COMISIÓN
EUROPEA

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

Bruselas, 19.7.2017
JOIN(2017) 30 final

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

1. INTRODUCCIÓN

La UE se enfrenta a uno de los mayores retos en materia de seguridad de su historia. Las amenazas adoptan cada vez más formas no convencionales; algunas físicas, como las nuevas formas de terrorismo; algunas que utilizan el espacio digital con ciberataques complejos; otras más sutiles destinadas a aplicar presión coercitiva, como campañas de desinformación y manipulación mediática. Tratan de debilitar los valores europeos fundamentales, como la dignidad humana, la libertad y la democracia. Los recientes ciberataques coordinados en todo el mundo, cuya atribución ha resultado difícil, han demostrado la vulnerabilidad de nuestras sociedades e instituciones.

En abril de 2016, la Comisión Europea y la Alta Representante adoptaron una Comunicación conjunta sobre la lucha contra las amenazas híbridas[1] (Comunicación conjunta). Reconociendo la naturaleza compleja y transfronteriza de las amenazas híbridas, dicha Comunicación propone «una perspectiva de la administración en su conjunto» para reforzar la resiliencia general de nuestras sociedades. El Consejo[2] acogió con satisfacción la iniciativa y las acciones propuestas, e invitó a la Comisión y a la Alta Representante a que le informaran sobre los avances al respecto en julio de 2017. Si bien la UE puede ayudar a los Estados miembros a reforzar su resiliencia ante las amenazas híbridas, la responsabilidad principal recae en los Estados miembros, ya que la lucha contra las amenazas híbridas constituye un asunto de defensa y seguridad nacional.

Dicha Comunicación conjunta sobre la lucha contra las amenazas híbridas constituye una parte importante del enfoque general más integrado de la UE en materia de defensa y de seguridad. Contribuye a la creación de una Europa que proteja, tal como pidió el presidente Juncker en su discurso sobre el Estado de la Unión de septiembre de 2016. En 2016, la Unión Europea también sentó las bases de una política de defensa europea más sólida para responder a las expectativas de los ciudadanos de una mayor protección. La Estrategia Global sobre Política Exterior y de Seguridad de la UE[3] detalló la necesidad de un enfoque integrado para vincular la resiliencia interna con las acciones exteriores de la UE y reclamó sinergias entre la política de defensa y las políticas que cubren el mercado interior, la industria, y los servicios policiales y de inteligencia. A raíz de la adopción, en noviembre de 2016, del Plan de Acción Europeo de Defensa, la Comisión presentó iniciativas concretas que contribuirán a fortalecer la capacidad de la UE de responder a las amenazas híbridas, fomentando la resiliencia en las cadenas de suministro de defensa y reforzando el mercado único de la defensa. En particular, el 7 de junio de 2017, la Comisión puso en marcha el Fondo Europeo de Defensa, con una propuesta de financiación de 600 millones EUR hasta 2020 y 1 500 millones EUR anuales a partir de 2020. La Comunicación sobre la Unión de la Seguridad[4] reconoció la necesidad de contrarrestar las amenazas híbridas y la importancia de garantizar una mayor coherencia entre las acciones de seguridad internas y externas.

[1] Comunicación conjunta al Parlamento Europeo y al Consejo «Comunicación conjunta sobre la lucha contra las amenazas híbridas - Una respuesta de la Unión Europea», JOIN (2016) 18 final.
[2] Conclusiones del Consejo sobre la lucha contra las amenazas híbridas, comunicado de prensa 196/16, de 19 de abril de 2016.
[3] Presentada por la Alta Representante al Consejo Europeo el 28 de junio de 2016.
[4] COM(2016) 230 final de 20.4.2016.

Los dirigentes de la UE han puesto la seguridad y la defensa en el centro del debate sobre el futuro de Europa[5]. Esta circunstancia se reconoció en la **Declaración de Roma** de 25 de marzo de 2017, que expuso la visión de una Unión segura y comprometida con el fortalecimiento de su política común de seguridad y defensa. Los Presidentes del Consejo Europeo, la Comisión Europea y el Secretario General de la OTAN firmaron una Declaración conjunta en Varsovia el 8 de julio de 2016 con el fin de dar un nuevo impulso y un nuevo contenido a la asociación estratégica UE-OTAN. La Declaración conjunta señaló siete ámbitos concretos, incluida la lucha contra las amenazas híbridas, en los que debe ampliarse la cooperación entre ambas organizaciones. Un conjunto común de 42 propuestas de aplicación fue refrendado posteriormente por los Consejos de la UE y la OTAN y el primer informe, que mostraba progresos sustanciales, se publicó en junio de 2017[6].

El documento de reflexión de la Comisión sobre el futuro de la defensa europea presentado en junio de 2017[7] esboza diferentes escenarios posibles sobre cómo abordar las crecientes amenazas a la seguridad y la defensa a que se enfrenta Europa y mejorar las capacidades de defensa propias de aquí a 2025. En los tres casos, la seguridad y la defensa son consideradas como parte integral del proyecto europeo, a fin de proteger y promover nuestros intereses en nuestro territorio y en el extranjero. Europa debe convertirse en un proveedor de seguridad y garantizar progresivamente su propia seguridad. Ningún Estado miembro puede afrontar los retos futuros en solitario, en particular el de la lucha contra las amenazas híbridas. La cooperación en materia de seguridad y defensa no es, pues, una opción; es una necesidad para ofrecer resultados en una Europa que proteja.

El objetivo del presente informe es dar cuenta de los avances y de los próximos pasos sobre las acciones en los cuatro ámbitos propuestos en la Comunicación conjunta: 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; y mejorar la cooperación con la OTAN para garantizar la complementariedad de las medidas. Debe leerse en relación con los informes mensuales de situación relativos a una Unión de la Seguridad genuina y efectiva.

2. RECONOCER LA NATURALEZA HÍBRIDA DE UNA AMENAZA

Las actividades híbridas se están convirtiendo en una característica frecuente del entorno de la seguridad europea. La intensidad de estas actividades es cada vez mayor y crece la preocupación por las interferencias en las elecciones, las campañas de desinformación, las actividades cibernéticas hostiles y los autores de actos híbridos que intentan radicalizar a miembros vulnerables de la sociedad que actúan por delegación. La vulnerabilidad a las amenazas híbridas no se limita a las fronteras nacionales. Las amenazas híbridas necesitan una respuesta coordinada también a nivel de la UE y la OTAN. La evolución de la situación desde abril de 2016 muestra que, a pesar de que las amenazas siguen a menudo evaluándose aisladamente, en la Unión aumenta el reconocimiento y la comprensión de la naturaleza

[5] Hoja de Ruta de Bratislava del Consejo Europeo, de 16 de septiembre de 2016, y Declaración de Roma de los dirigentes de los 27 Estados miembros y del Consejo Europeo, el Parlamento Europeo y la Comisión Europea, de 25 de marzo de 2017.

[6] http://www.consilium.europa.eu/es/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation

[7] Documento de reflexión sobre el futuro de la defensa europea, de 7.6.2017, https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_es.pdf

híbrida de algunas de las actividades observadas y de la necesidad de una actuación coordinada. La UE proseguirá sus esfuerzos para mejorar el conocimiento de la situación y la cooperación.

<u>Acción 1</u>: 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.

El Consejo ha creado un grupo de «Amigos de la Presidencia», que reúne a expertos de los Estados miembros para elaborar una encuesta genérica que permita identificar mejor los indicadores clave de las amenazas híbridas, incorporarlos a los mecanismos de evaluación de riesgos existentes y de alerta temprana y compartirlos, si procede. Se ha acordado un mandato y ya han comenzado los trabajos. La encuesta genérica debería estar lista a finales de 2017 y las encuestas empezarían justo después. La protección contra las amenazas híbridas debe reforzarse mutuamente. Por lo tanto, se anima a los Estados miembros a efectuar estas encuestas en el plazo más breve posible, lo que facilitará valiosa información sobre el grado de vulnerabilidad y preparación en toda Europa.

a. MEJORAR LA CONCIENCIACIÓN

La puesta en común de la labor de evaluación y análisis de la información es una herramienta clave para reducir la incertidumbre y mejorar el conocimiento de la situación. Se han realizado importantes progresos durante el pasado año. Se ha creado la célula de fusión de la UE contra las amenazas híbridas, que ya es plenamente operativa, así como el Grupo de Trabajo East StratCom, y Finlandia ha puesto en marcha el Centro Europeo para la Lucha contra las Amenazas Híbridas. Gran parte del trabajo se ha centrado en el análisis de las herramientas y medios de propaganda y desinformación, y existe una buena cooperación entre el Grupo de Trabajo East StratCom, la célula de fusión contra las amenazas híbridas y la OTAN. Esto constituye una buena base para seguir construyendo una cultura que analice y evalúe más profundamente las amenazas a nuestra seguridad interior y exterior con una óptica híbrida.

<u>Célula de fusión contra las amenazas híbridas</u>

<u>Acción 2</u>: Creación de una célula de fusión de la UE contra las amenazas híbridas en el seno de la estructura del Centro de Análisis de Inteligencia 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.

Se ha creado la célula de fusión de la UE contra las amenazas híbridas, en el seno del Centro de Análisis de Inteligencia de la UE, para recibir y analizar información clasificada y de dominio público relativa a amenazas híbridas, procedente de diferentes partes interesadas. El análisis se comparte dentro de la UE y entre los Estados miembros, y a su vez alimenta los procesos decisorios de la UE, lo que incluye los insumos de las evaluaciones del riesgo para la seguridad realizadas a escala de la UE. La División de Inteligencia del Estado Mayor de la UE contribuye a la labor de la célula de fusión con análisis militares. Hasta la fecha, se han realizado más de 50 evaluaciones y sesiones informativas sobre temas híbridos. Desde enero de 2017, la célula ha elaborado periódicamente un «boletín híbrido», que analiza las cuestiones híbridas y las amenazas actuales, y que se comparte directamente con las

instituciones y organismos de la UE y los puntos de contacto nacionales[8]. Tal y como estaba previsto, en mayo de 2017 se ha alcanzado la capacidad operativa plena de la célula. Por último, continúa el compromiso entre miembros del personal con la incipiente sección de análisis híbrido de la OTAN, tanto compartiendo la experiencia adquirida en la creación de la célula de fusión como poniendo en común información (respetando plenamente las normas de la UE sobre intercambio de información clasificada). La célula de fusión de la UE contra las amenazas híbridas está actualmente identificando nuevas iniciativas para reforzar la futura cooperación, y desempeñará un papel clave en los ejercicios paralelos UE-OTAN, previstos para otoño de 2017, en los que se pondrá a prueba la capacidad de respuesta de la célula de fusión de la UE contra las amenazas híbridas y se incorporarán las lecciones extraídas.

Comunicación estratégica

Acción 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.

En los últimos meses, el incremento de las campañas de desinformación y la propagación sistemática de noticias falsas en los medios de comunicación social son algunas de las medidas utilizadas para debilitar a los adversarios. En los casos en que los medios de comunicación social son la plataforma preferida, una información que parezca fiable y legítima puede hacer cambiar a la opinión pública en beneficio de algunos individuos, organizaciones o administraciones. Estas tácticas híbridas tienen el objetivo más amplio de crear confusión en nuestras sociedades y desacreditar a los gobiernos democráticos y a nuestras estructuras, instituciones y elecciones. Las noticias falsas suelen propagarse a través de plataformas en línea (véase también la acción 17). La Comisión y la Alta Representante acogen con satisfacción las medidas recientemente adoptadas por algunos medios de comunicación y plataformas en línea para luchar contra la desinformación. La Comisión seguirá fomentando este tipo de medidas voluntarias.

La Alta Representante ha puesto en marcha el Grupo de Trabajo East StratCom, que prevé los casos y las campañas de desinformación y responde a los mismos. Esto mejora considerablemente la comunicación sobre las políticas de la Unión en los países de la vecindad oriental y también refuerza el entorno mediático en estos países. El Grupo de Trabajo ha descubierto en los últimos dos años más de 3 000 casos diferentes de desinformación en 18 lenguas. La próxima puesta en marcha de un nuevo sitio web (#EUvsdisinformation) con un mecanismo de búsqueda en línea mejorará considerablemente el acceso de los usuarios a la información. Sin embargo, algunos trabajos de investigación y análisis muestran que el número de canales de desinformación y mensajes difundidos diariamente es mucho mayor. El proyecto EU-STRAT, financiado por Horizonte 2020, analiza la política y los medios de comunicación en los países de la Asociación Oriental.

La Alta Representante invita a los Estados miembros a apoyar la labor de los grupos de trabajo StratCom para combatir de manera más eficaz el crecimiento de las amenazas híbridas. Esto ayudará al Grupo Operativo Sur a mejorar la comunicación y el acercamiento al mundo árabe, incluso en lengua árabe, combatir las ideas erróneas y comunicar información objetiva sobre la Unión Europea y sus políticas. La interacción con los periodistas locales

[8] Hasta la fecha, 21 Estados miembros han designado puntos de contacto nacionales. Se trata de personas que trabajan en las capitales de los Estados miembros en funciones políticas y de resiliencia.

contribuirá a garantizar que las noticias estén culturalmente adaptadas. Ambos grupos de trabajo, con el apoyo de la célula de fusión de la UE contra las amenazas híbridas, pretenden apoyar y complementar los esfuerzos correspondientes de los Estados miembros. Además, la Comisión cofinancia el Equipo Consultivo sobre Comunicaciones Estratégicas, una red de colaboración de 26 Estados miembros que comparte análisis, buenas prácticas e ideas sobre el uso de comunicaciones estratégicas en la lucha contra el extremismo violento, en particular sobre desinformación.

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

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

En respuesta a la convocatoria de propuestas para crear un centro de excelencia, en abril de 2017, Finlandia puso en marcha el Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas. Diez Estados miembros de la UE[9], Noruega y los Estados Unidos son miembros, y la Unión Europea y la OTAN han sido invitadas a prestar apoyo a la junta directiva[10]. La misión del Centro es fomentar el diálogo estratégico, así como la realización de actividades de investigación y análisis, trabajando con las comunidades de interés para mejorar la resiliencia y la capacidad de respuesta, con el fin de contribuir a la lucha contra las amenazas híbridas. El Centro debería servir también de plataforma para futuros ejercicios híbridos. El Centro ya ha establecido estrechos contactos con la célula de fusión de la UE contra las amenazas híbridas, y la labor de ambas organizaciones debe complementarse. Actualmente, la UE está analizando cómo puede brindar apoyo concreto al Centro.

b. REFORZAR LA RESILIENCIA

La Comunicación conjunta pone la resiliencia (p. ej., de las infraestructuras de transporte, comunicaciones, energía, finanzas o seguridad regional) en el centro de la acción de la UE para oponerse a las campañas de información y propaganda, a los intentos de debilitar a las empresas, las sociedades y los flujos económicos, así como a los ataques a la tecnología de la información y la infraestructura ciberrelacionada. Considera que el refuerzo de la resiliencia es un recurso preventivo y disuasorio para solidificar las sociedades y evitar la escalada de las crisis, tanto dentro como fuera de la UE. El valor añadido de la UE reside en ayudar a los Estados miembros y los países socios a aumentar su resiliencia, a partir de una amplia gama de instrumentos y programas existentes. Se han hecho progresos significativos en acciones 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.

Protección de las infraestructuras críticas

Acción 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.

[9] Alemania, España, Estonia, Finlandia, Francia, Letonia, Lituania, Polonia, Suecia y el Reino Unido.
[10] El Centro está abierto a que se adhieran a él otros Estados miembros de la UE y aliados de la OTAN.

En el contexto del Programa Europeo para la Protección de Infraestructuras Críticas (PEPIC), la Comisión hizo avanzar los trabajos para identificar herramientas comunes, incluidos los indicadores de vulnerabilidad, a fin de mejorar la resiliencia de las infraestructuras críticas ante las amenazas híbridas en los sectores pertinentes. En mayo de 2017, la Comisión organizó un taller sobre las amenazas híbridas para las infraestructuras críticas, en el que participaron casi todos los Estados miembros, los operadores de infraestructuras críticas, la célula de fusión de la UE contra las amenazas híbridas y la OTAN en calidad de observadora. Se llegó a un acuerdo sobre una hoja de ruta común y medidas para el futuro trabajo, a partir de un cuestionario enviado a las autoridades nacionales de los Estados miembros. La Comisión proseguirá sus consultas con las partes interesadas en otoño, con el fin de llegar a un acuerdo sobre una serie de indicadores de aquí a finales de 2017.

La Agencia Europea de Defensa trabaja para identificar carencias de capacidad y de investigación comunes derivadas de la relación entre las capacidades de defensa y las infraestructuras energéticas. La Agencia Europea de Defensa elaborará un documento conceptual en otoño de 2017, así como acciones piloto de metodologías holísticas.

Aumentar la seguridad de abastecimiento energético de la UE.

Acción 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.

La Comisión formuló propuestas concretas en el paquete de seguridad del abastecimiento en diciembre de 2016 y abril de 2017, y el Consejo y el Parlamento Europeo llegaron a un acuerdo sobre el nuevo Reglamento de seguridad del suministro de gas, que pretende evitar las crisis de suministro de gas. Las nuevas normas garantizarán un enfoque común y coordinado regionalmente de las medidas de seguridad de suministro entre los Estados miembros. Esto hará que la UE esté mejor preparada para los problemas de escasez de gas y los gestione mejor, en caso de crisis o atentado híbrido. Por primera vez, se aplicará el principio de solidaridad: los Estados miembros podrán ayudar a los países vecinos en caso de atentado o crisis grave, de modo que las empresas y los hogares europeos no sufran cortes de suministro.

La UE también ha avanzado en el desarrollo de proyectos clave, con el fin de diversificar sus rutas y fuentes de abastecimiento energético en consonancia con la Estrategia Marco de la Unión de la Energía y la Estrategia Europea de Seguridad Energética. Por ejemplo, en el Corredor Meridional de Gas, se están realizando obras de construcción en todos los principales gasoductos: la expansión del gasoducto del Cáucaso Meridional, los oleoductos transanatolio y transadriático, el abastecedor Shah Deniz II, así como la ampliación del Corredor Meridional de Gas a Asia Central, en particular a Turkmenistán. Las importaciones de gas natural licuado (GNL) a Europa están aumentando y proceden de nuevas fuentes, como los Estados Unidos. El ejemplo de la terminal de Lituania muestra cómo los proyectos de diversificación pueden reducir la dependencia de un único proveedor. Reforzar los esfuerzos energéticos y hacer mejor uso de las fuentes de energía autóctonas, en especial las energías renovables, contribuye también a la diversificación de las rutas y fuentes energéticas.

En el ámbito de la seguridad nuclear, la Comisión está apoyando activamente, en particular a través de talleres con las autoridades nacionales y reguladoras, una aplicación coherente y eficaz de las dos Directivas sobre seguridad nuclear y normas básicas de seguridad, que los

Estados miembros deben transponer no más tarde de finales de 2017 y 2018, respectivamente. Además, el Programa de Investigación y Formación de Euratom contribuye a aumentar la seguridad nuclear.

Transporte y protección de las cadenas de suministro

Acción 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 Estrategia de Seguridad Marítima de la UE y de la estrategia de gestión de riesgos aduaneros de la UE junto con sus planes 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.

En consonancia con la Comunicación sobre la Unión de la Seguridad, la Comisión está facilitando evaluaciones del riesgo para la seguridad a escala de la UE, junto con los Estados miembros, el Centro de Análisis de Inteligencia de la UE y las agencias pertinentes, a fin de identificar amenazas a la seguridad de los transportes y apoyar la elaboración de medidas paliativas eficaces y proporcionadas. El derribo del vuelo MH17 de Malaysia Airlines en Ucrania oriental en 2014 puso de manifiesto el riesgo que plantea sobrevolar zonas de conflicto. En consonancia con las recomendaciones del Grupo de trabajo europeo de alto nivel sobre zonas en conflicto[11], la Comisión ha desarrollado una metodología de evaluación de riesgos conjunta de la UE, con el apoyo de expertos nacionales en seguridad y aviación y el SEAE, que permite el intercambio de información clasificada y la definición de una visión común de los riesgos. En marzo de 2017, la Agencia Europea de Seguridad Aérea (AESA) publicó el primer «boletín de información sobre zonas de conflicto»[12], a partir de los resultados de dicha evaluación de riesgos conjunta de la UE. La Comisión está estudiando ampliar las actividades de evaluación de riesgos llevadas a cabo en el ámbito de la seguridad de la aviación a otros modos de transporte (por ejemplo, ferrocarril o transporte marítimo) y se harán propuestas en 2018. En junio de 2017, la Comisión, el SEAE y los Estados miembros han puesto en marcha un ejercicio de evaluación de riesgos sobre seguridad ferroviaria para identificar carencias y posibles medidas para atenuar los riesgos.

Se han hecho considerables esfuerzos en materia de seguridad aérea y gestión del tránsito aéreo (GTA) en los proyectos de investigación sobre seguridad del 7.º Programa Marco y del programa Horizonte 2020. En el ámbito de la aviación civil, la Comisión, junto a la Agencia Europea de Seguridad Aérea y las partes interesadas, está desarrollando dos nuevas iniciativas para reforzar la ciberseguridad y también la lucha contra las amenazas híbridas: la creación del Equipo de Respuesta a Emergencias Informáticas sobre aviación, y la creación de un grupo operativo sobre ciberseguridad en la Empresa Común para la Investigación sobre la gestión del tránsito aéreo en el Cielo Único Europeo (SESAR), responsable de la gestión del tránsito aéreo en el Cielo Único Europeo. La Agencia Europea de Defensa proporciona los insumos militares sobre ciberseguridad aérea a la Empresa Común SESAR, así como a la Agencia Europea de Seguridad Aérea a través de la «Plataforma de Coordinación de la Estrategia Europea en materia de ciberseguridad», que, a petición de los Estados miembros y la industria, contribuirá a coordinar a nivel de la UE todas las actividades en el ámbito de la aviación. En consonancia con la hoja de ruta sobre ciberseguridad en la aviación, en 2016 la

[11] https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

[12] https://ad.easa.europa.eu/czib-docs/page-1

Agencia Europea de Seguridad Aérea llevó a cabo análisis de deficiencias de las normas existentes y, en particular, la definición y la creación del Centro Europeo de Ciberseguridad en la Aviación; este último está ahora operativo y coopera con el equipo de respuesta a emergencias informáticas CERT-UE (Memorando de Acuerdo firmado en febrero de 2017) elaborando análisis de amenazas para la aviación, así como con Eurocontrol (se ha adoptado una hoja de ruta para la cooperación), y se ha creado un sitio web para la distribución de análisis de fuentes abiertas. En otoño de 2017, se adoptará un programa de normalización y un intercambio seguro de información.

Gestión de los riesgos aduaneros

Desde una perspectiva aduanera, la Comisión se centra en mejorar de forma significativa el sistema de información anticipada sobre la carga y de gestión de riesgos aduaneros. Esto abarca la gama completa de riesgos aduaneros, incluso los relacionados con las amenazas a la seguridad y la integridad de las cadenas de suministro internacionales y a las infraestructuras críticas correspondientes (p. ej., las amenazas directas que plantean las importaciones a las instalaciones portuarias, los aeropuertos o las fronteras terrestres). La modernización tiene por objeto garantizar que las aduanas de la UE recaben toda la información necesaria de los operadores en lo que se refiere a la circulación de mercancías; que puedan compartir esta información de manera más eficaz con los Estados miembros; que apliquen normas sobre riesgos comunes, así como específicas de los Estados miembros; y que sean capaces de identificar más eficazmente las partidas de riesgo cooperando más estrechamente con otras autoridades, en particular, con otras agencias de seguridad y de aplicación de la legislación. El desarrollo de las tecnologías de la información necesarias para aplicar esta mejora por parte de la Comisión se encuentra actualmente en su fase inicial, y las inversiones pertinentes a nivel central se pondrán en marcha en los próximos meses.

Espacio

Acción 8: En el contexto de la 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.

La Comisión, a la hora de preparar el marco normativo de comunicaciones por satélite gubernamentales (GovSatCom) y de vigilancia y seguimiento espacial en 2018, integrará los aspectos de resiliencia ante las amenazas híbridas en su evaluación. En consonancia con la Estrategia espacial, al preparar la evolución de los programas Galileo y Copernicus, la Comisión evaluará el potencial de estos servicios para contribuir a paliar el problema de la vulnerabilidad de las infraestructuras críticas. El informe de evaluación debería estar listo en el otoño de 2017 y la propuesta sobre la próxima generación de Copernicus y Galileo en 2018. La Agencia Europea de Defensa está trabajando en proyectos colaborativos de desarrollo de capacidades en el ámbito de las comunicaciones basadas en el espacio, el posicionamiento militar, la navegación y la temporización, y la observación de la Tierra. Todos los proyectos se centrarán en las necesidades de resiliencia a la luz de las amenazas híbridas actuales y emergentes.

Capacidades de defensa

<u>Acción 9</u>: 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.

En 2016 y 2017, la Agencia Europea de Defensa realizó tres ejercicios de simulación sobre posibles escenarios de amenazas híbridas, junto con la Comisión, el SEAE y expertos de los Estados miembros. Sus resultados se tendrán en cuenta en la revisión del Plan de Desarrollo de Capacidades, de manera que las mejoras de la capacidad clave resultantes que se necesiten para hacer frente a las amenazas híbridas se integrarán en las nuevas prioridades de desarrollo de capacidades de la UE. Los trabajos de revisión del Catálogo de Necesidades de 2005 tendrán en cuenta la dimensión de las amenazas híbridas. En abril de 2017, la Agencia Europea de Defensa finalizó un informe de análisis sobre las implicaciones militares de los atentados híbridos contra las infraestructuras críticas portuarias, que se debatirá en un taller con expertos marítimos en octubre de 2017. Otro análisis específico de la función militar en el contexto de la lucha contra minidrones está previsto para 2018. Por otra parte, las prioridades para reforzar las capacidades de resiliencia ante las amenazas híbridas identificadas por los Estados miembros también podrían ser subvencionables en el marco del Fondo Europeo de Defensa a partir de 2019. La Comisión invita a los colegisladores a garantizar su rápida adopción, y a los Estados miembros a que presenten propuestas de proyectos de capacitación para reforzar la resiliencia de la UE ante las amenazas híbridas.

<u>Acción 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.

Para reforzar la preparación y la resiliencia ante las amenazas híbridas, incluidas las capacidades de los sistemas de salud y alimentario, la Comisión apoya a los Estados miembros mediante formación y ejercicios de simulación, así como facilitando el intercambio de directrices de experiencia y la financiación de acciones conjuntas. Este proceso se realiza en particular a través del marco de seguridad sanitaria de la UE sobre las amenazas transfronterizas graves para la salud y del Programa de Salud Pública para aplicar el Reglamento Sanitario Internacional, un pilar legislativo vinculante para 196 países, entre ellos los Estados miembros, que tiene por objeto prevenir y responder a los riesgos transfronterizos graves para la salud pública en todo el mundo. Para comprobar la preparación y respuesta intersectorial en el sector sanitario, los servicios de la Comisión llevarán a cabo un ejercicio sobre las amenazas híbridas complejas y multidimensionales en el otoño de 2017. La Comisión y los Estados miembros están elaborando una acción conjunta sobre vacunación, que incluye una previsión de la demanda y suministro de vacunas e investigación sobre procesos innovadores de fabricación de vacunas, con vistas a reforzar el suministro de vacunas y la seguridad sanitaria a nivel de la UE (2018-2020). La Comisión colabora también con la Autoridad Europea de Seguridad Alimentaria y el Centro Europeo para la Prevención y el Control de las Enfermedades para adaptarse a nuevas técnicas más eficaces de investigación científica, a fin de obtener una información e identificación más precisa de las amenazas para la salud, y así gestionar rápidamente los brotes de seguridad alimentaria. La Comisión ha creado una red de entidades financiadoras de la investigación (la Colaboración Global en Investigación para la Prevención de Enfermedades Infecciosas) para garantizar una respuesta de investigación coordinada en el plazo de 48 horas de cualquier brote importante.

<u>Acción 11</u>: 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-UE (Equipo de Respuesta a

Emergencias Informáticas 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.

Los recientes ciberataques mundiales que han utilizado programas maliciosos y *ransomware* (programas de secuestro de archivos a cambio de un rescate) para desactivar miles de sistemas informáticos han puesto de relieve una vez más la urgente necesidad de incrementar la resiliencia cibernética y las acciones de seguridad en el interior de la UE. Tal como se anunciaba en la revisión intermedia del mercado único digital, la Comisión y la Alta Representante están revisando la estrategia de ciberseguridad de la UE de 2013, en particular mediante la adopción de un paquete previsto para septiembre de 2017. El objetivo será proporcionar una respuesta intersectorial más eficaz a estas amenazas, aumentando la confianza en la economía y la sociedad digitales. Asimismo, revisará el mandato de la Agencia de Seguridad de las Redes y de la Información de la UE (ENISA) para definir su papel en el nuevo ecosistema de ciberseguridad. El Consejo Europeo[13] ha acogido con satisfacción la intención de la Comisión de revisar la estrategia de ciberseguridad.

La adopción de la Directiva de servicios de información en red[14] en julio de 2016 supuso un importante paso adelante en la mejora de la resiliencia en materia de ciberseguridad a escala europea. La Directiva establece las primeras normas de ciberseguridad a escala de la UE, mejora las capacidades de ciberseguridad y refuerza la cooperación entre los Estados miembros. También exige a las empresas de sectores vitales que adopten las medidas de seguridad oportunas y notifiquen los incidentes graves a las autoridades nacionales competentes. Entre estos sectores, cabe citar los de las infraestructuras de la energía, el transporte, el agua, la asistencia sanitaria, la banca y el mercado financiero. Los mercados en línea, los motores de búsqueda y los servicios de computación en la nube deberán adoptar medidas similares. Su aplicación coherente en los diferentes sectores, así como a través de las fronteras, se garantizará mediante el Grupo de Cooperación de Servicios de Información en Red (creado por la Comisión en 2016), encargado de evitar la fragmentación del mercado. En este contexto, se considera que la Directiva de servicios de información en red es el marco de referencia de todas las iniciativas sectoriales en el ámbito de la ciberseguridad. Además, la Directiva crea la red de equipos de respuesta a incidentes de seguridad informática (CSIRT), que reúne a todas las partes interesadas pertinentes. Paralelamente, la Comisión y el CERT-UE supervisarán activamente el panorama de las ciberamenazas e intercambiarán información con las autoridades nacionales a fin de garantizar que los sistemas de tecnología de la información de las instituciones de la UE son seguros y resilientes a los ciberataques. El incidente de *ransomware* WannaCry ofreció en mayo de 2017 a la Red la primera oportunidad de cooperar e intercambiar información operativa difundiendo asesoramiento. El Equipo de Respuesta a Emergencias Informáticas de la UE se mantuvo en estrecho contacto con el Centro Europeo de Ciberdelincuencia (EC3) de Europol, los equipos de respuesta a incidentes de seguridad informática (CSIRT) de los países damnificados, las unidades de ciberdelincuencia y los socios clave de la industria para reducir la amenaza y ayudar a las víctimas. El intercambio de informes de situación nacionales permitió un conocimiento

[13] Conclusiones del Consejo Europeo de 22 y 23 de junio de 2017.

[14] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, DO L 194 de 19.7.2016, p. 1.

común de la situación en toda la UE. Esta experiencia permitirá a la Red estar mejor preparada para los próximos incidentes (por ejemplo, *NonPetya*). También se pusieron de manifiesto varios retos, que se están abordando.

***Acción 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.**

En julio de 2016, la Comisión, en coordinación con los Estados miembros, firmó con la **industria** un asociación público-privada contractual sobre ciberseguridad, que invertirá hasta 450 millones EUR en el marco del programa de investigación e innovación de la UE Horizonte 2020, a fin de desarrollar y ensayar tecnologías destinadas a proteger mejor a los usuarios y a las infraestructuras contra las amenazas híbridas y cibernéticas. La Asociación publicó la primera Agenda estratégica de investigación paneuropea, centrada en reforzar la resiliencia de las infraestructuras críticas, así como de los ciudadanos, frente a los ciberataques. La Asociación ha aumentado la coordinación entre las partes interesadas, lo que ha dado lugar a mejoras en la eficiencia y la eficacia de la financiación de la ciberseguridad, en el marco del programa Horizonte 2020. La Asociación trabaja en paralelo sobre cuestiones relacionadas con la certificación de ciberseguridad de las tecnologías de la información y la comunicación, así como sobre la manera de abordar la grave escasez de profesionales de ciberseguridad cualificados. Habida cuenta de las importantes necesidades de investigación civil y la gran resiliencia necesaria en el sector de la defensa, el Grupo de Investigación Cibernética y Tecnología de la Agencia Europea de Defensa contribuye en los campos de investigación definidos por la Organización de Ciberseguridad Europea en su Agenda estratégica de investigación e innovación.

***Acción 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.**

En el sector de la **energía**, la Comisión está elaborando una estrategia sectorial en materia de ciberseguridad con la creación de la plataforma de expertos en materia de ciberseguridad para el sector de la energía, a fin de reforzar la aplicación de la Directiva de servicios de información en red. Un estudio de febrero de 2017 apoyó esta plataforma identificando las mejores técnicas disponibles para aumentar el nivel de ciberseguridad de los sistemas de medición inteligente. La Comisión también creó una plataforma basada en la web, el «Centro de la UE para el intercambio de información sobre incidentes y amenazas», que analiza y comparte información sobre amenazas e incidentes cibernéticos en el sector de la energía.

Mejora de la resiliencia del sector financiero ante las amenazas híbridas

***Acción 14*: La Comisión, en cooperación con ENISA[15], los Estados miembros, las autoridades y entidades financieras pertinentes a escala nacional, internacional y europea, fomentará y facilitará**

[15] Agencia de Seguridad de las Redes y de la Información de la Unión Europea.

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.

Reconociendo que la amenaza cibernética es uno de los principales riesgos para la estabilidad financiera, la Comisión revisó el marco reglamentario sobre servicios de pago en la Unión Europea, que actualmente se está implementando. La Directiva de Servicios de Pago revisada[16] introdujo nuevas disposiciones destinadas a reforzar la seguridad de los instrumentos de pago y la autenticación reforzada de cliente, con el objetivo de reducir el fraude, en especial en los pagos en línea. El nuevo marco legislativo será aplicable a partir de enero de 2018. En la actualidad, la Comisión, asistida por la Autoridad Bancaria Europea y en consulta con las partes interesadas, elabora las normas técnicas de regulación, que espera publicar en 2017, sobre la autenticación reforzada de cliente y sobre una comunicación común segura para hacer operativa la seguridad en las transacciones de pago. Por otra parte, en el ámbito internacional, la Comisión ha trabajado en estrecha colaboración con los respectivos socios del G-7 sobre los «principios fundamentales del G-7 sobre ciberseguridad en el sector financiero», aprobados en octubre de 2016 por los gobernadores de los Bancos Centrales y los Ministros de Hacienda del G-7. Estos principios están dirigidos a los entes del sector financiero (privados y públicos) y contribuyen a un planteamiento coordinado de la ciberseguridad en el sector financiero para abordar conjuntamente las amenazas cibernéticas, en particular ciberataques más numerosos y sofisticados.

Transporte

Acción 15: 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.

La aplicación del Plan de Acción de la Estrategia de Seguridad Marítima de la UE[17] ayudará a romper la mentalidad de compartimentos estancos en materia de intercambio de información y a que las autoridades civiles y militares compartan activos. Un enfoque de la administración en su conjunto se ha traducido en un aumento de la cooperación entre los diferentes agentes. Se prevé que a finales de 2017 se complete una agenda estratégica de investigación civil-militar conjunta entre la Comisión y el SEAE, con un taller final sobre protección de las infraestructuras marítimas críticas. Este trabajo podría en el futuro ampliarse a fin de abarcar las amenazas incipientes para las tuberías submarinas, la transferencia de energía, la fibra óptica y los cables de comunicaciones tradicionales frente a interferencias procedentes de fuera de las aguas nacionales.

Un reciente estudio[18] analizó la capacidad de evaluación del riesgo de las autoridades nacionales que realizan funciones de guardacostas. Identificó los principales obstáculos para la colaboración y recomendó soluciones prácticas a fin de aumentar la cooperación entre las autoridades marítimas a escala nacional y de la UE en este ámbito específico. La evaluación

[16] Directiva (UE) 2015/2366 del Parlamento Europeo y del Consejo, de 25 de noviembre de 2015, sobre servicios de pago en el mercado interior, DO L 337 de 23.12.2015, p. 35.

[17] https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf y en el 2.º informe sobre la aplicación del plan de acción de la ESMUE, presentado a los Estados miembros el 21 de junio de 2017.

[18] Estudio sobre evaluación de la capacidad de evaluación del riesgo de las autoridades de los Estados miembros que realizan funciones de guardacostas» («Evaluation of risk assessment capacity at the level of Member States' authorities performing coast guard functions»), 2017, https://ec.europa.eu/maritimeaffairs/documentation/studies

de los riesgos es esencial en la lucha contra las amenazas marítimas, y aún más decisiva para la evaluación y prevención de las amenazas híbridas, ya que exige consideraciones adicionales y más complejas. Los resultados de este estudio se presentarán en diferentes foros relacionados con la guardia costera, de modo que las recomendaciones propuestas puedan evaluarse y aplicarse para intensificar la cooperación en este ámbito, siendo los principales objetivos la preparación y la respuesta ante las amenazas híbridas.

Lucha contra la financiación del terrorismo

Acción 16: 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.

Los autores de amenazas híbridas y quienes les apoyan requieren fondos para ejecutar sus planes. Los esfuerzos de la UE contra la delincuencia y la financiación del terrorismo con arreglo a la Agenda Europea de Seguridad y el plan de acción de lucha contra la financiación del terrorismo también pueden contribuir a la lucha contra las amenazas híbridas. En diciembre de 2016, la Comisión presentó tres propuestas legislativas, en particular sobre sanciones penales del blanqueo de capitales y pagos ilícitos de dinero en efectivo, así como sobre el embargo preventivo y el decomiso de activos[19].
Todos los Estados miembros debían transponer antes del 26 de junio de 2017 la 4.ª Directiva antiblanqueo[20], y en julio de 2016 la Comisión presentó una propuesta legislativa específica para complementarla y reforzarla con medidas adicionales[21].

El 26 de junio de 2017, la Comisión publicó la Evaluación Supranacional de Riesgos prevista en la 4.ª Directiva antiblanqueo. También se presentó una propuesta de Reglamento para evitar la importación y el almacenamiento en la UE de bienes culturales ilegalmente exportados de países terceros[22]. A finales de este año, la Comisión informará sobre su evaluación continua de la necesidad de posibles medidas adicionales de seguimiento de la financiación del terrorismo en la UE. La Comisión también está revisando la legislación sobre lucha contra el fraude y falsificación de medios de pago distintos del efectivo[23].

El octavo informe **de situación relativo a una Unión de la Seguridad genuina y efectiva** proporciona más detalles sobre la situación de la aplicación del plan de acción de lucha contra la financiación del terrorismo.

Fomento de los valores comunes de la UE y de sociedades inclusivas, abiertas y resilientes

Reforzar la resiliencia frente a la radicalización y el extremismo violento

[19] Tercer informe de situación relativo a una Unión de la Seguridad genuina y efectiva, COM(2016) 831 final.
[20] Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) n.º 648/2012 del Parlamento Europeo y del Consejo, y se derogan la Directiva 2005/60/CE del Parlamento Europeo y del Consejo y la Directiva 2006/70/CE de la Comisión (Texto pertinente a efectos del EEE), DO L 141 de 5.6.2015, p. 73.
[21] Para más detalles, véase el tercer informe de situación relativo a una Unión de la Seguridad genuina y efectiva, COM(2016) 831 final, y el octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva, COM(2017) 354 final.
[22] COM(2017) de 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final 0.
[23] Octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva, COM(2017) 354 final.

La radicalización ideológica y religiosa y los conflictos étnicos y minoritarios pueden ser instigados por agentes externos apoyando a grupos específicos o alimentando conflictos entre grupos. Han surgido nuevos desafíos, como las amenazas de los terroristas solitarios, las nuevas vías de radicalización, incluso potencialmente en el contexto de la crisis migratoria, así como el ascenso de la extrema derecha (incluida la violencia contra los migrantes) y los riesgos de polarización. Aunque los trabajos sobre la radicalización se llevan a cabo en el seno de la Unión de la Seguridad, pueden ser también indirectamente relevantes desde el punto de vista de las amenazas híbridas, en la medida en que las personas vulnerables a la radicalización pueden ser manipulados por los autores de las amenazas híbridas.

Acción 17: ***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.***

Prevenir la radicalización

La Comisión sigue aplicando su respuesta pluridimensional a la radicalización, tal como figura en la Comunicación de junio de 2016 sobre el apoyo a la prevención de la radicalización que conduce al extremismo violento[24], con acciones clave como el fomento de la educación inclusiva y los valores comunes, la lucha contra la propaganda extremista en internet y contra la radicalización en los centros penitenciarios, la intensificación de la cooperación con terceros países y el refuerzo de la investigación para comprender mejor la naturaleza evolutiva de la radicalización e definir mejor las respuestas políticas. La Red para la Sensibilización frente a la Radicalización (RSR) ha estado a la vanguardia de los trabajos de la Comisión para apoyar a los Estados miembros en este ámbito, en colaboración con profesionales locales a nivel comunitario. Se ofrecen más detalles en el octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva[25].

Incitación al odio y radicalización en línea

En consonancia con la Agenda Europea de Seguridad[26], la Comisión ha tomado medidas para reducir la existencia de contenidos ilícitos en línea, especialmente a través de la Unidad de Notificación de Contenidos de Internet de la UE en Europol y el Foro de Internet de la UE[27]. También se han realizado avances significativos en el marco del Código de conducta para combatir el discurso ilegal del odio en línea[28]. Se ofrecen más detalles en el octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva[29]. Estas acciones se reforzarán, también a la luz de las conclusiones del Consejo Europeo[30], la Cumbre del G-7[31] y la Cumbre del G-20 de Hamburgo[32].

[24] http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

[25] COM(2017) 354 final.

[26] Para más detalles al respecto, véase el octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva, COM(2017) 354 final.

[27] Para más detalles al respecto, véase el octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva, COM(2017) 354 final.

[28] Código de conducta para combatir el discurso ilegal del odio en línea, de 31 de mayo de 2016, http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf

[29] Para más detalles al respecto, véase el octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva, COM(2017) 354 final.

[30] Conclusiones del Consejo de los días 22 y 23 de junio de 2017.

Las plataformas en línea desempeñan un papel clave para hacer frente a los contenidos potencialmente nocivos o ilegales. En el marco de la Estrategia para el Mercado Único Digital[33], tal como figura en su revisión intermedia, la Comisión garantizará una mejor coordinación de los diálogos sobre las plataformas, centrándose en los mecanismos y las soluciones técnicas para la eliminación del contenido ilegal. Cuando proceda, el objetivo debería ser apoyar estos mecanismos con orientaciones sobre aspectos como la notificación y retirada de los contenidos ilícitos. La Comisión proporcionará asimismo orientaciones sobre las normas de responsabilidad.

Reforzar la cooperación con los terceros países

Acción 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.***

La Unión ha hecho hincapié en el refuerzo de las capacidades y la resiliencia 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 y abriendo diálogos sobre seguridad y lucha contra el terrorismo con los países de la cuenca del Mediterráneo. En este sentido, se puso en marcha un proyecto piloto de estudio de riesgos, con la cooperación de la República de Moldavia. Su objetivo era ayudar a identificar las principales vulnerabilidades del país y garantizar que la ayuda de la UE se centre específicamente en estas zonas. Las conclusiones del estudio piloto pusieron de manifiesto que el estudio en sí se consideraba útil. Sobre la base de la experiencia adquirida, la Comisión y el SEAE harán recomendaciones para conceder prioridad a las acciones de mejora de la eficacia, las comunicaciones estratégicas, la protección de las infraestructuras críticas y la ciberseguridad.

De cara al futuro, otros países vecinos podrían beneficiarse del estudio, sobre la base de esta primera experiencia; si bien con adaptaciones para tener en cuenta las diferentes situaciones locales nacionales y las amenazas específicas, así como para evitar la duplicación con los diálogos en curso de seguridad y contra el terrorismo. De manera más general, el 7 de junio de 2017 la Comisión y la Alta Representante adoptaron una Comunicación conjunta sobre «Un planteamiento estratégico de la resiliencia en la acción exterior de la UE»[34]. El objetivo es ayudar a los países socios a ser más resilientes frente a los actuales retos mundiales. Reconoce la necesidad de pasar de la contención de crisis a un planteamiento de carácter más estructural y a largo plazo sobre las vulnerabilidades, haciendo énfasis en la anticipación, la prevención y la preparación.

Resiliencia cibernética para el desarrollo

[31] Cumbre del G-7 de Taormina, Italia, 26-27.5.2017.
[32] Cumbre del G-20 de Hamburgo, Alemania, 7-8.7.2017.
[33] Véase la citada Comunicación de la Comisión COM(2017) 228 final.
[34] Comunicación conjunta al Parlamento Europeo y al Consejo: Un planteamiento estratégico de la resiliencia en la acción exterior de la UE, JOIN (2017) 21 final.

La UE ayuda a terceros países a reforzar la resiliencia de sus redes de información. La creciente digitalización tiene una dimensión de seguridad intrínseca que plantea retos particulares a la resiliencia de los sistemas de redes de información a nivel mundial, ya que los ciberataques no conocen fronteras. La UE ayuda a terceros países a desarrollar su capacidad para prevenir y responder de forma adecuada a los ciberataques y fallos fortuitos. Tras un proyecto piloto sobre ciberseguridad en la Antigua República Yugoslava de Macedonia, Kosovo[35] y Moldavia finalizado en 2016, la Comisión pondrá en marcha un nuevo programa para mejorar la resiliencia cibernética de terceros países, principalmente de África y Asia, para el período 2017-2020, y también en Ucrania. Su objetivo es aumentar la seguridad y preparación de las redes e infraestructuras críticas de información de terceros países sobre la base de una perspectiva de la administración en su conjunto, garantizando al mismo tiempo el respeto de los derechos humanos y el Estado de Derecho.

Seguridad de la aviación

La aviación civil sigue siendo un objetivo importante y simbólico para los terroristas, pero también puede ser un objetivo incluido en una campaña híbrida. Si bien la UE ha desarrollado un sólido marco de seguridad aérea, los vuelos procedentes de terceros países pueden ser más vulnerables. En consonancia con la Resolución 2309 (2016) del Consejo de Seguridad de las Naciones Unidas, la Comisión está intensificando sus esfuerzos para desarrollar capacidades en terceros países. En enero de 2017, la Comisión puso en marcha una nueva evaluación integrada de riesgos para garantizar la priorización y coordinación de los esfuerzos de desarrollo de capacidades a escala de la UE y de los Estados miembros, así como con socios internacionales. En 2016, la Comisión puso en marcha un proyecto de cuatro años sobre la seguridad de la aviación civil en África y la Península Arábiga para combatir la amenaza del terrorismo contra la aviación civil. El proyecto se centra en la puesta en común de conocimientos entre los expertos de los Estados socios y de los Estados miembros de la Conferencia Europea de Aviación Civil, y actividades de mentoría, formación y *coaching*. Las actividades se ampliarán en 2017.

c. 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, 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. Se ha avanzado mucho en este ámbito en el último año y existe actualmente 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 realizará un seguimiento y se celebrarán ejercicios periódicos.

Acción 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***

[35] Esta designación se entiende sin perjuicio de las posiciones sobre su estatuto y está en consonancia con la RCSNU 1244 y con el dictamen de la Corte Internacional de Justicia sobre la declaración de independencia de Kosovo.

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.

La Comunicación conjunta recomendó crear mecanismos de respuesta rápida a las situaciones provocadas por las amenazas híbridas, coordinar mecanismos de respuesta en la UE[36] y sistemas de alerta temprana. A tal fin, los servicios de la Comisión y el SEAE publicaron el protocolo de actuación conjunta de la UE para contrarrestar las amenazas híbridas (*EU Playbook*)[37], que expone las modalidades de coordinación, análisis y fusión de la inteligencia que se tienen en cuenta en los procesos de elaboración de las políticas, los ejercicios y la formación, así como la cooperación con las organizaciones asociadas, en particular la OTAN, en caso de amenazas híbridas. Del mismo modo, la OTAN ha elaborado un cuaderno de estrategias para una mayor interacción entre la OTAN y la UE en la prevención y la lucha contra las amenazas híbridas en los ámbitos de la ciberdefensa, las comunicaciones estratégicas, el conocimiento de la situación y la gestión de crisis. El protocolo de actuación conjunta de la UE para contrarrestar las amenazas híbridas se pondrá a prueba a través de un ejercicio en otoño de 2017, como parte del ejercicio paralelo y coordinado de la Unión Europea, que incluye la interacción con la OTAN.

<u>Acción 20</u>: 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.

El artículo 42, apartado 7, del TUE hace referencia a la agresión armada en el territorio de un Estado miembro, mientras que el artículo 222 del TFUE (cláusula de solidaridad) hace referencia a un ataque terrorista o una catástrofe natural o de origen humano en el territorio de un Estado miembro. Es más probable que sea este último el que se utilice en caso de atentados híbridos, que son una combinación de acciones subversivas y delictivas. La invocación de la cláusula de solidaridad activa la coordinación a nivel del Consejo (Dispositivo Integrado de Respuesta Política a las Crisis, DIRPC) y la implicación de las instituciones, agencias y organismos pertinentes de la UE, así como los programas y mecanismos de ayuda de la UE. La Decisión 2014/415/UE del Consejo prevé las modalidades de aplicación por la Unión de la cláusula de solidaridad. Estas modalidades de aplicación siguen siendo válidas y no hay necesidad de revisar la Decisión del Consejo. Si un atentado híbrido incluye una agresión armada, también podría invocarse el artículo 42, apartado 7. En este caso, tanto los Estados miembros como la UE facilitarían ayuda y asistencia. La Comisión y la Alta Representante seguirán evaluando los medios más eficaces para hacer frente a estos ataques.

La adopción del citado protocolo de actuación conjunta de la UE apoya directamente esta evaluación y se practicará como parte del ejercicio paralelo y coordinado de la UE en octubre de 2017. El ejercicio pondrá a prueba los diversos mecanismos y la capacidad de la UE para interactuar con el objetivo de acelerar la toma de decisiones en caso de falta de claridad por la ambigüedad provocada por una amenaza híbrida.

[36] El Dispositivo Integrado de Respuesta Política de la UE a las Crisis del Consejo, el sistema ARGUS de la Comisión y el CRM del SEAE.
[37] El Documento de trabajo (2016) 227 de los servicios de la Comisión se adoptó el 7 de julio de 2016.

<u>Acción 21:</u> 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.

En respuesta al encargo para integrar las capacidades militares de apoyo a la PESC/PCSD y tras un seminario con expertos militares 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 para contrarrestar las amenazas híbridas en el seno de la PCSD finalizó en julio de 2017 y se llevará adelante a través del plan de aplicación de desarrollo del concepto.

d. COOPERACIÓN UE-OTAN

<u>Acción 22</u>: 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.

Sobre la base de la Declaración Conjunta firmada por los Presidentes del Consejo Europeo y de la Comisión Europea junto al Secretario General de la OTAN en Varsovia el 8 de julio de 2016, la UE y la OTAN elaboraron un conjunto común de 42 propuestas de aplicación, que fue ulteriormente refrendado en distintos procesos paralelos, el 6 de diciembre de 2016 por los Consejos de la UE y la OTAN[38]. En junio de 2017, la Alta Representante y Vicepresidenta y el Secretario General de la OTAN publicaron un informe sobre los progresos generales obtenidos en las 42 acciones de la Declaración conjunta. La lucha contra las amenazas híbridas es uno de los siete ámbitos de cooperación identificados en la Declaración Conjunta y abarca diez de las cuarenta y dos acciones. El informe pone de manifiesto que los esfuerzos conjuntos realizados durante el pasado año han producido resultados sustanciales. Ya se han mencionado muchas de las acciones específicas dirigidas a combatir las amenazas híbridas, incluido el Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas, un mejor conocimiento de la situación, la creación de la célula de fusión de la UE contra las amenazas híbridas y su interacción con la recién creada sección de análisis híbrido de la OTAN, así como la colaboración entre equipos de comunicaciones estratégicas. Por primera vez, el personal de la OTAN y el de la UE ejercerán conjuntamente su respuesta ante un escenario híbrido. Se espera que este ejercicio ponga a prueba la aplicación de más de un tercio de las propuestas comunes. La UE llevará a cabo su propio ejercicio paralelo y coordinado este año y se está preparando para asumir un papel de liderazgo en 2018.

En cuanto a la resiliencia, el personal de la UE y el la OTAN han participado en sesiones informativas, en particular sobre el Dispositivo Integrado de Respuesta Política a las Crisis de la UE. Los contactos periódicos entre el personal de la UE y el de la OTAN, en particular a través de talleres o de la participación de la OTAN en la Junta Directiva de la Agencia Europea de Defensa, han permitido intercambiar información sobre los requisitos básicos de resiliencia nacional de la OTAN. Nuevos intercambios entre la Comisión y la OTAN sobre el fortalecimiento de la resiliencia están previstos para el otoño. El próximo informe de progreso sobre la cooperación UE-OTAN propondrá posibilidades para ampliar la cooperación entre ambas organizaciones.

[38] http://www.consilium.europa.eu/es/press/press-releases/2016/12/06-eu-nato-joint-declaration/

3. CONCLUSIONES

La Comunicación conjunta presenta medidas destinadas a contribuir a la lucha contra las amenazas híbridas y reforzar la resiliencia a escala nacional y de la UE, así como de los socios. Aunque la Comisión y la Alta Representante están obteniendo resultados en todos los ámbitos, cooperando estrechamente con los Estados miembros y los socios, es vital que se mantenga este impulso ante la persistencia y continua evolución de las amenazas híbridas. Los Estados miembros tienen la responsabilidad primaria en materia de lucha contra las amenazas híbridas relacionadas con la seguridad nacional y el mantenimiento de la ley y el orden. La resiliencia nacional y los esfuerzos colectivos de protección contra las amenazas híbridas deben entenderse como elementos de refuerzo mutuo del mismo esfuerzo global. Por lo tanto, se anima a los Estados miembros a efectuar encuestas sobre las amenazas híbridas en el plazo más breve posible, lo que facilitará valiosa información sobre el grado de vulnerabilidad y preparación en toda Europa. Tomando como base los significativos progresos en la mejora de la sensibilización, debería maximizarse el potencial de la célula de fusión de la UE contra las amenazas híbridas. La Alta Representante invita a los Estados miembros a apoyar la labor de los grupos de trabajo StratCom para combatir de manera más eficaz el crecimiento de las amenazas híbridas. La UE apoyará plenamente el Centro Europeo para la Lucha contra las Amenazas Híbridas liderado por Finlandia.

La única fuerza de la UE reside en ayudar a los Estados miembros y a los países socios a aumentar su resiliencia, basándose en una amplia gama de instrumentos y programas existentes. Se han elaborado medidas para reforzar la resiliencia en ámbitos como el transporte, la energía, 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. La actuación de la UE para aumentar la resiliencia continuará a medida que la naturaleza de las amenazas híbridas evolucione. En particular, la UE elaborará indicadores para mejorar la protección y la resiliencia de las infraestructuras críticas ante las amenazas híbridas en los sectores pertinentes.

El Fondo Europeo de Defensa puede cofinanciar, junto con los Estados miembros, las prioridades en materia de capacidades para reforzar la resiliencia ante las amenazas híbridas. El próximo paquete de ciberseguridad y las medidas intersectoriales encaminadas a implementar la Directiva sobre seguridad de las redes y de la información ofrecerán nuevas plataformas para combatir las amenazas híbridas en toda la UE.

La Comisión y la Alta Representante piden a los Estados miembros y a las partes interesadas que, cuando sea necesario, lleguen a un acuerdo rápido y garanticen la rápida y eficaz ejecución de las numerosas medidas encaminadas a reforzar la resiliencia esbozadas en dicha Comunicación. La UE aumentará y profundizará su cooperación ya fructífera con la OTAN.

La Unión mantiene su compromiso de movilizar todos los instrumentos pertinentes de la UE para hacer frente a la complejidad de las amenazas híbridas. Apoyar los esfuerzos de los Estados miembros sigue siendo una prioridad para la Unión, actuando como un proveedor de seguridad más fuerte y reactivo, junto a sus socios principales.