiento y coordinación de las capacidades de acción militar en la lucha contra las amenazas híbridas al amparo de la Política Común de Seguridad y Defensa***

En respuesta al encargo de integrar las capacidades militares de apoyo a la Política Exterior y de Seguridad Común y la Política Común de Seguridad y Defensa y tras un seminario con expertos militares celebrado en diciembre de 2016 y la orientación del Grupo del Comité Militar de la Unión Europea de mayo de 2017, el asesoramiento militar sobre la contribución militar de la UE a la lucha contra las amenazas híbridas en el seno de la Política Común de Seguridad y Defensa finalizó en julio de 2017. Esta labor se está llevando a cabo mediante el plan de aplicación de desarrollo del concepto. En consulta con el Centro de Excelencia para la Lucha contra las Amenazas Híbridas, el Estado Mayor de la UE está desarrollando un concepto de contribución militar a la lucha contra las amenazas híbridas, en particular por medio de misiones y operaciones de Política Común de Seguridad y Defensa.

Además, el Estado Mayor de la UE y los Estados miembros refuerzan día a día la alerta temprana al prestar apoyo en inteligencia militar a la célula de fusión de la UE contra las amenazas híbridas. La Capacidad Única de Análisis de Inteligencia respalda a los grupos de trabajo de comunicación estratégica del SEAE mediante asesoramiento militar para luchar contra las campañas de información errónea dirigidas a la UE y a los Estados miembros.

Las capacidades militares de lucha contra las amenazas híbridas se practicarán durante el ejercicio paralelo y coordinado con la OTAN de 2018 (PACE18). Sobre la base de la simulación de amenazas híbridas de PACE18, el Estado Mayor de la UE y el Estado Mayor Internacional de la OTAN celebrarán debates informales para garantizar su complementariedad en la lucha contra las amenazas híbridas en los casos en que exista coincidencia de necesidades, basándose en el principio de inclusividad y respetando la autonomía decisoria y las normas de protección de datos de cada organización.

COOPERACIÓN UE-OTAN

<u>Acción 22:</u> ***Cooperación UE-OTAN en conocimiento de la situación, comunicaciones estratégicas, ciberseguridad y «prevención y gestión de crisis»***

La lucha contra las amenazas híbridas sigue siendo un ámbito clave de la interacción entre la UE y la OTAN, pues, en caso de amenaza híbrida, los recursos y las capacidades que estas dos organizaciones pueden movilizar son complementarios y potencian la capacidad de los Estados miembros y los Aliados de prevenir tales amenazas, disuadir de ellas y reaccionar. El ejercicio PACE17 ha puesto a prueba los protocolos de actuación de ambas organizaciones y ha demostrado su capacidad de colaborar de manera ágil y efectiva en apoyo de aquellos de sus miembros que se vean afectados. Ambos protocolos de actuación se revisarán y actualizarán a la luz de la experiencia adquirida. En el ámbito de las comunicaciones estratégicas, se han desarrollado consultas de apoyo a Ucrania, Bosnia y Herzegovina, la Moldavia y Georgia.

En septiembre de 2017 se llevó a cabo un taller de resiliencia UE-OTAN en el que expertos de sectores estratégicos críticos intercambiaron información sobre sus respectivas actividades y analizaron propuestas de trabajo para el futuro, en especial en el ámbito de la protección de las infraestructuras estratégicas críticas.

El proyecto Movilidad Militar de 2018 tiene por objetivo facilitar el desplazamiento de material y personal militar. Este proyecto podría tener en cuenta los retos que probablemente plantearán las amenazas híbridas diseñados explícitamente para para ralentizar la reacción de los Estados miembros y los Aliados. En las series EUPACE19 y EUPACE20 se programarán ejercicios paralelos que tendrán en cuenta esta cuestión.

La coordinación de los esfuerzos en materia de ciberformación constituye un importante ámbito en el que conviene intensificar la interacción. La OTAN participó también como observador en el ejercicio teórico de CyberEurope de la ENISA realizado en junio de 2018.

CONCLUSIÓN

La mejora del conocimiento de la situación y el desarrollo de la resiliencia ante la evolución de las amenazas híbridas de diferentes orígenes siguen constituyendo un reto que requiere el esfuerzo constante de la UE. La Comunicación conjunta recoge una amplia serie de actuaciones que van de la mejora de la fusión y el intercambio de información al refuerzo de la protección de las infraestructuras críticas y la ciberseguridad y el desarrollo de la resiliencia ante la radicalización y el extremismo violento en la sociedad. El marco de la UE de lucha contra las amenazas híbridas ha facilitado el apoyo a los Estados miembros por medio de diferentes medidas dirigidas a consolidar la capacidad de la UE y los Estados miembros de soportar el estrés, responder de manera coordinada a los ataques y, finalmente, recuperarse.

La reacción de la UE a las amenazas híbridas ha superado las pruebas y se ha practicado conjuntamente con la OTAN en diversos ejercicios. El plan continuará en esta línea. La clave de los esfuerzos necesarios para desarrollar la resiliencia radica en la estrecha cooperación entre todos los agentes pertinentes de la UE y la OTAN. Por otra parte, al apoyar a los países vecinos en la detección de sus vulnerabilidades y el refuerzo de sus capacidades de lucha contra las amenazas híbridas, se contribuye a que la naturaleza de las amenazas externas se comprenda mejor y, por tanto, se potencia la seguridad de los vecinos de la Unión.