COMISIÓN
EUROPEA

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

Bruselas, 13.6.2018
JOIN(2018) 16 final

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO, AL CONSEJO EUROPEO Y AL CONSEJO

Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas

1. INTRODUCCIÓN

Las actividades híbridas por parte de actores tanto estatales como no estatales siguen constituyendo una seria y crítica amenaza para la UE y sus Estados miembros. Cada vez son más habituales los esfuerzos para desestabilizar los países por la vía de la erosión de la confianza pública en las instituciones de la administración y de la puesta en entredicho de los valores fundamentales de las sociedades. Nuestras sociedades se enfrentan a un intrincado desafío planteado por quienes pretenden perjudicar a la UE y a sus Estados miembros con armas que van desde ciberataques que perturban la economía y los servicios públicos a acciones militares hostiles, pasando por campañas de desinformación con objetivos muy precisos.

Las campañas híbridas presentan múltiples facetas y combinan las medidas coercitivas con las subversivas, y las herramientas y las tácticas convencionales con las no convencionales (diplomáticas, militares, económicas y tecnológicas), todo con el fin de desestabilizar al adversario. Están concebidas para que resulte difícil detectarlas o atribuirles autoría, y pueden ser llevadas a cabo por actores tanto estatales como no estatales. El atentado perpetrado el pasado mes de marzo en Salisbury con un agente neurotóxico[1] puso además de manifiesto la versatilidad de las amenazas híbridas y la multitud de tácticas actualmente disponibles. En respuesta, el Consejo Europeo[2] destacó la necesidad de reforzar la capacidad de la UE y de sus Estados miembros para detectar, prevenir y responder a las amenazas híbridas en ámbitos como la ciberseguridad, la comunicación estratégica y la contrainteligencia. También hizo especial hincapié en la necesidad de resiliencia frente a las amenazas químicas, biológicas, radiológicas y nucleares (QBRN).

La amenaza que representan las armas no convencionales forma una categoría propia debido a la escala potencial de los daños que pueden provocar. Además de ser difícil de detectar y de atribuir, sus consecuencias son difíciles de subsanar. Las amenazas químicas, biológicas, radiológicas y nucleares, que van más allá de las amenazas híbridas e incluyen también las amenazas terroristas, son además una fuente general de preocupación para la comunidad internacional[3], en particular en lo que respecta al creciente riesgo de propagación tanto en el ámbito geográfico como a agentes no estatales.

El aumento de la resiliencia frente a estas amenazas y el desarrollo de las capacidades son responsabilidades que corresponden primordialmente a los Estados miembros. No obstante, las instituciones de la UE han adoptado ya una serie de medidas para contribuir a reforzar los esfuerzos nacionales. Debe mencionarse a este respecto el trabajo realizado en estrecha colaboración con otros actores internacionales, en particular la Organización del Tratado del Atlántico Norte (OTAN)[4], labor que podría profundizarse y transformarse en ayuda a los Estados miembros en ámbitos como la respuesta rápida[5].

---

1 Por lo que respecta al atentado de Salisbury, el Consejo Europeo de 22 de marzo de 2018 «manifestó su acuerdo con la valoración del gobierno británico de que es muy probable que la Federación de Rusia sea la responsable y con que no hay ninguna explicación alternativa verosímil.»

2 Conclusiones del Consejo Europeo de marzo de 2018.

3 En la que se incluye el Consejo de Seguridad de las Naciones Unidas, véase la Resolución S/RES/2325 (2016) de 14 de diciembre de 2016.

4 La lucha contra las amenazas híbridas es uno de los siete ámbitos de cooperación con la Organización del Tratado del Atlántico Norte que se destacan en la Declaración conjunta firmada en Varsovia en julio de 2016 por el presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la Organización del Tratado del Atlántico Norte.

5 El G-7, reunido en la cumbre de Charlevoix celebrada en junio de 2018, acordó asimismo desarrollar un Mecanismo de respuesta rápida del G-7 frente a las amenazas para las democracias: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

La presente Comunicación conjunta responde a la invitación del Consejo Europeo de progresar en esta labor. Forma parte de un paquete más amplio que incluye también el Decimoquinto Informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva[6], en el que se hace balance y se presentan las próximas etapas de la aplicación del Plan de acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos y nucleares, de octubre de 2017[7], así como el Segundo informe de situación[8] sobre la ejecución de las 22 acciones del marco común de lucha contra las amenazas híbridas — Una respuesta de la Unión Europea[9].

2. LA RESPUESTA DE LA UE

La Comisión y la alta representante han realizado incansables esfuerzos por desarrollar las capacidades de la UE y ayudar efectivamente a los Estados miembros a repeler las amenazas híbridas, químicas, biológicas, radiológicas y nucleares. Ya se han alcanzado resultados tangibles en ámbitos como las comunicaciones estratégicas, la conciencia situacional, el aumento de la preparación y la resiliencia y el refuerzo de las capacidades de respuesta a las crisis.

El Grupo de Trabajo East Stratcom, creado tras el Consejo Europeo de marzo de 2015, ha encabezado la labor de previsión, rastreo y lucha contra la desinformación originaria de fuentes extranjeras. Sus análisis de expertos y otros productos públicamente disponibles[10] han aumentado considerablemente el grado de concienciación en cuanto al impacto de la desinformación rusa. Durante los dos últimos años, ha destapado más de 4 000 casos de desinformación, muchos de los cuales apuntaban deliberadamente a Europa. El Grupo de Trabajo East Stratcom se ha centrado también en la mejora de la difusión de comunicaciones positivas, con un aumento de la cobertura en los países de la vecindad oriental. El éxito de este Grupo de Trabajo ha dado lugar a la creación de otros dos de diferente ámbito geográfico: el Grupo de Trabajo para los Balcanes Occidentales y el Grupo Operativo Sur para los países arábigoparlantes.

Se han dado grandes pasos en la construcción de las estructuras necesarias para mejorar la conciencia situacional y respaldar el proceso de adopción de decisiones. En 2016 se creó la Célula de fusión contra las amenazas híbridas dentro del Centro de Análisis de Inteligencia del Servicio Europeo de Acción Exterior. La Célula de fusión recibe y analiza tanto la información clasificada como la de dominio público, de diversa procedencia, sobre las amenazas híbridas. Se han realizado hasta la fecha más de 100 evaluaciones y sesiones informativas que se han puesto en conocimiento de la UE y los Estados miembros para alimentar el proceso de toma de decisiones de la UE. La Célula de fusión contra las amenazas híbridas mantiene una estrecha relación de trabajo con el Centro Europeo de Excelencia para la Lucha contra las Amenazas Híbridas, ubicado en Helsinki. Creado en abril de 2017 para fomentar el diálogo estratégico y realizar actividades de investigación y análisis sobre las amenazas híbridas, el Centro de Excelencia ha ampliado su composición a 16 países[11] y recibe un apoyo permanente de la UE.

---

6 Decimoquinto Informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva, COM(2018) 470.

7 COM(2017) 610 final.

8 Informe conjunto sobre la aplicación del marco común relativo a la lucha contra las amenazas híbridas (julio de 2017-julio de 2018), JOIN(2018) 14.

9 JOIN(2016) 18 final.

10 Véase www.euvsdisinfo.eu

11 De sus 16 miembros actuales, 14 son Estados miembros de la UE: Alemania, Chequia, Dinamarca, España, Estonia, Finlandia, Francia, Italia, Letonia, Lituania, los Países Bajos, Polonia, el Reino Unido y Suecia. La iniciativa de su creación procede del marco común relativo a la lucha contra las amenazas

También se han dado importantes pasos en el incremento de la preparación y la resiliencia, en particular contra las amenazas químicas, biológicas, radiológicas y nucleares. En los últimos seis meses se han producido grandes avances en la detección de lagunas de preparación frente a los incidentes de seguridad químicos, biológicos, radiológicos y nucleares, especialmente en lo que afecta a la capacidad de detección que puede contribuir a prevenir ataques químicos, biológicos, radiológicos y nucleares. A iniciativa de la Comisión, un consorcio de expertos nacionales llevó a cabo un análisis de las carencias del equipo de detección en distintos tipos de situaciones químicas, biológicas, radiológicas y nucleares. El informe sobre el análisis de estas carencias se ha facilitado a los Estados miembros para que puedan adoptar decisiones adecuadamente fundamentadas sobre las estrategias de detección y adoptar las medidas operativas necesarias para subsanar dichas carencias.

Este trabajo ha ido acompañado de ejercicios de medición de los avances. El ejercicio paralelo y coordinado de 2017 (PACE17) con la Organización del Tratado del Atlántico Norte ha permitido realizar una comprobación detallada de las capacidades de respuesta de la UE frente a las crisis híbridas a gran escala. Sin precedentes en cuanto a su alcance, este ejercicio no solo puso a prueba el protocolo de actuación de la UE frente a la amenaza híbrida (también conocido como «UE Playbook»), sino además los distintos mecanismos de respuesta de la UE y su capacidad para interactuar eficientemente, así como la interacción de la respuesta de la UE a las amenazas híbridas con la acción de la Organización del Tratado del Atlántico Norte. Se encuentra en fase de planificación un ejercicio para 2018 cuya doble ambición es consolidar el carácter anual de esta práctica y ayudar a los Estados miembros a reforzar sus capacidades de respuesta ante las crisis híbridas.

Estas acciones concretas ilustran la medida en que los marcos estratégicos implantados por la UE están dando frutos: en efecto, en los dos últimos años se ha establecido una serie de estructuras para ayudar a orientar y centrar la labor de la UE.

El documento de abril de 2016 titulado *Marco común para la lucha contra las amenazas híbridas — Una respuesta de la Unión Europea*[12] aboga por un enfoque integral de la Administración en su conjunto y propone 22 ámbitos de acción para contribuir a contrarrestar las **amenazas híbridas** y desarrollar la resiliencia tanto de la UE y sus Estados miembros como de los socios internacionales. La mayor parte de las acciones que se definen en el marco común se centran en la mejora de la conciencia situacional y el desarrollo de resiliencia, ampliando la capacidad de respuesta. Abarcan aspectos que van desde el refuerzo de la capacidad de análisis de inteligencia de la UE a la lucha contra la radicalización y el extremismo violento, pasando por la mayor protección de la infraestructura crítica y la ciberseguridad. Las ciberamenazas y los ciberataques ocupan también un lugar destacado en el marco común. El Segundo informe de situación sobre la aplicación del marco común, adoptado en paralelo a la presente Comunicación conjunta, pone de manifiesto la realización de avances tangibles en la ejecución de esas acciones y confirma la intensificación y la profundización de los esfuerzos de la UE en la lucha contra las amenazas híbridas[13].

En materia de **ciberseguridad**, el 9 de mayo de 2018 fue una fecha decisiva, pues dio término al plazo para que todos los Estados miembros de la UE incorporasen a sus ordenamientos jurídicos el primer conjunto de normas jurídicamente vinculantes a escala de la UE en materia de ciberseguridad: la Directiva sobre la seguridad de las redes y

---

híbridas. El Centro también ha recibido el apoyo activo de UE y de la Organización del Tratado del Atlántico Norte, en el marco de su cooperación.

[13] Primer informe de aplicación (julio de 2017): JOIN(2017) 30 final.

sistemas de información. Es un importante componente del planteamiento más general establecido en la Comunicación conjunta de septiembre de 2017 titulada: «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE[14]», que incluye medidas concretas de amplio alcance para imprimir un fuerte impulso a las estructuras y las capacidades de ciberseguridad de la UE. El documento se centró en la creación, por parte de la UE, de resiliencia frente a los ciberataques y en el incremento de la capacidad de ciberseguridad de la UE; en el desarrollo de una respuesta eficaz de Derecho penal, y en el refuerzo de la estabilidad global mediante la cooperación internacional. El documento iba acompañado de una propuesta de Reglamento de ciberseguridad destinado a reforzar el apoyo a escala de la UE[15] y ha sido respaldado con una serie de propuestas que aún deben llegar a la fase de aplicación (véase más adelante).

La **desinformación** es perniciosa para nuestras democracias, pues merma la capacidad de los ciudadanos para decidir con conocimiento de causa y participar en el proceso democrático. Internet ha aumentado de forma ingente el volumen y la variedad de noticias a las que pueden acceder los ciudadanos. No obstante, las nuevas tecnologías pueden utilizarse para propagar desinformación a una velocidad y una escala sin precedentes y apuntando a objetivos concretos para sembrar la desconfianza y crear tensiones sociales. La Comunicación de la Comisión titulada «La lucha contra la desinformación en línea: un enfoque europeo»*[16]* ofrece un planteamiento europeo para dar respuesta al problema de la desinformación y hace un llamamiento a las distintas partes interesadas, especialmente a las plataformas en línea, para que actúen en una amplia gama de aspectos que incluyen el aumento de la transparencia; la fiabilidad y la responsabilidad de las plataformas en línea; el aumento de la seguridad y la resiliencia de los procesos electorales; el fomento de la educación y de la alfabetización mediática; el apoyo al periodismo de calidad, y la lucha contra la desinformación a través de una comunicación estratégica. Las primeras medidas concretas incluyen un código de buenas prácticas sobre la desinformación, de cuya elaboración se encargará un Foro multilateral sobre desinformación, y una red de verificadores de datos que se creará antes del verano. El 29 de mayo de 2018 tuvo lugar la primera reunión del Foro multilateral sobre desinformación en la que se acordaron los pasos necesarios para la adopción del código en julio de 2018. Antes de que termine 2018, la Comisión evaluará los avances realizados hacia la solución del problema y determinará si se necesita alguna intervención adicional. Las actividades previstas serán complementarias y coherentes con las del Grupo de Trabajo East Stratcom.

Por lo que se refiere a los riesgos **químicos, biológicos, radiológicos y nucleares** (QBRN), el Plan de acción de la Comisión de octubre de 2017[17] proponía 23 acciones y medidas prácticas destinadas a mejorar la protección de los ciudadanos y las infraestructuras contra estas amenazas, en particular a través de una cooperación más estrecha entre la UE y sus Estados miembros, así como con la Organización del Tratado del Atlántico Norte. Como parte de las medidas de la Unión de la Seguridad para aumentar la protección y la resiliencia frente al terrorismo, el Plan seguía un enfoque preventivo basado en el razonamiento de que la probabilidad de los riesgos químicos, biológicos, radiológicos y nucleares era baja pero su impacto era elevado y duradero en caso de ataque. Desde entonces, el atentado de Salisbury y la creciente preocupación en cuanto al interés de los terroristas por utilizar materiales químicos, biológicos, radiológicos y nucleares y su capacidad para hacerlo, tanto dentro como fuera de la UE[18],

---

14 JOIN(2017) 450 final.
15 COM (2017) 477, véase más adelante.
16 COM(2018) 236 final.
17 COM(2017) 610 final.
18 Europol, Informe sobre la situación y las tendencias del terrorismo en la UE (TE-SAT) 2017, p. 16, disponible en: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Véanse también las declaraciones del Director General de la OPAQ: www.globaltimes.cn/content/1044644.shtml

han puesto de manifiesto que la amenaza planteada por las sustancias químicas, biológicas, radiológicas y nucleares es muy real. Esta apreciación acentúa aún más la urgencia de dar plena aplicación al Plan de acción, basado en un enfoque que contempla todos los riesgos y centrado en cuatro objetivos: reducir la accesibilidad de los materiales químicos, biológicos, radiológicos y nucleares; fortalecer la preparación y la respuesta frente a incidentes de seguridad químicos, biológicos, radiológicos y nucleares; reforzar los vínculos internos y externos de la seguridad química, biológica, radiológica y nuclear con los principales socios regionales e internacionales de la UE; y ampliar el conocimiento de los riesgos químicos, biológicos, radiológicos y nucleares. El informe más reciente sobre la evolución hacia la Unión de la Seguridad, adoptado en paralelo a la presente Comunicación conjunta, da cumplida cuenta de los avances tangibles en la ejecución del Plan de acción.

Por último, para potenciar la eficacia de los esfuerzos de lucha contra las amenazas híbridas y reforzar el mensaje de unidad entre los Estados miembros de la UE y los aliados de la Organización del Tratado del Atlántico Norte (OTAN), la cooperación contra las amenazas híbridas se ha definido como un aspecto fundamental de la **cooperación entre la UE y la OTAN**, como subraya la Declaración conjunta de Varsovia de julio de 2016[19]. Casi una tercera parte de las propuestas comunes de cooperación actuales se centran en las amenazas híbridas[20]. Este año, los ejercicios y el «Protocolo de actuación de la UE»[21] anteriormente descritos han proseguido en un régimen de intensificación de la cooperación.

3. INTENSIFICAR LA RESPUESTA ANTE UNAS AMENAZAS CAMBIANTES

3.1. Conciencia situacional — Mejora de la capacidad de detección de amenazas híbridas

Los esfuerzos por repeler las amenazas híbridas y responder a ellas deben sustentarse en una capacidad de detección temprana de actividades y fuentes híbridas malintencionadas, tanto interiores como exteriores, y en la comprensión de los posibles vínculos entre hechos aparentemente inconexos. Con tal fin, es esencial hacer uso de todos los flujos de datos disponibles, incluida la inteligencia procedente de fuentes de dominio público.

La Célula de fusión contra las amenazas híbridas creada dentro del Servicio Europeo de Acción Exterior como punto central de análisis de las amenazas híbridas representa un activo importante, pero ha de obtener los conocimientos especializados necesarios para hacer frente al espectro completo de amenazas híbridas, en particular en lo que respecta a los riesgos químicos, biológicos, radiológicos y nucleares, así como a la contrainteligencia. La ampliación de los conocimientos especializados reforzaría el apoyo a toda respuesta frente a crisis futuras de la UE al ofrecer productos de inteligencia civil y militar más completos en esos ámbitos específicos. Tal iniciativa podría ser respaldada por una actuación de los Estados miembros dirigida a aumentar la contribución, en términos de inteligencia, de sus servicios nacionales a la Célula de fusión contra las amenazas híbridas de la UE y a potenciar la capacidad de la red existente de puntos de contacto nacionales con la Célula para suministrar y procesar información respecto de la cual el factor el tiempo es crucial. Otro paso sería que los Estados miembros estudiasen la forma de aumentar las contribuciones de inteligencia de sus servicios nacionales al Centro de

[19] La declaración firmada por el presidente Juncker, el presidente Tusk y el general Stoltenberg, secretario general de la OTAN, constituye la base vigente para la cooperación entre la UE y la OTAN.
[20] 15283/16 y 14802/17.
[21] SWD(2016) 227 final.

Análisis de Inteligencia de la UE (INTCEN) con el fin de permitir un análisis más exhaustivo de las posibles amenazas.

Etapas futuras

- La alta representante ampliará la Célula de fusión de la UE contra las amenazas híbridas mediante la adición de componentes analíticos especializados en materia química, biológica, radiológica y nuclear, así como en contrainteligencia y ciberanálisis. Se invita a los Estados miembros a que acrecienten sus contribuciones de inteligencia a la Célula de fusión contra las amenazas híbridas con vistas al análisis de las amenazas híbridas existentes y emergentes.

- La Comisión, en coordinación con la alta representante, ultimará el trabajo sobre los indicadores de vulnerabilidad que permitirán a los Estados miembros evaluar mejor el potencial de amenazas híbridas en distintos sectores. Esta labor sustentará asimismo el análisis de las tendencias de las amenazas híbridas efectuado por la UE.

3.2. **Refuerzo de la acción contra las amenazas químicas, biológicas, radiológicas y nucleares**

El Plan de acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares, de octubre de 2017, establece el marco de acción para reforzar la preparación, la resistencia y la coordinación a escala de la UE. Ese marco incluye toda una gama de medidas de ayuda a los Estados miembros mediante la puesta en común de conocimientos especializados, la creación de capacidad conjunta, el intercambio de información y mejores prácticas y la intensificación de la cooperación operativa. Los Estados miembros y la Comisión deben cooperar, con carácter urgente, para dar plena aplicación al Plan de acción. Además, partiendo de los progresos ya realizados en el análisis de las carencias de las capacidades de detección y en el intercambio de las mejores prácticas dentro del recién creado Grupo consultivo en materia química, biológica, radiológica y nuclear, la Unión debería ahora adoptar nuevas medidas para hacer frente a las amenazas en pleno desarrollo y evolución, especialmente las químicas. Siguiendo el modelo de las medidas de restricción del acceso a los precursores de explosivos[22], la UE ha de adoptar rápidas medidas operativas para controlar mejor el acceso a materiales químicos de alto riesgo y optimizar la capacidad de detectar ese tipo de materiales en la fase más temprana posible. Los Estados miembros deberían considerar también la posibilidad de hacer nuevos ejercicios de análisis e inventariado de carencias al nivel de la UE, por ejemplo en materia de resiliencia frente a la amenaza química, biológica, radiológica y nuclear y de activos y enfoques de resiliencia y descontaminación. Prepararse para las consecuencias de un atentado químico, biológico, radiológico y nuclear y gestionarlas exige el refuerzo de la cooperación y la coordinación entre los Estados miembros, incluidas las autoridades de protección civil. El Mecanismo de Protección Civil de la Unión puede desempeñar un papel fundamental en este proceso con el objetivo de reforzar la capacidad colectiva europea de preparación y respuesta.

[22] Como parte del trabajo llevado a cabo en la Unión de la Seguridad para acotar el espacio dentro del que operan los terroristas y los delincuentes, la Comisión ha adoptado rigurosas medidas para reducir el acceso a los precursores de explosivos que pueden utilizarse con fines ilícitos para la fabricación de explosivos caseros. En octubre de 2017, la Comisión presentó una Recomendación en la que se incluían medidas inmediatas para prevenir el uso indebido de precursores de explosivos con arreglo a las normas vigentes (C(2017) 6950 final). Partiendo de esa base, la Comisión adoptó en abril de 2018 una propuesta para revisar y reforzar el Reglamento n.º 98/2013, sobre la comercialización y la utilización de precursores de explosivos (COM(2018) 209 final).

La cooperación internacional es otro elemento importante de esta labor, y la UE puede ensanchar sus conexiones con los Centros de excelencia química, biológica, radiológica y nuclear y buscar sinergias con la Organización del Tratado del Atlántico Norte y con los programas de prevención, preparación y respuesta ante catástrofes naturales para el sur y el este[23].

Etapas futuras

- La UE debe estudiar medidas para defender el respeto de las normas y principios internacionales contra el uso de armas químicas, entre las que puede contarse un régimen específico de sanciones de la UE aplicable a las armas químicas.

- Con el fin de avanzar en la aplicación del Plan de acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares, la Comisión trabajará junto con los Estados miembros para completar las medidas siguientes antes del final de 2018:
  - elaborar una lista de sustancias químicas que plantean una amenaza concreta, que servirá de base a actividades operativas destinadas a reducir el acceso a dichas sustancias;
  - entablar un diálogo con los agentes privados de la cadena de suministro para iniciar una colaboración destinada a hacer frente a las nuevas amenazas que plantean las sustancias químicas que pueden utilizarse como precursores;
  - acelerar la revisión de los escenarios de amenazas y el análisis de los métodos de detección existentes para mejorar la detección de amenazas químicas, con el objetivo de desarrollar orientaciones operativas que permitan a los Estados miembros incrementar su capacidad de detección.

- Los Estados miembros deben compilar inventarios de sus existencias de productos médicos de respuesta sanitaria, productos de laboratorio, tratamientos y otras capacidades. La Comisión trabajará con los Estados miembros para analizar regularmente la disponibilidad de esas existencias en toda la UE con el fin de aumentar el acceso a las mismas y su rápido despliegue en caso de atentados.

3.3. **Comunicación estratégica — Difusión coherente de información**

Un importante reto relacionado con las amenazas híbridas es la labor de concienciación y educación de la población a fin de que pueda distinguir la información de la desinformación. Basándose en la experiencia del Grupo de Trabajo East Stratcom, la Célula de fusión de la UE contra las amenazas híbridas y el Centro Europeo de Excelencia para la lucha contra las amenazas híbridas, así como en otras iniciativas de la Comisión[24], la Comisión y la alta representante seguirán desarrollando y profesionalizando las capacidades de comunicación estratégica de la UE, garantizando una interacción y una

[23] En la vecindad oriental y meridional se organizan actividades de formación y ejercicios de protección civil en el marco de los programas regionales de prevención, preparación y respuesta ante catástrofes naturales o de origen humano.

[24] Las Representaciones de la Comisión, por ejemplo, también desarrollan una actividad de verificación de datos y desmitificación. Algunas de ellas han desarrollado herramientas adaptadas al entorno local, como *Les Décodeurs de l'Europe* en Francia, UE Vero Falso en Italia, un concurso público de tiras cómicas para desmontar mitos sobre la UE en Austria, otra iniciativa similar en Rumanía y la publicación de la Representación en el Reino Unido titulada *Euromyths A-Z*. Hay otros proyectos de esas características en fase de preparación.

coherencia sistemáticas entre las estructuras existentes. Esta práctica se ampliará a otras instituciones de la UE y a los Estados miembros, en particular a través de la plataforma en línea protegida sobre desinformación.

La mejora de la coordinación y la cooperación en el ámbito de la comunicación estratégica en todas las instituciones de la UE, con los Estados miembros y con los socios y organizaciones internacionales será un aspecto fundamental que requerirá preparación y práctica antes de reaccionar a las crisis en tiempo real.

Los períodos electorales han resultado un objetivo particularmente estratégico y vulnerable a los ataques cibernéticos y a la elusión en línea de las salvaguardias y normas convencionales («fuera de línea») como los periodos de reflexión, las normas de financiación transparentes y la igualdad de trato de los candidatos. Se han producido, entre otras intrusiones, atentados contra las infraestructuras electorales y los sistemas de campaña electoral a través de las TI, así como campañas de desinformación masiva en línea con fines políticos y ciberataques por parte de terceros países con el objetivo de desacreditar y deslegitimar los procesos electorales democráticos. Se están siguiendo diversas líneas de trabajo al nivel de la UE para sensibilizar a los Estados miembros en cuanto a la preparación y respuesta frente a estas nuevas amenazas. En el Consejo, las autoridades de ciberseguridad de los Estados miembros[25] emitirán directrices voluntarias y determinarán las mejores prácticas comunes en materia de ciberseguridad de las tecnologías aplicables a las elecciones a lo largo de todo el proceso electoral. Estas tecnologías incluyen los sistemas de información y las soluciones de TIC utilizadas para el registro de los votantes y los candidatos, para la emisión y el recuento de los votos y para el anuncio de los resultados, además de los sistemas auxiliares que inciden directamente en la legitimidad de los resultados de las elecciones.

Es preciso asimismo garantizar la rapidez, fiabilidad y consistencia de la información facilitada a la población en caso de ataques híbridos. Todo incidente químico, biológico, radiológico y nuclear o evento que cause un impacto similar suscita protestas públicas y exigencias de respuestas rápidas por parte de los ciudadanos. Los mensajes estratégicos desempeñan un papel crucial, por ejemplo entre las organizaciones internacionales que pudieran estar adoptando sus planes de respuesta por separado.

[25] Bajo los auspicios del Grupo de cooperación establecido en virtud de la Directiva sobre la seguridad de las redes y sistemas de información.

Etapas futuras

- El Servicio Europeo de Acción Exterior y la Comisión trabajarán juntos, en el marco de sus competencias respectivas, para establecer una cooperación más estructurada en materia de comunicaciones estratégicas con el fin de hacer frente a la desinformación procedente del interior y el exterior de la UE y de imposibilitar la producción de desinformación hostil y las interferencias híbridas por parte de Gobiernos extranjeros.

- En el otoño, la Comisión organizará con los Estados miembros y las partes interesadas pertinentes una serie de actos de alto nivel entre los que se incluirá el Coloquio sobre derechos fundamentales que, en esta edición, se dedicará a la democracia y al fomento de buenas prácticas y de directrices sobre la forma de prevenir, mitigar y dar respuesta a las amenazas de desinformación ante procesos electorales.

- La alta representante y la Comisión estudiarán las maneras de respaldar más eficazmente, en términos de instrumentos y de recursos, el trabajo llevado a cabo por los tres Grupos de Trabajo StratCom con el fin de garantizar que los esfuerzos de la UE tengan la dimensión suficiente para hacer frente a la complejidad de campañas de desinformación llevadas a cabo por actores hostiles.

3.4. **Aumento de la resiliencia y de la disuasión en el sector de la ciberseguridad**

La ciberseguridad es un factor crítico tanto para nuestra prosperidad como para nuestra seguridad. A medida que nuestra vida cotidiana y nuestras economías se van haciendo cada vez más dependientes de las tecnologías digitales, aumenta nuestro grado de exposición.

Actualmente, la efectividad de la ciberseguridad en la UE se ve obstaculizada por la insuficiencia de la inversión y la coordinación. La UE trata ahora de resolver este problema mediante el desarrollo de capacidades gracias a medidas de apoyo, al aumento de la coordinación y la creación de nuevas estructuras que posibiliten el avance de la tecnología de ciberseguridad y su despliegue[26]. La Directiva sobre la seguridad de las redes y sistemas de información[27] establece un nivel mínimo de seguridad de las redes y sistemas de información en toda la Unión. Su plena aplicación por todos los Estados miembros es esencial para reforzar la ciberresiliencia: se trata de un primer paso esencial. El Reglamento general de protección de datos introduce la obligación de notificar los casos de violación de la seguridad de los datos personales a la autoridad de control competente. Entre las demás medidas clave cabe citar el refuerzo y la modernización de la Agencia de Ciberseguridad de la Unión Europea y un marco de certificación de la UE para los productos y servicios de TIC que inspire confianza a los consumidores[28]. Está también en marcha toda una labor de apoyo a la red de centros de competencia de los Estados miembros para estimular el desarrollo y el despliegue de soluciones de ciberseguridad y complementar los esfuerzos de creación de capacidad en este ámbito a escala nacional y de la UE. Esta actividad se basará en el trabajo del Programa Europa Digital presentado

[26] En diciembre de 2017, en el contexto del desarrollo de la innovación en las regiones de Europa, se puso en marcha una nueva acción piloto interregional en torno a la que se agruparon las regiones de la UE para intensificar su actividad relacionada con la ciberseguridad.

[27] 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.

[28] COM(2017) 477.

por la Comisión el 6 de junio[29], que otorga una nueva prioridad a la inversión de la UE en materia de ciberseguridad.

Al mismo tiempo, la Recomendación de la Comisión sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala[30] determinó la forma en que debía organizarse la cooperación entre los Estados miembros y los diferentes actores de la UE al responder a un ciberataque a gran escala y de carácter transfronterizo. En ella se destacaba el papel esencial de la conciencia situacional para una coordinación eficaz a los niveles técnico, operativo y estratégico/político. El Grupo de cooperación establecido en virtud de la Directiva sobre la seguridad de las redes y sistemas de información también está trabajando para mejorar el intercambio y la puesta en común de información entre las partes interesadas, desarrollando una taxonomía común para la descripción de incidentes. Esta metodología será objeto de ensayo en los próximos ejercicios. La Célula de fusión contra las amenazas híbridas facilita un análisis estratégico de las ciberamenazas actuales y emergentes realizado a partir de las contribuciones de los servicios de inteligencia de los Estados miembros.

El marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia») ha supuesto un importante paso hacia adelante desde el punto de vista operativo, dado que fija las medidas que, en virtud de la Política Exterior y de Seguridad Común, pueden emplearse para endurecer la respuesta de la UE a las actividades que atentan contra sus intereses políticos, económicos y de seguridad. Cuanto más frecuente y pleno sea el recurso a este marco por parte de los Estados miembros, mejor servirá como mecanismo eficaz de disuasión. En abril, el Consejo de Asuntos Exteriores adoptó unas conclusiones sobre las actividades cibernéticas hostiles que condenan firmemente el uso malintencionado de las tecnologías de la información y la comunicación, como por ejemplo para los ataques WannaCry y NotPetya, que han causado considerables daños y pérdidas económicas en la UE y fuera de ella.

La UE y sus Estados miembros deben mejorar su capacidad de atribución de la autoría de los ciberataques, sobre todo mediante un mayor intercambio de inteligencia. La identificación de los autores podría disuadir a los agresores potenciales y aumentar las probabilidades de que los responsables rindan cuentas de sus actos. La mejora de los mecanismos de disuasión es un objetivo clave de la estrategia de la Comisión para aumentar la ciberseguridad. Las recientes propuestas de la Comisión dirigidas a mejorar la obtención transfronteriza de pruebas electrónicas para procedimientos penales aumentarían considerablemente la capacidad de las fuerzas y cuerpos de seguridad para investigar y enjuiciar los casos de ciberdelincuencia.

Una ciberresiliencia fuerte requiere un enfoque colectivo y de amplio alcance. Con ese fin, se necesitan estructuras más sólidas y eficaces de fomento de la ciberseguridad y de respuesta a los ciberataques en los Estados miembros, también dentro de las instituciones, agencias, delegaciones, misiones y operaciones de la UE: la inexistencia de una red segura de comunicaciones entre las instituciones europeas es una deficiencia importante. Debe aumentarse la sensibilización en materia de ciberseguridad en las instituciones de la UE y entre el personal de estas profundizando la cultura de seguridad e intensificando la formación correspondiente.

[29] Propuesta de Reglamento por el que se establece el programa «Europa Digital» para el período 2021-2027, COM(2018) 434.

[30] C(2017) 6100.

Etapas futuras

- El Parlamento Europeo y el Consejo han de acelerar la actividad que permitirá concluir antes del final de año, mediante un acuerdo, las negociaciones sobre las propuestas en materia de ciberseguridad, y aprobar rápidamente la propuesta de acto legislativo sobre la recopilación de pruebas electrónicas.

- La Comisión y la alta representante colaborarán estrechamente con los Estados miembros para avanzar en los aspectos cibernéticos de la gestión de crisis y los mecanismos de respuesta a escala de la UE. Se invita a los Estados miembros a que prosigan su labor de atribución de los ciberataques y continúen haciendo un uso práctico del conjunto de instrumentos de ciberdiplomacia para reforzar la respuesta política frente a los ciberataques.

- En respuesta a la necesidad de reforzar nuestras capacidades de ciberdefensa, se está creando una plataforma de formación y educación especializadas para contribuir a la coordinación de la oferta de formación en ciberdefensa impartida por los Estados miembros. Se buscarán sinergias con medidas similares de la Organización del Tratado del Atlántico Norte.

3.5. **Desarrollo de resiliencia frente a las actividades de inteligencia hostiles**

La lucha contra la actividad de inteligencia hostil requiere, en primer lugar, una coordinación más estrecha y eficaz entre los Estados miembros, de conformidad con la legislación pertinente de la UE y las normas y dispositivos nacionales. Sin embargo, nos hallamos también ante el imperativo de incrementar las capacidades de las instituciones de la UE para hacer frente a la creciente amenaza de actividades de esa índole específicamente dirigidas a las instituciones y para crear una cultura de concienciación en materia de seguridad apoyada en una mejora de la formación y la seguridad física. Las instituciones podrían también trabajar con los Estados miembros para crear un sistema de acreditación de la UE más consistente. Ese sistema se basaría en un mecanismo de notificación proactiva que permitiría a los Estados miembros y a las instituciones estar mucho más concienciados en cuanto a los agentes potencialmente hostiles, especialmente cuando algunos de ellos hayan sido identificados ya por los Estados miembros.

La coordinación entre los Estados miembros y entre estos y otras organizaciones internacionales pertinentes, en particular la Organización del Tratado del Atlántico Norte, contribuiría a impulsar la contrainteligencia contra la actividad hostil en la UE. Un ejemplo de ámbito en el que sería beneficiosa una mayor coordinación entre los Estados miembros es el del control de las inversiones, a partir de un Reglamento[31] propuesto en septiembre de 2017 por la Comisión para el control de las inversiones extranjeras directas de los Estados miembros por motivos de seguridad o de orden público. El aumento de la coordinación entre Estados miembros sería también importante para el escrutinio de las transacciones financieras, dado que los servicios de inteligencia hostiles recurren cada vez más a intrincados mecanismos financieros para financiar sus medidas activas contra la UE.

[31] Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece un marco para el control de las inversiones extranjeras directas en la Unión Europea, COM(2017) 487.

Etapas futuras

- El Servicio Europeo de Acción Exterior y la Comisión pondrán en marcha medidas prácticas perfeccionadas para sustentar y desarrollar la capacidad de la UE para interactuar con los Estados miembros con el fin de combatir la actividad de inteligencia hostil específicamente dirigida a las instituciones.

- La Célula de fusión contra las amenazas híbridas se complementará con conocimientos especializados en contrainteligencia y ofrecerá análisis detallados y sesiones informativas sobre la naturaleza de la actividad de inteligencia hostil probable contra las personas y las instituciones.

- El Parlamento Europeo y el Consejo habrán de acelerar su actividad para concluir las negociaciones sobre la propuesta relativa al control de las inversiones antes de que termine el año.

4. CONCLUSIÓN

Las amenazas híbridas y las amenazas químicas, biológicas, radiológicas y nucleares están desde hace algún tiempo en el punto de mira de la UE. El incidente sufrido en el mes de marzo en el Reino Unido puso de manifiesto la amplitud del espectro de la guerra híbrida y la especial necesidad de resiliencia frente a las amenazas químicas, biológicas, radiológicas y nucleares.

La Comisión y la alta representante han adoptado y propuesto una serie de iniciativas dirigidas a hacer frente a los desafíos que plantean las amenazas híbridas. Además, la Comisión está acelerando la aplicación del Plan de acción de 2017 para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares.

La presente Comunicación conjunta tiene por objeto informar al Consejo Europeo de la actividad en curso y determinar los ámbitos en los que es preciso redoblar los esfuerzos para seguir intensificando y reforzando la contribución esencial de la UE a la lucha contra estas amenazas. Corresponde ahora a los Estados miembros, a la Comisión y a la alta representante dar un rápido seguimiento a estas propuestas.