Consejo de la Unión Europea

Bruselas, 27 de mayo de 2022
(OR. en)

9563/22

JAI 761	**DROIPEN 69**
COSI 149	**COPEN 210**
ENFOPOL 298	**FREMP 110**
ENFOCUSTOM 89	**JAIEX 61**
IXIM 145	**CFSP/PESC 705**
CT 99	**COPS 238**
CRIMORG 81	**HYBRID 49**
FRONT 218	**DISINFO 47**
ASIM 47	**TELECOM 248**
VISA 87	**DIGIT 108**
CYBER 191	**COMPET 408**
DATAPROTECT 175	**RECH 307**
CATS 30	

NOTA DE TRANSMISIÓN

De:	Por la secretaria general de la Comisión Europea, D.ª Martine DEPREZ, directora
Fecha de recepción:	25 de mayo de 2022
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2022) 252 final
Asunto:	COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO relativa al cuarto informe de situación sobre la aplicación de la Estrategia de la UE para una Unión de la Seguridad

Adjunto se remite a las Delegaciones el documento – COM(2022) 252 final.

Adj.: COM(2022) 252 final

COMISIÓN
EUROPEA

Bruselas, 25.5.2022
COM(2022) 252 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

relativa al cuarto informe de situación sobre la aplicación de la Estrategia de la UE para una Unión de la Seguridad

I. INTRODUCCIÓN

La guerra de agresión de Rusia contra Ucrania domina la agenda actual de la UE en materia de seguridad. La guerra no solo amenaza a Ucrania, sino que busca dañar la estabilidad y la seguridad mundiales. Dentro de la UE, conlleva una serie de riesgos para la seguridad de los ciudadanos. Existen nuevas incertidumbres acerca de los suministros de energía y otras materias primas, y las infraestructuras críticas pueden ser objeto de ciberataques. La seguridad y la protección interiores de la UE se ven comprometidas por posibles ataques o accidentes causados por agentes químicos, biológicos o radiológicos en la zona de guerra. La delincuencia organizada puede aprovechar rápidamente las vulnerabilidades de millones de personas que han huido de la guerra, a través de la trata de mujeres y niños, que se encuentran especialmente en riesgo.

Ante estas nuevas y posibles amenazas, la UE se ha mantenido firme y unida. Aunque de momento las repercusiones de la guerra se han limitado al territorio de Ucrania, la UE ha intensificado *la vigilancia y la coordinación* con un mayor seguimiento del panorama de amenazas, y ha trabajado para reforzar la resiliencia a fin de garantizar la *preparación*.

En la Declaración de Versalles de los días 10 y 11 de marzo de 2022[1], los líderes europeos hicieron hincapié en la necesidad de prepararnos para los retos de rápida aparición, en particular «protegiéndonos frente a la intensificación de la guerra híbrida, reforzando nuestra ciberresiliencia, protegiendo nuestras infraestructuras —en particular nuestras infraestructuras críticas— y luchando contra la desinformación».

El marco de la Unión de la Seguridad es fundamental para garantizar la seguridad en toda la UE. Las cuatro prioridades estratégicas expuestas en la Estrategia de la Unión de la Seguridad[2] siguen siendo directamente pertinentes para esta tarea en el contexto geopolítico actual: i) un entorno de seguridad con garantías de futuro; ii) hacer frente a las amenazas cambiantes; iii) proteger a los europeos frente al terrorismo y la delincuencia organizada; y iv) un ecosistema europeo de seguridad sólido. La guerra ha puesto de relieve la necesidad de que la UE y sus Estados miembros hagan pleno uso de los instrumentos legislativos y políticos ya disponibles en el marco de la Estrategia de la Unión de la Seguridad, que sustentan el apoyo coordinado de la UE a los Estados miembros en cuestiones que van desde la delincuencia organizada y el terrorismo, hasta la ciberseguridad y las amenazas híbridas.

Las agencias europeas en el ámbito de la justicia y los asuntos de interior también han redoblado sus esfuerzos como respuesta a la guerra en Ucrania, desempeñando un papel clave en la evaluación de las amenazas y en el apoyo de las respuestas operativas[3]. Otro factor importante es el refuerzo continuo de la práctica operativa y la gobernanza del espacio Schengen.

Este cuarto informe de situación de la Unión de la Seguridad se centra en los acontecimientos de los últimos meses desde la guerra de agresión de Rusia contra Ucrania. Ofrece una visión general de las medidas adoptadas en todos los aspectos de la Unión de la Seguridad y tiene en cuenta las necesidades de preparación debido a las posibles amenazas a la seguridad

---

1 https://www.consilium.europa.eu/media/54800/20220311-versailles-declaration-es.pdf/.

2 COM/2020/605.

3 *Joint Statement from EU Justice and Home Affairs Agencies on Ukraine* [«Declaración conjunta de las Agencias de Justicia y Asuntos de Interior sobre Ucrania», documento en inglés]. Agencia de Asilo de la Unión Europea (europa.eu).

derivadas de la guerra en Ucrania. Los avances en otros expedientes de la Unión de la Seguridad figuran en el anexo.

II. CIBERSEGURIDAD E INFRAESTRUCTURAS CRÍTICAS

Desde el estallido de la guerra, agentes privados y operaciones delictivas han publicado el hecho de que están realizando actividades informáticas en apoyo de una u otra parte. El «hacktivismo»[4] plantea una amenaza debido al riesgo de efectos indirectos en la UE contra los servicios críticos, el riesgo de ataques procedentes de redes oficiales u otros efectos indirectos imprevistos. Si bien hasta ahora la guerra se ha llevado a cabo, en gran medida, a través de medios convencionales con escasos efectos indirectos, el riesgo de escalada en este ámbito es real.

Por tanto, la UE ha intensificado su coordinación y preparación. Las amenazas derivadas de la guerra subrayan la necesidad de desarrollar una cultura de intercambio de información y conocimientos especializados entre la UE y los Estados miembros, y entre todas las comunidades de ciberseguridad. Esto incluye el desarrollo de un conocimiento de la situación integrado, compartido por las instituciones, los órganos y organismos de la UE y por los Estados miembros, en particular respecto de las infraestructuras críticas de las que depende el buen funcionamiento del mercado interior.

Atribución de ciberataques contra Ucrania

Los ciberataques a la propia Ucrania empezaron antes de la agresión rusa, en los primeros días de la guerra[5], y su objetivo era poner en peligro las cuentas de usuario del personal militar ucraniano y perturbar los servicios esenciales, en especial el control fronterizo y las telecomunicaciones.

El 14 de enero de 2022, el Alto Representante realizó una declaración[6] en nombre de la Unión Europea en la que condenaba los ciberataques contra Ucrania y volvía a confirmar el apoyo inequívoco de la UE a Ucrania.

El 10 de mayo, la Unión Europea y sus Estados miembros, junto con socios internacionales, condenaron firmemente[7] la actividad informática malintencionada contra Ucrania del 24 de febrero, que tuvo por objetivo la red satelital KA-SAT, propiedad de Viasat, y atribuyeron directamente el ataque a la Federación de Rusia. Este ciberataque tuvo unas repercusiones

[4] Un ejemplo reciente de «hacktivismo» es el uso de programas «protestware» para propagar programas maliciosos a los protocolos de internet rusos a través de un conocido paquete de código abierto, lo que puede dar lugar a riesgos en la cadena de suministro y a la pérdida de confianza en la comunidad de código abierto. La Comisión ha dejado claro que (aunque sean bienintencionados) los ciberataques a Rusia son ilegales.

[5] Informe especial de Microsoft: *An overview of Russia's cyberattack activity in Ukraine* [«Descripción general de la actividad de los ciberataques de Rusia en Ucrania», documento en inglés]; *The hybrid war in Ukraine - Microsoft On the Issues* [«La guerra híbrida en Ucrania – Microsoft sobre los problemas», documento en inglés].

[6] https://www.consilium.europa.eu/es/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/.

[7] Operaciones cibernéticas de Rusia contra Ucrania: Declaración del Alto Representante en nombre de la Unión Europea – Consejo de la UE (europa.eu).

significativas, pues provocó interrupciones y perturbaciones indiscriminadas que afectaron a diversas autoridades públicas, empresas y usuarios de Ucrania, así como a varios Estados miembros de la UE.

Vigilancia y coordinación

Desde la guerra de agresión de Rusia contra Ucrania, ha aumentado el seguimiento de la situación de la ciberseguridad en los Estados miembros y en las instituciones de la UE. La Agencia de la Unión Europea para la Ciberseguridad (ENISA), el Centro Europeo de Ciberdelincuencia de Europol, el equipo de respuesta a emergencias informáticas de las instituciones, órganos y organismos de la UE (CERT-UE) y el Centro de Inteligencia y de Situación de la UE (INTCEN), han contribuido al conocimiento compartido de la situación, en particular mediante la realización de un seguimiento periódico de la actividad informática sospechosa, especialmente en sectores específicos como los de la energía, el transporte y la aviación, y han proporcionado evaluaciones para orientar la acción preventiva.

También se ha intensificado la coordinación y el intercambio de información con redes de ciberseguridad, como la red de organizaciones de enlace para la gestión de cibercrisis (CyCLONe), que está compuesta por los organismos nacionales de ciberseguridad, la Comisión y ENISA. Para reflejar este enfoque de forma interna en las instituciones de la UE, un mecanismo de coordinación, el Grupo Operativo sobre crisis cibernéticas, permite que se comparta información entre todos los servicios, órganos y organismos pertinentes, en especial ENISA, el Centro Europeo de Ciberdelincuencia de EUROPOL y CERT-UE. Se necesitan esfuerzos constantes para garantizar canales de comunicación entre los niveles político, operativo y técnico, así como para mejorar la cooperación con la red de equipos de respuesta a incidentes de seguridad informática (CSIRT).

Europol también activó el Protocolo de respuesta policial ante emergencias de la UE que permite un seguimiento reforzado de las ciberamenazas y el intercambio de información entre una amplia variedad de partes interesadas para obtener una visión integral de la ciberinteligencia.

Más allá de las ciberamenazas, hay una vigilancia intensificada por parte de los Estados miembros, del Servicio Europeo de Acción Exterior (SEAE) y de los servicios de la Comisión sobre la exposición de las infraestructuras críticas a amenazas físicas no cibernéticas. Las infraestructuras críticas y las entidades que las explotan pueden verse expuestas a riesgos físicos, como el sabotaje por parte de agentes estatales o por agentes patrocinados por el Estado como parte de posibles represalias contra la UE.

Preparación

La preparación en el ámbito de la ciberseguridad y la seguridad de las infraestructuras críticas es más importante que nunca, dada la creciente exposición de Europa a una acumulación de amenazas como consecuencia de la guerra. Los esfuerzos por intensificar la preparación han incluido una serie de acciones directas, en particular algunas que ya estaban previstas antes de la agresión de Rusia contra Ucrania. Entre ellas se incluyen ejercicios, orientaciones, medidas legislativas, aumentar la resiliencia en sectores críticos, y colaborar con los socios.

La Presidencia francesa del Consejo de la Unión Europea, junto con el Servicio Europeo de Acción Exterior (SEAE) y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) organizaron un ejercicio basado en hipótesis a principios de 2022, denominado Ejercicio de enlace de cibercrisis sobre solidaridad (EU CyCLES), con el objetivo de sensibilizar a nivel político y reforzar la cooperación entre los niveles operativo y político en caso de un ciberataque a gran escala.

ENISA y CERT-UE publicaron en febrero unas **directrices** sobre cómo aumentar la resiliencia y la preparación en la UE[8]. Estas iniciativas recomiendan a todas las organizaciones de los sectores público y privado de la UE adoptar un conjunto mínimo de mejores prácticas en materia de ciberseguridad a fin de mejorar considerablemente la cultura de la ciberseguridad. En marzo, CERT-UE publicó unas directrices técnicas de seguimiento, con el apoyo de ENISA[9], así como unas directrices de seguridad para reforzar la configuración de la aplicación informática Signal[10] con una serie de recomendaciones prácticas a las organizaciones para mejorar sus posiciones en materia de ciberseguridad.

Iniciativas legislativas

La situación actual pone de relieve la urgencia de **aplicar la legislación existente** y acelerar la **adopción de las iniciativas pendientes**.

La Comisión está apoyando a los Estados miembros a la hora de implementar la **Directiva SRI**[11], que exige que los Estados miembros estén debidamente equipados, por ejemplo con un equipo de respuesta a incidentes de seguridad informática (CSIRT) y mediante la definición de autoridades competentes. Proporciona la base para la cooperación efectiva entre los Estados miembros. El acuerdo político alcanzado por los colegisladores sobre la **Directiva SRI 2**[12] es un nuevo avance a la hora de proporcionar un marco sólido de preparación de la UE.

SRI 2: reforzar aún más la preparación

- La nueva Directiva relativa a las redes y sistemas de información abordará las deficiencias de la anterior Directiva SRI para adaptarla a las necesidades actuales y prepararla para el futuro. Dispone las normas mínimas para un marco regulador y establece los mecanismos para una cooperación eficaz entre las autoridades pertinentes de cada Estado miembro.
- Amplía el ámbito de aplicación de las normas con nuevos sectores cruciales para la economía y la sociedad (por ejemplo, los sectores farmacéuticos y de los productos sanitarios, o el de la producción de alimentos). Todas las entidades medianas y grandes

[8] *Boosting your Organisation's Cyber Resilience* [«Impulsar la ciberresiliencia de su organización», documento en inglés], publicación conjunta, 14.2.2022.

[9] *Security Guidance 2022-01 - Cybersecurity mitigation measures against critical threats* [«Orientaciones sobre seguridad 2022-01: Medidas de mitigación de ciberseguridad ante amenazas críticas», documento en inglés].

[10] *CERT-EU Security Guidance 22-002 - Hardening Signal* [«CERT-UE Orientaciones de seguridad 22-002: Endurecer Signal», documento en inglés].

[11] 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.

[12] COM(2020) 823.

que operan en los sectores o que prestan servicios cubiertos por la directiva entrarán dentro de su ámbito de aplicación. También están cubiertas las entidades de la administración pública de los gobiernos centrales (con excepción del poder judicial, los parlamentos y los bancos centrales) y a nivel regional. Además, los Estados miembros pueden decidir que se aplique a dichas entidades a nivel local.

- La Directiva SRI 2 determinará la base de referencia para las medidas de gestión de los riesgos de ciberseguridad y establece formalmente la red europea de organizaciones de enlace para la gestión de cibercrisis (CyCLONe UE), que respaldará la gestión coordinada de los incidentes de ciberseguridad a gran escala.
- La propuesta también introduce disposiciones más precisas sobre el proceso de notificación de incidentes, el contenido de los informes y los plazos, y dispone medidas correctivas y sanciones para garantizar su ejecución.
- Los Estados miembros dispondrán de veintiún meses a partir de la entrada en vigor de la Directiva para incorporar las disposiciones a su legislación nacional.

Los avances de la Directiva SRI 2 deben ir seguidos lo antes posible de la conclusión de las negociaciones sobre la propuesta de **Directiva relativa a la resiliencia de las entidades críticas**[13] («Directiva REC») que, una vez adoptada e implementada, debe aumentar la resiliencia de las entidades críticas ante una serie de amenazas, en especial los ataques terroristas, las amenazas internas o el sabotaje. También es fundamental que el nivel de ambición de la Directiva relativa a la resiliencia de las entidades críticas coincida con el de la propuesta de la Comisión y que se mantenga la coherencia con el compromiso político alcanzado sobre la Directiva SRI 2. Todas estas medidas impulsarán la resiliencia y la preparación con la puesta en marcha de un sistema más coherente y sólido, en especial a través de planes nacionales de respuesta a incidentes y crisis. Estas también formaron parte de la Recomendación de la Comisión del año pasado[14] por la que se creó la **unidad informática conjunta**, que establece cómo deben cooperar a nivel operativo los distintos agentes del ecosistema de ciberseguridad (diplomáticos, policiales, civiles y, cuando corresponda, de defensa). El panorama actual de amenazas pone de relieve el valor de dicha cooperación eficaz entre los principales agentes.

La Comisión sigue supervisando la aplicación del conjunto de instrumentos sobre ciberseguridad de la **5G**[15]. En este contexto, el 11 de mayo el Grupo de Cooperación SRI adoptó un informe sobre la seguridad de las Open RAN (redes de acceso por radio abiertas[16]. También sigue trabajando conjuntamente con los Estados miembros para que el Centro Europeo de Competencia en Ciberseguridad sea plenamente operativo.

El 22 de marzo de 2022, la Comisión propuso **nuevas normas para establecer medidas comunes en materia de ciberseguridad y seguridad de la información en todas las instituciones, órganos y organismos de la UE (IOUE).** Estas normas reforzarán la resiliencia de la administración de la UE y su capacidad de responder a ciberamenazas e

[13] COM(2020) 829.

[14] *Recommendation on building a Joint Cyber Unit | Shaping Europe's digital future* [Recomendación sobre el desarrollo de una unidad informática conjunta – Configurar el futuro digital de Europa», documento en inglés] (europa.eu).

[15] https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[16] Grupo de Cooperación SRI, Informe sobre la ciberseguridad de las Open RAN, de 11 de mayo de 2022.

incidentes. Al situar estas actividades en un marco común, la cooperación interinstitucional se verá reforzada y se minimizará la exposición al riesgo. La propuesta de **Reglamento sobre ciberseguridad para las IOUE**[17] reforzará el mandato del CERT-UE y dará lugar a la creación de un nuevo Consejo Interinstitucional de Ciberseguridad, potenciará las capacidades en materia de ciberseguridad y fomentará las evaluaciones periódicas de madurez y una mejor ciberhigiene. La propuesta de **Reglamento sobre la seguridad de la información**[18] creará un conjunto mínimo de reglas y normas sobre seguridad de la información para todas las IOUE con el fin de garantizar una protección reforzada y coherente contra la evolución de las amenazas a su información. La Comisión pide al Parlamento Europeo y al Consejo que adopten rápidamente estas medidas.

La Comisión ya ha finalizado su consulta pública sobre medidas para impulsar la **ciberresiliencia** de los productos digitales, con la preparación de una propuesta que se publicará este otoño[19]. De este modo se abordarán las vulnerabilidades de los productos digitales y servicios auxiliares que, si bien crean oportunidades para las economías y sociedades de la UE, también dan lugar a nuevos desafíos ya que, cuanto más conectado esté todo más fácil será que un incidente de ciberseguridad afecte a todo un sistema y, por tanto, interrumpa las actividades económicas y sociales.

El 9 de marzo de 2022, los ministros de la UE responsables de las telecomunicaciones adoptaron por unanimidad en Nevers el llamamiento para reforzar las capacidades de la UE en materia de ciberseguridad, que incluía «la ejecución de un nuevo fondo de respuesta de emergencia para la ciberseguridad que deberá ponerlo en marcha la Comisión»[20]. La Comisión está reflexionando sobre el mejor uso de los fondos existentes para apoyar las acciones preventivas y de respuesta.

Sectores críticos

La seguridad del abastecimiento **energético** de la UE es crucial para el bienestar de los ciudadanos y para el buen funcionamiento de nuestras economías, y la situación actual ha puesto de manifiesto la necesidad de unas normas claras sobre ciberseguridad en este sector. La Comisión está trabajando en un código de red en materia de ciberseguridad para los flujos transfronterizos de electricidad, tal y como exige el Reglamento sobre la electricidad[21], para establecer normas sobre las evaluaciones de riesgos, los requisitos mínimos comunes, la planificación, la supervisión, la información y la gestión de crisis. Desde la guerra de agresión de Rusia contra Ucrania, los objetivos previstos para el código de red en materia de ciberseguridad son incluso más pertinentes. La Comisión también ha puesto en marcha una cooperación estructural entre ENISA, la Red Europea de Gestores de Redes de Transporte de Electricidad (REGRT de Electricidad)[22], la Red Europea de Gestores de Redes de Transporte

[17] COM(2022) 122.
[18] COM(2022) 119.
[19] Ley de ciberresiliencia: nuevas normas de ciberseguridad para productos digitales y servicios auxiliares (europa.eu).
[20] 08/03/2022 - *Déclaration conjointe des ministres de l'Union européenne chargés du numérique et des communications électroniques adressée au secteur numérique - Presse - Ministère des Finances* (economie.gouv.fr).
[21] Reglamento (UE) 2019/943 del Parlamento Europeo y del Consejo, de 5 de junio de 2019, relativo al mercado interior de la electricidad, DO L 158, 14.6.2019, p. 54. La Agencia está revisando actualmente una propuesta de Cooperación de los Reguladores de la Energía.
[22] Red Europea de Gestores de Redes de Transporte de Electricidad.

de Gas (REGRT de Gas)[23] y la Comunidad de la Energía en el seguimiento periódico de la situación de la ciberseguridad en el sector de la energía.

La UE ha trabajado para proteger la seguridad de los socios sin crear nuevos riesgos para sí misma. La sincronización de emergencia de las redes eléctricas de Ucrania y Moldavia con la red de Europa continental tuvo lugar en marzo de 2022 tras la adopción de medidas de mitigación del riesgo, especialmente en términos de ciberseguridad.

La guerra y las sanciones también han creado muchos desafíos para el **transporte** de la UE, desde riesgos de seguridad para la aviación civil de la UE y conductores de camiones atrapados en zonas de conflictos, hasta la destrucción de las infraestructuras de transporte ucranianas, con la interrupción de las cadenas de suministro y la amenaza para la seguridad alimentaria mundial. La Agencia de la Unión Europea para la Seguridad Aérea, en estrecha colaboración con la Comisión y la Organización Europea para la Seguridad de la Navegación Aérea (Eurocontrol), ha aconsejado a los operadores desde el inicio de la guerra que no operen dentro del espacio aéreo de Ucrania y que eviten utilizar el espacio aéreo dentro de las cien millas náuticas de la frontera de Ucrania con Bielorrusia y Rusia.

La Comisión también ha estado trabajando para reforzar la preparación y la resiliencia del sector del transporte de la UE. En concreto, un nuevo plan de contingencia para el transporte[24], adoptado el 23 de mayo, extrae lecciones tanto de la pandemia de COVID-19 como de la agresión militar de Rusia contra Ucrania. Propone un conjunto de diez acciones para orientar a la UE y a sus Estados miembros a la hora de introducir medidas de respuesta a las crisis, en particular la garantía de una conectividad mínima, el desarrollo de una resiliencia ante amenazas cibernéticas e híbridas y la mejora de la cooperación con los socios internacionales en materia de preparación y respuesta ante las crisis. También destaca la importancia de pruebas periódicas de resiliencia para diferentes contextos de crisis, reuniendo a las agencias de la UE u otros agentes pertinentes y basándose en procesos existentes.

Según lo previsto en el marco de **seguridad sanitaria de la UE,** el intercambio de información basado en el sistema de alerta precoz y respuesta, en especial el apoyo para evacuaciones médicas desde Ucrania, debe protegerse de los ciberataques, por lo que la seguridad del sistema se está reforzando.

Cooperación con los socios

La UE sigue trabajando con sus socios internacionales para impedir, desalentar, disuadir y responder a comportamientos malintencionados en el ciberespacio. La guerra de agresión de Rusia contra Ucrania ha hecho que la cooperación en este ámbito sea más importante que nunca. A este respecto, el SEAE ha estado trabajando para intercambiar conocimientos de la situación y coordinar la respuesta a las actividades informáticas malintencionadas contra Ucrania, así como en el apoyo a Ucrania y otros países de la región, trabajando con los socios, incluidos los Estados Unidos y la OTAN, para garantizar la complementariedad y evitar solapamientos.

También se intensificó la cooperación con Estados Unidos en el contexto del Consejo UE-EE. UU. de Comercio y Tecnología. La declaración conjunta[25] tras la reunión ministerial

[23] Red Europea de Gestores de Redes de Transporte de Gas.
[24] COM(2022) 21.
[25] https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_22_3108.

celebrada en mayo en París hizo hincapié en el papel central del Consejo UE-EE. UU. de Comercio y Tecnología en la asociación trasatlántica renovada que sirva para coordinar medidas conjuntas de la UE y Estados Unidos ante la agresión de Rusia contra Ucrania. Ambas partes convinieron que una estrecha cooperación para potenciar la resiliencia de las cadenas de suministro es más importante que nunca. Además, se creó un grupo de trabajo específico sobre financiación pública para unas infraestructuras digitales seguras y resilientes en terceros países, a fin de preparar el camino para la financiación pública conjunta UE-EE. UU. de proyectos digitales en terceros países, sobre la base de una serie de principios generales comunes.

La Brújula Estratégica adoptada en marzo de 2022 (véase la sección VII) reforzará aún más el conjunto de instrumentos de la UE en materia de ciberdiplomacia y desarrollará la política de la UE sobre ciberdefensa para estar mejor preparados y responder mejor a los ciberataques, como parte de una estrategia más amplia para mejorar la capacidad de la UE de actuar en situaciones de crisis y defender sus intereses.

Apoyo en materia de ciberseguridad a Ucrania y a los países vecinos

La UE ya estaba apoyando la ciberresiliencia de Ucrania antes de la guerra. Ya en junio de 2021, la UE y Ucrania mantuvieron un primer ciberdiálogo, y la UE prestó apoyo para la ciberseguridad y la transformación digital resiliente a través del programa EU4Digital de Ucrania por valor de 25 millones EUR. Otro programa de hermanamiento por valor de 1,5 millones EUR está diseñado para ayudar a las instituciones de ciberseguridad de Ucrania a ajustarse a las normas de la UE.

Tras el estallido de la guerra, la UE está fomentando la cooperación entre los ciberexpertos de la UE y ucranianos, y coordinando el suministro de asistencia técnica, de equipos, de software y de servicios pertinentes, a fin de reforzar la ciberresiliencia y la ciberdefensa de Ucrania.

Además, la UE está trabajando para evaluar el posible apoyo a medio plazo a Moldavia, Georgia y los Balcanes Occidentales. Los días 3 y 4 de marzo de 2022, se llevó a cabo una misión de evaluación conjunta a Moldavia sobre las necesidades de ciberseguridad que ha dado lugar a la adopción de una medida específica de respuesta a la crisis para aumentar rápidamente la ciberseguridad en el país. Se está preparando un apoyo similar de respuesta rápida para una serie de países en los Balcanes Occidentales que se consideran especialmente expuestos al riesgo debido a su alineación con las sanciones de la UE. También se está evaluando una posible asistencia adicional a Moldavia a través del Fondo Europeo de Apoyo a la Paz.

III. DELINCUENCIA ORGANIZADA Y TERRORISMO

La guerra de agresión de Rusia contra Ucrania ha obligado a millones de personas a abandonar sus hogares, lo que ha aumentado considerablemente los movimientos en todas las fronteras exteriores de la UE. A 18 de mayo, casi seis millones de personas habían llegado a la UE desde Ucrania y Moldavia y, hasta la fecha, 2,8 millones de personas se han inscrito para protección temporal en la UE. La UE ha procurado ofrecer la acogida más rápida y flexible a quienes huyen de la guerra, sin poner en peligro la seguridad en la frontera exterior de la UE. La UE ha adoptado medidas sin precedentes para ofrecer a los que huyen de la guerra protección temporal y se ha comprometido a tratar a todos los recién llegados sin

distinción. Al mismo tiempo, no se pueden ignorar los posibles riesgos derivados de tantas personas desplazándose y la UE, con el firme apoyo de las agencias pertinentes de la Unión, sigue atenta a la reciente evolución de la delincuencia organizada y el terrorismo.

Un espacio Schengen sólido en un momento de crecientes amenazas

Garantizar un alto nivel de seguridad en el espacio **Schengen** y dentro de la UE nunca ha sido tan importante como en el clima de las amenazas acentuadas derivadas de la guerra justo más allá de la frontera exterior de la UE.

Cumpliendo la ambiciosa agenda del espacio Schengen establecida en la estrategia de junio de 2021, la Comisión adoptó en mayo el primer informe sobre el estado de Schengen[26]. El ciclo anual de Schengen ofrece un nuevo modelo de gobernanza para el espacio Schengen, con un control sanitario periódico sobre el estado del espacio Schengen. Esto contribuirá a garantizar la rápida detección de las deficiencias y unos procedimientos de seguimiento eficientes, a fin de que el espacio Schengen sea más fuerte y resiliente.

Este primer informe reconoce la necesidad de redoblar los esfuerzos para aplicar iniciativas clave a escala de la Unión, en particular controles sistemáticos de todos los viajeros en las fronteras exteriores, haciendo pleno uso de los mandatos de Frontex y Europol, así como de los instrumentos de cooperación policial transfronteriza propuestos y disponibles.

En particular, la nueva arquitectura de los sistemas de información de la UE para la gestión de las fronteras, la migración y la seguridad —y su interoperabilidad— es la piedra angular de los esfuerzos para mejorar la seguridad interior y la gestión de las fronteras. Será fundamental la aplicación efectiva de todos los elementos del marco de interoperabilidad en consonancia con los plazos acordados.

Vigilancia y coordinación

Es clave una cooperación policial más estrecha entre todos los Estados miembros y con terceros países para garantizar la sensibilización sobre las amenazas delictivas y terroristas emergentes, así como la adopción de medidas sobre las redes delictivas y las personas que intentan sacar provecho de la guerra contra Ucrania. Los Estados miembros y los socios operativos están compartiendo activamente la información disponible y los datos relativos a las actividades delictivas pertinentes con Europol, que hace controles cruzados y analiza la información, y la convierte en notificaciones de datos operativos procesables, como las notificaciones de alerta rápida y las evaluaciones de amenazas, que se comparten con los socios.

Delincuencia organizada

La delincuencia organizada ya está encontrando formas de sacar provecho de la situación actual. El análisis de la información policial confidencial inicial detectó patrones delictivos

[26] COM(2022) 301.

en una serie de ámbitos, en particular la trata de seres humanos, las declaraciones falsas de bienes importados y exportados, el fraude en línea, la ciberdelincuencia y el tráfico de armas de fuego. También hay indicios de ciberdelincuentes haciéndose pasar por recaudadores de fondos para Ucrania, con el fin de robar dinero y criptomonedas[27]. Las organizaciones delictivas de Ucrania pueden intentar reubicarse debido a la situación actual y continuar con sus actividades en la UE.

La Comisión y la Presidencia francesa del Consejo trabajaron juntas, así como con las agencias JAI de la UE, en especial Europol, para movilizar la plataforma multidisciplinar europea contra las amenazas delictivas (**EMPACT**) para evaluar, anticipar, impedir y contrarrestar las amenazas de la delincuencia grave y organizada existentes y de nueva aparición. El 7 de abril de 2022, Europol celebró una reunión de la EMPACT en la que participaron representantes y expertos de los Estados miembros de la UE y la comunidad de seguridad de la UE para centrarse en las amenazas de la delincuencia grave y organizada que han surgido como consecuencia de la guerra en Ucrania. Entre las medidas concretas que se debatieron se encuentran la recopilación de más datos, la ejecución de acciones operativas de emergencia y la reorientación de las existentes, así como días de acción conjunta *ad hoc*.

CELBET (equipo de expertos en aduanas de las fronteras terrestres orientales y sudorientales), un proyecto de colaboración financiado por la Comisión Europea, está siguiendo los acontecimientos en la frontera como parte de su misión con el fin de prestar apoyo operativo y orientaciones a los agentes de aduanas y está haciendo seguimiento de las incautaciones de las aduanas en los pasos fronterizos de la frontera de la UE (Polonia, Eslovaquia, Hungría y Rumanía) con Ucrania.

Actividad delictiva y terrorista

Aunque todavía no ha surgido una amenaza terrorista inminente en la UE en relación con la invasión de Ucrania, la necesidad de vigilancia es evidente.

El aumento de los riesgos de actividad delictiva y terrorista subrayan la importancia de que los Estados miembros hagan uso de las bases de datos de la UE pertinentes, como el Sistema de Información Schengen, introduzcan datos en ellas cuando sea necesario, y los consulten durante los controles de las personas que entran a la UE. Esto ayudará a garantizar que las personas que suponen una amenaza para la seguridad interior de la UE sean identificadas en las fronteras exteriores. La Agencia de la Unión Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA), sigue garantizando la plena disponibilidad y eficacia de los sistemas de gestión de las fronteras de la UE. Las directrices[28] a los Estados miembros han aclarado la forma de equilibrar la necesidad de garantizar el tratamiento fluido de las llegadas a la frontera exterior a la vez que se siguen realizando los controles de seguridad necesarios.

[27] El grupo de análisis de amenazas de Google observó un creciente número de agentes de riesgo usando la guerra en Ucrania como un reclamo en campañas de *phishing* y de programas maliciosos. Los investigadores de la empresa de seguridad de internet Cyren informan de un aumento de las criptoestafas que sacan provecho del conflicto a través del uso de sitios web falsos para hacer donaciones.

[28] Comunicación de la Comisión por la que se proporcionan directrices operativas para la gestión de las fronteras exteriores a fin de facilitar el cruce de fronteras en las fronteras entre la UE y Ucrania, (2022/C 104 I/01).

Preparación

Además de las directrices y la coordinación, la preparación de la UE se ha intensificado mediante el despliegue del personal de las agencias de la UE.

Europol ha enviado a equipos operativos a los Estados miembros de la UE limítrofes con Ucrania. Estos equipos están compuestos por agentes invitados de Europol procedentes de los Estados miembros y expertos de Europol en Hungría, Lituania, Polonia, Rumanía y Eslovaquia, así como Moldavia[29]. Los agentes invitados de Europol apoyan a las autoridades nacionales con inspecciones de seguridad de segunda línea en las fronteras exteriores de la UE. Los expertos de Europol prestan apoyo mediante la recopilación y evaluación de información para detectar amenazas terroristas y delictivas, apoyar las investigaciones, e identificar a personas que suponen un riesgo al intentar entrar en la UE. Estos equipos operativos recopilan información que contribuye a las evaluaciones de amenazas delictivas disponibles para los Estados miembros. Esta actividad de recopilación de información policial confidencial permite a Europol anticipar los avances y coordinar las actividades operativas con los Estados miembros de la UE para responder a las actividades de los grupos delictivos que buscan sacar provecho de la guerra en Ucrania y aprovechar la participación activa de Europol con la policía Ucrania a través del funcionario de enlace ucraniano presente en la sede de Europol, en los Países Bajos.

La **Agencia Europea de la Guardia de Fronteras y Costas (Frontex)** también está presente en los Estados miembros y en los países vecinos de la UE para apoyar las operaciones de control fronterizo: más de 2 100 guardias de fronteras se encuentran actualmente desplegados por toda la UE, en los Balcanes Occidentales y en Moldavia. **La Agencia de Asilo de la Unión Europea (AAUE)** ha enviado al menos a 750 efectivos a los Estados miembros meridionales de la UE y a Lituania para apoyar las actividades operativas, reforzar las capacidades de acogida y ayudar en los procedimientos de asilo.

Sobre la base de la **Decisión Prüm** actual[30], que establece un marco para que los Estados miembros desplieguen a los agentes policiales para operaciones conjuntas como las patrullas conjuntas, la Comisión y la Presidencia francesa del Consejo de la Unión Europea enviaron una carta conjunta a todos los Estados miembros para determinar las necesidades y solicitar el despliegue de funcionarios de policía, a fin de poner en marcha patrullas conjuntas en los Estados miembros de la UE situados en primera línea y más afectados por los pasos fronterizos masivos a causa de la guerra. La Comisión financiará estos despliegues en el marco del Fondo de Seguridad Interior o de la autoridad policial.

Lucha contra la trata de seres humanos

La UE ha estado alerta, desde los primeros días de la guerra, en cuanto a los riesgos de un ámbito concreto de la actividad delictiva que podría beneficiarse de los grandes desplazamientos de personas que buscan seguridad en la UE. Ha sido fundamental para impedir que los traficantes de personas se dirijan a las personas vulnerables que se desplazan

[29] Desde el 3 de mayo, Europol ha enviado a 1 efectivo de Europol y a 3 agentes invitados a Eslovaquia, a 1 efectivo de Europol a Polonia, a 1 efectivo de Europol y a 4 agentes invitados a Rumanía, y a 2 agentes invitados a Hungría. A Moldavia se ha enviado a 1 efectivo de Europol y a 2 agentes invitados.

[30] 2008/615/JAI, 2008/616/JAI.

y que son principalmente **mujeres y niños**, utilizando, por ejemplo, falsas ofertas de transporte o alojamiento.

En marzo, Europol y Eurojust emitieron notificaciones de alerta rápida a las autoridades nacionales competentes acerca de la posible trata de seres humanos y de la explotación de víctimas procedentes de Ucrania. Eurojust ayuda a mejorar el intercambio de información y a acelerar la cooperación judicial, en especial con Ucrania, y las investigaciones sobre la trata de seres humanos se han remitido a la agencia para su coordinación.

El coordinador de la UE para la lucha contra la trata de seres humanos ha mantenido reuniones con la red de ponentes nacionales o mecanismos equivalentes de la UE, las agencias de justicia y asuntos de interior y la plataforma de la sociedad civil de la UE contra la trata de seres humanos para el intercambio de información sobre las acciones necesarias para impedir y luchar contra los abusos y proteger a las víctimas. Se han abierto investigaciones sobre posibles casos en varios Estados miembros.

La UE se ha mostrado rápida y enérgica a la hora de garantizar una respuesta coordinada a esta amenaza real para las personas que necesitan la ayuda de la UE. Las directrices operativas[31], en especial las relativas al reto de la trata de seres humanos, se ofrecieron rápidamente a los Estados miembros que están implementando la Directiva sobre protección temporal para apoyar a aquellas personas que huyen de la guerra en Ucrania. Como parte del plan de diez puntos para una coordinación europea más estrecha a la hora de acoger a las personas que huyen de la guerra en Ucrania[32], presentado en el Consejo de Justicia y Asuntos de Interior el 28 de marzo de 2022, la coordinadora de la UE para la lucha contra la trata de seres humanos, en colaboración con las Agencias de la UE y los Estados miembros, ha elaborado un Plan Común de Lucha contra la Trata de Seres Humanos[33] para impedir la trata de seres humanos y ayudar a las víctimas. Se presta especial atención al registro de entidades y personas (en especial voluntarios) que quieren proporcionar alojamiento, transporte y otros tipos de asistencia, así como a la realización de comprobaciones de antecedentes penales. La Comisión también ha colaborado con la AAUE para apoyar la detección de víctimas de la trata de seres humanos cuando se realizan evaluaciones sanitarias en los centros de acogida. Los menores no acompañados o separados se encuentran en riesgo particular de abuso, explotación sexual o delincuencia forzada. Las directrices operativas indicadas anteriormente también ofrecen orientaciones para ayudar a los Estados miembros a tramitar la llegada, acogida y apoyo de niños y menores no acompañados especialmente. Con el fin de concienciar a las personas en situación de riesgo, la Comisión ha puesto en marcha un sitio web específico con una sección que incluye consejos prácticos sobre cómo evitar a los traficantes.

Si bien se han adoptado algunas medidas expresamente para aumentar la preparación como respuesta a las nuevas condiciones derivadas de la guerra, otras medidas clave proceden de **iniciativas legislativas** ya en curso antes de la guerra de agresión de Rusia contra Ucrania.

[31] C/2022/1806, EUR-Lex - 52022XC0321(03) - ES - EUR-Lex (europa.eu).

[32] https://ec.europa.eu/home-affairs/10-point-plan-stronger-european-coordination-welcoming-people-fleeing-war-ukraine_en.

[33] https://ec.europa.eu/home-affairs/news/new-anti-trafficking-plan-protect-people-fleeing-war-ukraine-2022-05-11_en.

La Comisión acoge con satisfacción el acuerdo en febrero de 2022 sobre el nuevo mandato de **Europol**[34] que, una vez ejecutado, permitirá a Europol apoyar mejor a los Estados miembros en la lucha contra la delincuencia organizada y el terrorismo. A continuación, la agencia dispondrá de los instrumentos y salvaguardias adecuados para apoyar a las fuerzas policiales en el análisis de macrodatos para investigar la delincuencia y en el desarrollo de métodos pioneros para luchar contra la ciberdelincuencia. Estos cambios vienen acompañados de un marco reforzado de protección de datos, así como de una mejor supervisión y rendición de cuentas parlamentarias.

El paquete sobre **cooperación policial** presentado por la Comisión el 8 de diciembre de 2021[35] y que actualmente se está negociando, reforzará la cooperación entre los funcionarios de policía de todos los Estados miembros, haciendo que el intercambio de datos sea más rápido, fácil y seguro, y mejorando y haciendo más eficiente la cooperación policial operativa sobre el terreno. La Comisión pide al Parlamento Europeo y al Consejo que adopten rápidamente este paquete de medidas.

Una vez adoptadas y aplicadas, estas propuestas legislativas respaldarán a las autoridades policiales en la lucha contra la delincuencia organizada transfronteriza. Esto será especialmente importante en un contexto en el que las organizaciones delictivas de Ucrania pueden intentar reubicarse debido a la situación actual y continuar con sus actividades en la UE.

La **Misión asesora de la UE en Ucrania** ha estado apoyando la reforma de las instituciones policiales y del Estado de Derecho en el país desde 2014. En marzo de 2022, se revisó el mandato de la Misión lo que permitió el apoyo en los pasos fronterizos de Ucrania con Polonia, Rumanía y Eslovaquia, contribuyendo al conocimiento de la situación sobre las actividades delictivas transfronterizas, en especial la trata de seres humanos, y el flujo de artículos humanitarios hacia Ucrania.

IV. ARMAS, MATERIALES PELIGROSOS E INCIDENTES CRÍTICOS

La guerra ha aumentado masivamente la circulación de armas de fuego y otras armas dentro de la propia Ucrania, lo que plantea nuevos riesgos para la UE y para otros estados limítrofes con Ucrania.

Vigilancia y coordinación

Las directrices operativas publicadas en marzo proporcionaron asesoramiento a los Estados miembros sobre cómo afrontar el reto del aumento de la circulación de armas de fuego en un momento de llegadas en masa a las fronteras exteriores de la UE[36]. Estas directrices destacan que la presencia de armas de fuego debe controlarse continuamente y que nadie sin autorización debe poder entrar en la UE con un arma. Cuando las autoridades ucranianas

[34] COM/2020/796.
[35] COM(2021) 780, COM(2021) 782, COM(2021) 784.
[36] Comunicación de la Comisión por la que se proporcionan directrices operativas para la gestión de las fronteras exteriores a fin de facilitar el cruce de fronteras entre las fronteras de la UE y Ucrania, (2022/C 104 I/01).

comuniquen la pérdida de algunas de estas armas de fuego, los Estados miembros deben comunicarlo en el Sistema de Información Schengen.

Es fundamental que todos los envíos de armas de fuego a Ucrania se registren adecuadamente, con toda la información pertinente (en especial el tipo, el país y el año de fabricación, la marca, el modelo, el calibre y el número de serie) a fin de facilitar la trazabilidad de dichas armas de fuego, tanto en Ucrania como en la UE.

La UE ha lamentado públicamente los temerarios ataques militares de Rusia contra instalaciones civiles, nucleares, biológicas y químicas de Ucrania y en sus inmediaciones, así como las actuaciones que han puesto en peligro la seguridad de dichas instalaciones. La Comisión supervisa la situación en Ucrania, prestando especial atención a la amenaza radiológica que es de las mayores preocupaciones desde el punto de vista de la seguridad interior de la UE[37]. La Comisión también supervisa posibles amenazas químicas y ha establecido un mecanismo de coordinación interna en caso de que sea necesaria una rápida evaluación del riesgo.

Preparación

Ucrania ya es uno de los países considerados clave para acciones concretas a nivel exterior en el Plan de Acción de la UE sobre el Tráfico de Armas de Fuego 2020-2025. También existe una acción operativa específica en la región, incluida Ucrania, en el marco de EMPACT Armas de Fuego. Sin embargo, dados los riesgos de desvío de las armas de fuego, serán necesarios proyectos específicos financiados por la Unión, así como una cooperación operativa con Europol, Frontex y el apartado de EMPACT Armas de Fuego. La Comisión pronto presentará una propuesta de revisión del Reglamento sobre armas de fuego[38] relativo a las exportaciones, las importaciones y el tránsito armas de fuego civiles, como parte del marco jurídico y operativo global para impedir, detectar, investigar y perseguir el tráfico de armas de fuego.

Con el fin de mejorar la preparación y la respuesta de la UE ante los riesgos para la salud pública, como las amenazas QBRN, la Comisión está desarrollando reservas estratégicas de capacidades de respuesta a través del Mecanismo de Protección Civil de la UE, financiado por la Autoridad de Preparación y Respuesta ante Emergencias Sanitarias (HERA, por sus siglas en inglés)[39]. Los servicios de la Comisión están trabajando juntos en el desarrollo de una reserva estratégica de rescEU de 540,5 millones EUR. Esta reserva consistirá en equipos y medicamentos, vacunas y otros tratamientos para pacientes expuestos a agentes de emergencia QBRN, así como en la reserva de descontaminación de rescEU para facilitar equipos de descontaminación y de respuesta compuestos por expertos. Como primer paso inmediato, la UE ha movilizado su reserva médica de rescEU para adquirir comprimidos de yoduro de potasio que pueden emplearse para proteger a las personas de los efectos nocivos

[37] La Comisión organizará, en colaboración con los socios estadounidenses, un taller centrado en los riesgos relativos a los materiales radiológicos en los hospitales que quedan fuera del control reglamentario.

[38] Reglamento (UE) n.º 258/2012 del Parlamento Europeo y del Consejo, de 14 de marzo de 2012, por el que se aplica el artículo 10 del Protocolo de las Naciones Unidas contra la falsificación y el tráfico ilícito de armas de fuego, sus piezas y componentes y municiones, que complementa la Convención de las Naciones Unidas contra la delincuencia transnacional organizada, y por el que se establecen autorizaciones de exportación y medidas de importación y tránsito para las armas de fuego, sus piezas y componentes y municiones.

[39] Plan de trabajo de 2022 de la HERA (europa.eu).

de la radiación, así como otros artículos que se necesitan urgentemente en Ucrania. Casi tres millones de comprimidos de yodo ya han sido entregados en Ucrania a través del Mecanismo de Protección Civil de la UE, con la ayuda de Francia y España.

V. ACCIÓN COORDINADA PARA EXIGIR RESPONSABILIDAD POR LA AGRESIÓN DE RUSIA

La UE está desempeñando un papel decisivo en las acciones de la comunidad internacional para presionar a Rusia para que ponga fin a su agresión contra el Estado ucraniano y los civiles ucranianos atrapados en el conflicto, lo que es inaceptable y contrario al Derecho internacional. Esta presión incluye medidas para indicar las consecuencias para los autores que incluyen sanciones severas y medidas para detectar y facilitar el enjuiciamiento de los crímenes de guerra.

Medidas restrictivas y decomiso

Desde el reconocimiento por parte de Rusia, el 21 de febrero de 2022, de las zonas no controladas por el Gobierno de las provincias ucranianas de Donetsk y Lugansk y la invasión de Ucrania, el 24 de febrero de 2022, la UE ha impuesto la mayor serie de medidas restrictivas de la historia contra Rusia. Hasta la fecha, se han adoptado cinco paquetes de sanciones. Estas medidas se centran en sectores clave, en especial las finanzas, el comercio, el transporte, la defensa y los medios, y están dirigidas a las élites políticas y militares, así como a destacados oligarcas rusos y bielorrusos. Las listas incluyen ya a más de mil personas y ochenta entidades. En el Consejo se está debatiendo un sexto paquete de sanciones.

Las repercusiones de estas y anteriores medidas restrictivas contra particulares y empresas de Rusia y Bielorrusia serán tan fuertes como firme su ejecución. La coordinación de la UE puede contribuir en gran medida a cerrar a posibles lagunas, y la Comisión ha proporcionado un amplio apoyo a las partes interesadas, a través de orientaciones escritas, reuniones de las partes interesadas y un grupo de expertos específico, así como una variedad de recursos para facilitar el cumplimiento.

Además, la Comisión ha creado el grupo de trabajo «Inmovilización y Decomiso» que reúne a los servicios de la Comisión, a los Estados miembros, a Eurojust y a Europol. Hasta la fecha, los Estados miembros han comunicado que han inmovilizado activos por un valor de 9 890 millones EUR[40]. El 11 de abril, Europol, junto con los Estados miembros, Eurojust y Frontex, pusieron en marcha la Operación Oscar para apoyar las investigaciones financieras y judiciales contra activos de origen delictivo propiedad de personas físicas y jurídicas sujetas a sanciones de la UE en relación con la guerra de Rusia contra Ucrania. El grupo de trabajo «Inmovilización y Decomiso» de la UE colabora estrechamente con el grupo de trabajo «Las élites rusas, sus representantes y los oligarcas rusos», creado por países del G7 (Alemania, Canadá, Francia, Italia, Japón, Estados Unidos y Reino Unido y socios afines como Australia, así como el grupo de trabajo US KleptoCapture y el grupo de trabajo ucraniano.

El grupo de trabajo «Inmovilización y Decomiso» sirve de plataforma para coordinar y facilitar el intercambio de información y experiencia en todos los Estados miembros para ofrecer orientaciones sobre la aplicación de sanciones y para facilitar el intercambio de

[40] También hay una cantidad de activos bloqueados del Banco Central ruso de aproximadamente 23 000 millones EUR.

mejores prácticas en materia de investigaciones judiciales y decomiso. En concreto, es importante que las autoridades policiales estén alertas y sean diligentes en relación con posibles delitos por parte de las personas y entidades sancionadas. El grupo de trabajo también tiene por objeto proponer debates sobre el posible despliegue de los fondos decomisados, por ejemplo, para contribuir a la reconstrucción de Ucrania.

La Comisión está adoptando hoy en día un paquete de **recuperación y decomiso de activos**[41] que tiene en cuenta las lecciones extraídas de la aplicación de las medidas restrictivas de la Unión contra personas y entidades rusas y bielorrusas. Facilitará la aplicación efectiva de las medidas restrictivas de la UE en toda la Unión permitiendo el rápido rastreo e identificación de los bienes que sean propiedad de personas o entidades objeto de dichas medidas, o que estén controlados por dichas personas o entidades. El marco mejorado de recuperación y decomiso de activos también se aplicará al incumplimiento de las medidas restrictivas y, de este modo, garantizará el rastreo, el embargo preventivo, la gestión y el decomiso efectivos de los ingresos derivados del incumplimiento de las medidas restrictivas. Con el fin de garantizar que los activos de las personas y entidades que infringen las medidas restrictivas puedan realmente ser decomisados, la Comisión también está adoptando hoy en día propuestas de Decisión del Consejo para que se incluya el incumplimiento de sanciones en la lista de delitos de la UE del artículo 83, apartado 1, del TFUE[42], acompañadas de una Comunicación[43], con el fin de proponer una Directiva para acercar la definición de las infracciones penales y las sanciones de las infracciones de las medidas restrictivas.

De manera más general, este paquete supone un paso crucial en la lucha contra la delincuencia organizada. Mantiene los compromisos de la Comisión adoptados en la Estrategia de la Unión de la Seguridad y la Estrategia contra la Delincuencia Organizada 2020-2025[44]. Revisa la Directiva sobre decomiso de 2014, la Decisión del Consejo de 2007sobre los organismos de recuperación de activos (ORA), y la Decisión marco de 2005 relativa al decomiso de los productos, instrumentos y bienes relacionados con el delito, a fin de reforzar las capacidades de seguimiento e identificación, y en última instancia, decomisar los beneficios ilícitos y hacer frente a las muy bajas tasas de decomiso en la UE[45]. El paquete amplía el alcance de las infracciones penales cubiertas y las normas en materia de decomiso en los casos en los que no es posible una condena penal para un delito concreto, pero en los que los activos provienen claramente de actividades delictivas. La revisión también fortalece la gestión eficaz de los activos inmovilizados y decomisados y refuerza la capacidad de los organismos de recuperación de activos para trazar y detectar los activos de origen ilícito. El nuevo marco de recuperación de activos de la UE está diseñado para abordar la compleja modalidad de funcionamiento de las organizaciones delictivas, que con frecuencia operan a través de las fronteras, en especial mediante criptoactivos.

Respuesta judicial coordinada

41 COM(2022) 245.
42 COM(2022) 247.
43 COM(2022) 249.
44 COM(2021) 170.
45 Europol estima que solamente el 2 % de los activos de origen delictivo son inmovilizados (2 400 millones EUR) y el 1 % decomisados (1 200 millones EUR), mientras que los ingresos procedentes de actividades delictivas en los principales mercados delictivos de la UE ascendieron a 139 000 millones EUR en 2019 (el 1 % del PIB de la UE).

También ha continuado el trabajo a escala de la UE para garantizar una respuesta judicial coordinada a los **delitos internacionales** supuestamente cometidos en Ucrania, para que los autores puedan responder por ellos.

Dos Estados miembros y Ucrania crearon un equipo conjunto de investigación (ECI) para investigar crímenes de guerra, crímenes contra la humanidad y otros delitos internacionales supuestamente cometidos en territorio ucraniano. Eurojust presta apoyo jurídico, analítico, financiero y logístico a este ECI. El 25 de abril de 2022, la Fiscalía de la Corte Penal Internacional se unió al ECI como participante[46] y se espera la incorporación de nuevos participantes pronto.

El 25 de abril de 2022, la Comisión presentó una propuesta para modificar el Reglamento Eurojust[47] a fin de que Eurojust conserve, analice y almacene las pruebas de los delitos internacionales. Eurojust y Europol seguirán colaborando estrechamente a lo largo de este proceso. También desempeña un papel fundamental en la coordinación de la respuesta judicial la Red contra el Genocidio, cuya secretaría alberga Eurojust, que ha preparado un atlas de las ONG activas actualmente en Ucrania y apoya a los profesionales nacionales de los Estados miembros y de Ucrania que se ocupan de casos pendientes relacionados con la guerra.

En abril de 2022, el Consejo volvió a revisar el mandato de la **Misión asesora de la UE en Ucrania**, preparando el camino para el apoyo de la Misión a las autoridades ucranianas en la investigación y el enjuiciamiento de los delitos internacionales cometidos en el contexto de la agresión militar de Rusia. La Misión proporcionará a las autoridades ucranianas asesoramiento estratégico sobre la investigación y el enjuiciamiento de los delitos internacionales, las modificaciones necesarias en la legislación ucraniana, la estrategia de comunicación, así como la formación en asuntos relacionados. La Misión es parte de una serie de iniciativas de coordinación en este contexto y, junto con la Delegación de la UE, es parte del Grupo Consultivo UE-EE. UU. sobre Crímenes Atroces para Ucrania.

VI. MANIPULACIÓN DE INFORMACIÓN E INJERENCIA POR PARTE DE AGENTES EXTRANJEROS

Los avances geopolíticos actuales han puesto de relieve los riesgos de la injerencia extranjera. La agresión militar de Rusia contra Ucrania ha estado acompañada de actividades de **injerencia y manipulación** de la información. Se han empleado alegaciones infundadas de «nazismo» y «genocidio» contra el Gobierno de Ucrania, operaciones de banderas falsas y acusaciones sin fundamento contra la OTAN y Occidente para justificar los brutales ataques a Ucrania, al tiempo que se han suprimido la libertad de expresión y la información independiente en Rusia. Persiste el riesgo de manipulación del material audiovisual y de desinformación que Rusia puede intentar usar como pretexto para nuevos ataques militares, para socavar la determinación de la resistencia ucraniana, dividir a la comunidad internacional en su oposición a la guerra o sembrar dudas sobre los incumplimientos del Derecho internacional por parte de Rusia. En la Brújula Estratégica, la UE se comprometió a responder con firmeza a la manipulación de información y a la injerencia por parte de agentes extranjeros, así como a mejorar su resiliencia y capacidad de contrarrestar dichas amenazas[48].

---

46 https://www.eurojust.europa.eu/eurojust-and-the war-in-ukraine.

47 COM(2022) 187 final.

48 https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf.

La manipulación del debate democrático dentro de la UE es la temática del Plan de Acción para la Democracia Europea, el plan coordinado de la Comisión para abordar la desinformación y aumentar la resiliencia democrática[49].

Vigilancia y coordinación

La Unión Europea respondió a través de una acción decisiva y coordinada a la campaña de desinformación de Rusia en el contexto de la agresión militar contra Ucrania. La UE ha colaborado estrechamente con sus Estados miembros a través del sistema de alerta rápida, y con los socios internacionales como la OTAN, Estados Unidos, Canadá y el mecanismo de respuesta rápida del G7, para compartir conocimientos sobre las tendencias y tácticas de manipulación empleadas por el Kremlin. Se han intensificado los trabajos para desmontar las manipulaciones del Kremlin, especialmente a través del sitio web EUvsDisinfo, que emite en inglés, ruso, ucraniano y otros idiomas, para ofrecer información objetiva dentro de la UE, en Ucrania y en la región, así como dentro de Rusia. Desde el 2 de marzo, se ha suspendido la retransmisión y la difusión de los canales de los medios estatales rusos RT y Sputnik en la UE o dirigidos a la UE, como consecuencia de las medidas restrictivas adoptadas por la UE. Las plataformas en línea, las principales redes sociales, los anunciantes y el sector de la publicidad signatarios del Código de Buenas Prácticas en materia de Desinformación[50] están adoptando medidas urgentes para limitar la desinformación relativa a la agresión de Rusia a Ucrania. La Comisión y el SEAE están supervisando estos esfuerzos. La información facilitada muestra que las plataformas han intensificado sus herramientas de supervisión e intervención relativas a la guerra.

Además, se están poniendo rápidamente en marcha acciones para apoyar a los países de Asia Central y los Balcanes Occidentales para reforzar la resiliencia de la información y contrarrestar la manipulación extranjera de la información y la desinformación.

Preparación

El uso manifiesto de la manipulación de información e injerencia por parte de agentes extranjeros, en especial la desinformación como uno de los instrumentos de las amenazas híbridas, ha conferido una mayor urgencia al seguimiento del Plan de Acción para la Democracia Europea. En los últimos meses, las instituciones de la UE han apoyado a los Estados miembros en la lucha contra la manipulación de información e injerencia por parte de agentes extranjeros, en especial en el marco del sistema de alerta rápida, compartiendo conocimientos sobre las tácticas empleadas por estos agentes y sobre las estrategias de respuesta. Siguen en curso los debates para seguir reforzando la respuesta global de la UE ante la manipulación de información e injerencia por parte de agentes extranjeros, sobre la base de una nota conceptual presentada por el SEAE sobre el desarrollo de un **conjunto de instrumentos** específicos para hacer frente a esta amenaza. Esto integra las medidas internas existentes y las nuevas herramientas de la UE en virtud de la política exterior y de seguridad común. También se beneficiará de la acción intensificada de la comunicación estratégica del Servicio Europeo de Acción Exterior[51], así como de la Comisión.

---

[49] COM(2020) 790.

[50] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[51] La División de Comunicación Estratégica, Grupos Especiales y Análisis de la Información del Servicio Europeo de Acción Exterior presta apoyo en materia de comunicación estratégica a la hora de aplicar la política exterior y de seguridad de la UE en regiones prioritarias conexas (vecindad meridional y oriental y

El Observatorio Europeo de los Medios de Comunicación Digitales («EDMO», por sus siglas en inglés) estableció un grupo de trabajo sobre desinformación tras el estallido de la guerra en Ucrania y coordina acciones mediante verificadores de datos e investigadores en su red. Ha analizado cómo los conspiracionistas de la COVID-19 han apostado rápidamente por la difusión de bulos prorrusos, un cambio observado en algunos Estados miembros[52].

La propuesta de Ley de Servicios Digitales busca adaptarse a la rápida evolución de las tecnologías digitales y lo que esto supone para los desafíos tecnológicos y democráticos, como el discurso de odio, la desinformación en línea y las estrategias de desestabilización. Los avances significativos en las negociaciones del Parlamento Europeo y del Consejo deberían permitir una rápida adopción del paquete de medidas.

VII. PREPARACIÓN MÁS AMPLIA

En un momento en el que la guerra ha vuelto a Europa, así como de importantes cambios geopolíticos, la coordinación de la seguridad en la UE se ha intensificado, haciendo uso de iniciativas ya en curso antes de la guerra de agresión de Rusia contra Ucrania. Las iniciativas centradas principalmente en la seguridad exterior de la UE tienen importantes implicaciones para la agenda interior de la Unión de la Seguridad.

El 15 de febrero de 2022, la Comisión presentó el **paquete «Defensa»**[53], con una serie de iniciativas en ámbitos críticos para la defensa y la seguridad dentro de la UE. Esta contribución de la Comisión a la defensa y la seguridad europeas abarca la gama completa de desafíos. Propone medidas concretas para lograr un mercado europeo de defensa más integrado y competitivo, en especial con la mejora de la cooperación dentro de la UE y el desarrollo de economías de escala. También implica una hoja de ruta sobre tecnologías críticas para la seguridad y la defensa a fin de impulsar la investigación, el desarrollo tecnológico y la innovación en estos sectores y reducir las dependencias en las tecnologías críticas y en las cadenas de valor. Este paquete también tiene por objeto reforzar la dimensión de defensa del espacio a escala de la UE. Además, analiza la manera en que la Comisión puede intensificar sus acciones contra las amenazas híbridas, en particular en el ámbito del ciberespacio, mejorar la movilidad militar dentro y fuera de Europa, y seguir abordando los retos del cambio climático relacionados con la defensa. Para complementar este trabajo, la Comunicación conjunta «**Sobre el análisis de los déficits de inversión en materia de defensa y el camino a seguir**»[54], de 18 de mayo, examina los déficits relacionados con las capacidades y la industria que deben abordarse con el fin de apoyar a los Estados miembros de la UE más expuestos y de determinar medidas para mitigar las carencias detectadas.

La resiliencia de la UE con respecto a estas amenazas también implica enfoques orientados a las capacidades en todos los sectores de la seguridad, tal y como se defiende en el Plan de

---

los Balcanes Occidentales), mediante el desarrollo y la ejecución de acciones de comunicación estratégica específicas centradas en fomentar las políticas, los valores, los objetivos y los intereses de la UE.

52 https://edmo.eu/2022/03/30/how-covid-19-conspiracy-theorists-pivoted-to-pro-russian-hoaxes/.

53 https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/contributing-european-defence_en

54 JOIN(2022) 24.

acción de la Comisión sobre las sinergias entre las industrias civil, de la defensa y espacial[55]. Se está trabajando para promover enfoques orientados a las capacidades en el ámbito de la seguridad interior y la aplicación de las leyes.

El 21 de marzo de 2022, el Consejo adoptó la **Brújula Estratégica para la Seguridad y la Defensa**[56], refrendada poco después por el Consejo Europeo. La Brújula describe un ambicioso plan de acción para reforzar la política de la UE en materia de seguridad y defensa de aquí a 2030. El objetivo es hacer de la UE un proveedor de seguridad más fuerte y capaz, que proteja a sus ciudadanos y contribuya a la paz y la seguridad internacionales. Contiene propuestas concretas, con un calendario de ejecución muy preciso, para mejorar la capacidad de la UE para actuar con decisión en situaciones de crisis.

Uno de los resultados de la Brújula Estratégica es el desarrollo de un **conjunto de instrumentos híbridos de la UE** que deben ofrecer un marco para una respuesta coordinada a las campañas híbridas que afectan a la UE y a sus Estados miembros, incluidas medidas internas y externas. Tras la determinación de las bases de referencia sectoriales sobre resiliencia llevada a cabo a principios de 2022[57], se finalizará un análisis de las carencias y las necesidades. En este marco, la UE seguirá desarrollando la preparación, la resiliencia y la respuesta a amenazas derivadas de la agresión de Rusia y cualquier otro intento de desestabilizar las democracias y el orden multilateral basado en normas.

VIII. PERSPECTIVAS

Mirando hacia el futuro, la UE deberá permanecer muy atenta a la evolución de las amenazas y aumentar **la preparación y la resiliencia ante todas las eventualidades**. Las repercusiones de la guerra pueden adoptar diferentes formas, de las cuales no todas pueden evaluarse todavía.

Aún se desconoce la magnitud del desplazamiento de las redes delictivas ucranianas. Los casos anteriores de Eurojust indican una tendencia de tráfico de heroína desde Afganistán a la UE a través de Ucrania, como lo corrobora el Observatorio Europeo de las Drogas y las Toxicomanías (OEDT)[58]. La inestabilidad puede dificultar aún más que se actúe contra el comercio de heroína a través de esta ruta, lo que conlleva el riesgo de un posible aumento del flujo de drogas hacia la UE.

Es más probable que algunos riesgos para la UE aumenten al final o durante posibles pausas de los combates. Se prestará especial atención a la circulación de armas de fuego, con un aumento del riesgo cuando cese la lucha en Ucrania. La experiencia pasada también apunta al riesgo de que el retorno de combatientes extranjeros que han adquirido experiencia de

---

55 COM(2021) 70.

56 Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales: https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/es/pdf.

57 SWD(2022) 21 final.

58 Informe sobre la situación de la droga y el alcohol en Ucrania en 2020 (según los datos de 2019) del OEDT: *Stopping the trafficking of a heroin substitute in France, Poland and Ukraine, including the planning and execution of a controlled delivery* [«Detener el tráfico de un sustituto de la heroína en Francia, Polonia y Ucrania, en particular la planificación y ejecución de una entrega controlada», documento en inglés], 2021/00446, Eurojust, mayo de 2020.

combate y que han entrado en contacto con grupos extremistas pueda traer la acción terrorista a la UE en una fase posterior. Este posible fenómeno debe ser supervisado atentamente, y la Comisión ya está facilitando debates entre los Estados miembros sobre los desafíos que plantea el retorno de voluntarios extranjeros de origen extremista violento.

En vista de estas posibles amenazas, es importante que continúe la aplicación de la Estrategia de la Unión de la Seguridad, en especial con la aplicación de estrategias clave como la Estrategia de Ciberseguridad de la UE, la Estrategia contra la Delincuencia Organizada 2020-2025, la Agenda de lucha contra el terrorismo (2020-2025), el Plan de Acción de la UE sobre el Tráfico de Armas de Fuego 2020-2025, la Estrategia de la UE sobre la lucha contra la trata de seres humanos 2021-2025 y la Estrategia de la UE sobre Drogas 2021-2025.

Proseguirán los esfuerzos para dotar a la UE del marco legislativo necesario. Por ejemplo, la Comisión está preparando la evaluación de impacto de una propuesta por la que se regula la comercialización y el uso de sustancias químicas de alto riesgo.

IX. CONCLUSIÓN

La Unión de la Seguridad sigue desempeñando su papel a la hora de preparar a la UE y a sus Estados miembros para hacer frente a las amenazas existentes y posibles. La guerra de agresión de Rusia contra Ucrania ha demostrado la rapidez con la que las amenazas teóricas pueden volverse reales y destaca la importancia de la vigilancia, la coordinación y la preparación.

Este cuarto informe de situación sobre la Estrategia de la Unión de la Seguridad demuestra que la UE es capaz de adaptarse, incluso ante amenazas excepcionales e imprevistas como la guerra de agresión de Rusia contra Ucrania. La aplicación decidida de la Estrategia de la Unión de la Seguridad es más importante que nunca.