Consejo de la Unión Europea

Bruselas, 14 de septiembre de 2017
(OR. en)

12211/17

CYBER 132
RELEX 767
JAI 790
ENFOPOL 413
TELECOM 212
MI 633
RECH 308

NOTA DE TRANSMISIÓN

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	13 de septiembre de 2017
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	JOIN(2017) 450 final
Asunto:	COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE

Adjunto se remite a las Delegaciones el documento – JOIN(2017) 450 final.

Adj.: JOIN(2017) 450 final

COMISIÓN
EUROPEA

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

Bruselas, 13.9.2017
JOIN(2017) 450 final

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO

Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE

1. INTRODUCCIÓN

La ciberseguridad es fundamental tanto para nuestra prosperidad como para nuestra seguridad. A medida que nuestra vida cotidiana y la economía se vuelven más dependientes de las tecnologías digitales, aumenta nuestro grado de exposición. Los responsables y los objetivos de los incidentes de ciberseguridad son cada vez más diversos. Las actividades cibernéticas maliciosas no solo amenazan nuestras economías y los esfuerzos destinados a lograr un Mercado Único Digital, sino también el funcionamiento mismo de nuestras democracias, nuestras libertades y nuestros valores. El futuro de nuestra seguridad dependerá de la transformación de nuestra capacidad para proteger a la UE contra las amenazas cibernéticas: tanto la infraestructura civil como la capacidad militar se basan en el uso de sistemas digitales seguros. Así lo ha reconocido el Consejo Europeo de junio de 2017[1] y así se admite en la Estrategia Global de Política Exterior y de Seguridad de la Unión Europea[2].

Los riesgos están aumentando exponencialmente. Hay estudios que sugieren que el impacto económico de la ciberdelincuencia se quintuplicó entre 2013 y 2017, y podría cuadruplicar sus niveles actuales de aquí a 2019[3]. Los programas de secuestro de archivos a cambio de un rescate[4] («ransomware») han proliferado especialmente, siendo los recientes ataques[5] un reflejo del aumento significativo de la ciberdelincuencia. No obstante, este tipo de programas está lejos de ser la única amenaza.

Las amenazas cibernéticas provienen tanto de agentes estatales como no estatales; a menudo son actividades delictivas con una motivación económica, pero también pueden tener un carácter político y estratégico. La amenaza criminal se ve agravada por la frontera difusa entre ciberdelincuencia y delito «tradicional», ya que los delincuentes usan Internet como una forma de ampliar sus actividades, pero también como una fuente para encontrar nuevos métodos y herramientas para cometer delitos[6]. Sin embargo, en la gran mayoría de los casos, las posibilidades de localizar al delincuente son mínimas, y las de emprender acciones penales contra él son aún menores.

Al mismo tiempo, los agentes estatales están logrando cada vez más sus objetivos geopolíticos no solo a través de métodos tradicionales, como la fuerza militar, sino también mediante el uso de herramientas cibernéticas más discretas, como la interferencia en los procesos democráticos internos. El uso del ciberespacio como campo de batalla, de forma exclusiva o como parte de una táctica híbrida, es ahora ampliamente reconocido. Las campañas de desinformación, la propagación de noticias falsas y las operaciones cibernéticas dirigidas a infraestructuras vitales son cada vez más comunes y exigen una respuesta. Por esta razón, en su Documento de reflexión sobre el futuro de la defensa europea[7], la Comisión subrayó la importancia de la cooperación en materia de ciberdefensa.

---

1 http://www.consilium.europa.eu/es/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Véase, por ejemplo, el informe de McAfee y el Centro de Estudios Estratégicos e Internacionales «Net losses: Estimating the Global Cost of Cybercrime» («Pérdidas netas: estimación del coste total de la ciberdelincuencia»), de junio de 2014.

4 El «ransomware» es un tipo de programa informático malintencionado («malware») que impide o limita el acceso de los usuarios a su sistema, ya sea bloqueando la pantalla o restringiendo el acceso a los archivos de los usuarios a menos que se pague un rescate.

5 En mayo de 2017, el ataque del «ransomware» WannaCry afectó a más de 400 000 ordenadores de más de 150 países. Un mes más tarde, el ataque del «ransomware» Petya golpeó Ucrania y varias empresas en todo el mundo.

6 Evaluación de la amenaza de la delincuencia grave y organizada de EUROPOL de 2017.

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_es.pdf.

A menos que mejoremos sustancialmente nuestra ciberseguridad, el riesgo aumentará en paralelo con la transformación digital. Para 2020, se prevé que decenas de miles de millones de dispositivos del «Internet de las cosas» estén conectados a la red, aunque todavía no se ha dado prioridad a la ciberseguridad en su diseño[8]. La incapacidad para proteger los dispositivos que controlarán nuestras redes eléctricas, automóviles y transporte público, fábricas, finanzas, hospitales y hogares podría tener consecuencias devastadoras y mermar la confianza del consumidor en las tecnologías emergentes. El riesgo de ataques por motivos políticos contra objetivos civiles y de que existan deficiencias en la ciberdefensa militar agrava aún más el peligro.

El enfoque establecido en la presente Comunicación conjunta permitirá a la UE estar mejor preparada para afrontar estas amenazas. Incrementará la resiliencia y la autonomía estratégica, potenciando las capacidades de tecnología y destrezas, y ayudando a construir un mercado único sólido. Para ello es necesario contar con las estructuras adecuadas para fortalecer la ciberseguridad y reaccionar cuando sea necesario, con la plena participación de todos los agentes clave. Este enfoque también disuadirá en mayor medida los ciberataques, al multiplicar los esfuerzos para detectar, rastrear y pedir cuentas a los responsables. Asimismo, reconocerá la dimensión global al desarrollar la cooperación internacional como plataforma para el liderazgo de la UE en materia de ciberseguridad. Estos pasos se basan en los enfoques del Mercado Único Digital, la Estrategia Global, la Agenda Europea de Seguridad[9], la Comunicación conjunta sobre la lucha contra las amenazas híbridas[10] y la Comunicación sobre la puesta en marcha del Fondo Europeo de Defensa[11][12].

La UE ya está trabajando en muchas de estas cuestiones, y es el momento de reunir las distintas líneas de trabajo. En 2013, la UE estableció una Estrategia de Ciberseguridad que abría una serie de líneas de trabajo para mejorar la ciberresiliencia[13]. Sus principales objetivos y principios, destinados a fomentar un ecosistema cibernético fiable, seguro y abierto, siguen siendo válidos. Pero ante un paisaje de amenazas que evolucionan y se agravan de forma continua, es necesario emprender nuevas acciones para resistir y disuadir los ataques en el futuro[14].

El alcance de sus políticas y los instrumentos, las estructuras y las capacidades de que dispone colocan a la UE en una buena posición para abordar la ciberseguridad. Si bien los Estados miembros siguen siendo responsables de su seguridad nacional, la dimensión y la naturaleza transfronteriza de la amenaza constituyen son un motivo poderoso para una actuación de la UE que ofrezca incentivos y respaldo a los Estados miembros a fin de desarrollar y mantener más y mejores capacidades nacionales de ciberseguridad, a la vez que se crea una capacidad a nivel europeo. Este enfoque pretende animar a todos los actores –la UE, los Estados miembros, la industria y los particulares– a otorgar a la ciberseguridad la prioridad que

---

8 IDC and TXT Solutions (2014), SMART 2013/0037 Cloud and IoT combination («Soluciones IDC y TXT (2014), SMART 2013/0037 Combinación de Internet de las cosas con la nube»), estudio para la Comisión Europea.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 Este enfoque ha sido avalado también por el asesoramiento científico independiente proporcionado por el Grupo de Alto Nivel de Asesores Científicos del Mecanismo de Asesoramiento Científico de la Comisión Europea (véanse las referencias a continuación).

13 JOIN (2013) 1 final. Hay una evaluación de esta estrategia disponible en SWD (2017) 295.

14 Salvo que se indique lo contrario, las propuestas de la presente Comunicación son presupuestariamente neutrales. Cualquier iniciativa que tenga implicaciones presupuestarias respetará los procedimientos presupuestarios anuales y no prejuzgará el próximo marco financiero plurianual, posterior a 2020.

necesita para aumentar la resiliencia y dar una mejor respuesta de la UE a los ciberataques. Proporcionará medidas concretas para ayudar a detectar e investigar cualquier forma de incidente cibernético contra la UE y sus Estados miembros, así como para dar una respuesta adecuada, en particular persiguiendo a los delincuentes. Permitirá que la acción exterior de la UE promueva eficazmente la ciberseguridad a escala global. El resultado será un giro en la estrategia de la UE, que pasará de un enfoque reactivo a uno proactivo a fin de proteger la prosperidad, la sociedad y los valores europeos, así como los derechos y las libertades fundamentales, dando respuesta a las amenazas presentes y futuras.

2. REFORZAR LA RESILIENCIA DE LA UE A LOS CIBERATAQUES

Una fuerte ciberresiliencia necesita un enfoque colectivo y amplio. Ello exige estructuras más sólidas y eficaces para promover la ciberseguridad y responder a los ciberataques en los Estados miembros, pero también en las propias instituciones, agencias y organismos de la UE. De igual modo, se necesita un enfoque más amplio y transversal para impulsar la ciberresiliencia y la autonomía estratégica, con un mercado único sólido, grandes avances en la capacidad tecnológica de la UE y un número mucho mayor de expertos cualificados. En el fondo, se trata de asumir que la ciberseguridad es un desafío común para todos los ciudadanos, de forma que participen los diferentes niveles de la administración, la economía y la sociedad.

2.1 Fortalecer la Agencia de Seguridad de las Redes y de la Información de la Unión Europea

La **Agencia de Seguridad de las Redes y de la Información de la Unión Europea (**ENISA) desempeña un papel clave en el fortalecimiento de la resiliencia y la respuesta cibernética de la UE, pero su actividad está limitada por su mandato actual. Por ello, la Comisión presenta un ambicioso proyecto de reforma, que incluye un **mandato permanente de la agencia**[15]. Se garantizará de este modo que ENISA pueda prestar apoyo a los Estados miembros, las instituciones de la UE y las empresas en ámbitos clave, como la aplicación de la Directiva relativa a la seguridad de las redes y sistemas de información[16] («Directiva SRI») y el marco de certificación de la ciberseguridad propuesto.

La nueva ENISA tendrá una importante función consultiva en la elaboración y la ejecución de las políticas, incluida la promoción de la coherencia entre las iniciativas sectoriales y la Directiva SRI y la colaboración en la apertura de centros de puesta en común y análisis de la información en sectores críticos. ENISA elevará el listón y mejorará la preparación europea mediante la organización de ejercicios paneuropeos anuales de ciberseguridad, en los que se combinará la respuesta a diferentes niveles. También apoyará el desarrollo de la política de la UE en materia de certificación de la seguridad de las tecnologías de la información y la comunicación (TIC), además de desempeñar un papel importante en la intensificación de la cooperación operativa y la gestión de crisis en toda la UE. La agencia también servirá como centro de información y conocimientos de la comunidad de ciberseguridad.

Una comprensión rápida y común de las amenazas y los incidentes a medida que se desarrollan es un requisito previo para decidir si se necesita una mitigación conjunta o una acción de respuesta respaldada por la UE. Ese intercambio de información requiere la participación de todos los agentes pertinentes –organismos y agencias de la UE, así como los

[15] COM(2017) 477.

[16] 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.

Estados miembros– a nivel técnico, operativo y estratégico. ENISA, en colaboración con los organismos competentes de los Estados miembros y la UE, en particular la red de equipos de respuesta a incidentes de seguridad informática[17], el CERT-UE, Europol y el Centro de Análisis de Inteligencia de la UE (INTCEN), también contribuirá a sensibilizar sobre la situación a nivel europeo. Esta labor puede constituir una aportación al análisis de las amenazas y la formulación de políticas en el contexto del seguimiento regular del panorama de amenazas y de la cooperación operativa efectiva, así como en respuesta a incidentes transfronterizos a gran escala.

2.2 Hacia un mercado único de la ciberseguridad

El crecimiento - en términos de productos, servicios y procesos - del mercado de la ciberseguridad en la UE se ve frenado de diversas formas. Un aspecto clave es la falta de programas de certificación de la ciberseguridad reconocidos en toda la Unión para crear estándares más elevados de resiliencia de los productos y afianzar la confianza del mercado de la UE. Por ello, la Comisión presenta una propuesta de **marco de certificación de la ciberseguridad de la UE**[18]. El marco establecería el procedimiento para la creación de programas de certificación de la ciberseguridad a escala de la UE que abarquen productos, servicios y sistemas que adapten el nivel de seguridad al uso de que se trate (infraestructuras críticas o dispositivos de consumo)[19]. Esto ofrecería una ventaja evidente a las empresas, al evitar la necesidad de pasar por diferentes procesos de certificación en el comercio transfronterizo, reduciendo así los costes administrativos y financieros. El uso de los programas desarrollados en este marco también ayudaría a mejorar la confianza de los consumidores, con un certificado de conformidad que informe y tranquilice a los compradores y usuarios sobre las propiedades de seguridad de los productos y servicios que adquieren y utilizan. Esto permitiría que un nivel elevado de ciberseguridad se convirtiera en una fuente de ventaja competitiva. El resultado reforzaría la resiliencia, ya que los productos y servicios de TIC serían evaluados formalmente con un conjunto definido de estándares de ciberseguridad, los cuales podrían desarrollarse en consonancia con los trabajos de mayor alcance que se están llevando a cabo sobre los estándares de las TIC[20].

Los programas del marco serían voluntarios y no generarían ninguna obligación reglamentaria para los distribuidores o los proveedores de servicios. Los programas no contravendrían ninguno de los requisitos legales aplicables, como la legislación de la UE sobre protección de datos.

Una vez establecido el marco, la Comisión invitará a las partes interesadas a centrarse en tres áreas prioritarias:

- Seguridad de las aplicaciones de elevado riesgo o críticas[21]: los sistemas de los que dependemos en nuestras actividades diarias, desde nuestros automóviles hasta la maquinaria de las fábricas, desde los sistemas más grandes - como los aviones o las centrales eléctricas - hasta los más pequeños - como los aparatos médicos), tienen un carácter cada vez más digital e interconectado. Por tanto, los componentes básicos de TIC en tales productos y sistemas requerirían rigurosas evaluaciones de seguridad.

[17] Como dispone el artículo 9 de la Directiva SRI.
[18] COM(2017) 477
[19] Un nivel de seguridad indica el grado de rigor de la evaluación de la seguridad y suele ser proporcional al nivel de riesgo asociado con estas áreas o funciones de aplicación (es decir, se requiere un mayor nivel de garantía para los productos o servicios de TIC utilizados en áreas o funciones de alto riesgo).
[20] COM(2016) 176.
[21] Se haría una excepción si la certificación obligatoria o voluntaria se rigiera por otros actos de la Unión.

- La ciberseguridad de productos, redes, sistemas y servicios digitales ampliamente extendidos que utilizan tanto el sector privado como el público para defenderse de los ataques y cumplir las obligaciones reglamentarias[22], tales como la encriptación de correos electrónicos, los cortafuegos y las redes privadas virtuales; es fundamental que el uso generalizado de dichas herramientas no propicie nuevas fuentes de riesgo o nuevas vulnerabilidades.

- El uso de los métodos de «seguridad mediante el diseño» en dispositivos de consumo masivo de bajo coste, digitales e interconectados que conforman el Internet de las cosas: los programas del marco podrían emplearse para señalar que los productos se fabrican utilizando métodos de fabricación seguros de última generación, que han sido sometidos a pruebas de seguridad adecuadas y que los proveedores se han comprometido a actualizar sus programas informáticos en caso de que se descubran nuevas vulnerabilidades o amenazas.

Estas prioridades deben tener especialmente en cuenta la evolución del panorama de las amenazas cibernéticas, así como la importancia de servicios esenciales como el transporte, la energía, la atención sanitaria, la banca, las infraestructuras de los mercados financieros, el agua potable o la infraestructura digital[23].

Aunque no se puede garantizar que ningún producto, sistema o servicio de TIC sea «100 %» seguro, existen varios defectos bien conocidos y documentados en el diseño de productos de TIC que pueden ser explotados para perpetrar ataques. La adopción por parte de los fabricantes de dispositivos, programas y equipos informáticos conectados de un enfoque de «seguridad mediante el diseño» garantizaría que se tuviera en cuenta la ciberseguridad antes de comercializar nuevos productos. Formaría parte del principio de «deber de diligencia», que se desarrollará en colaboración con el sector empresarial y que podría reducir las vulnerabilidades de los productos y programas informáticos mediante la aplicación de diversos métodos, que van desde el diseño hasta las pruebas y la verificación, incluida la verificación formal si es posible, el mantenimiento a largo plazo y el uso de procesos seguros del ciclo de vida de desarrollo, así como actualizaciones y parches para solucionar las vulnerabilidades previamente desconocidas y la rápida actualización y reparación[24]. Con ello aumentaría también la confianza de los consumidores en los productos digitales.

Además, debe reconocerse el importante papel de los investigadores de seguridad externos a la hora de descubrir vulnerabilidades en los productos y servicios existentes, y se han de crear las condiciones que permitan la revelación coordinada de las vulnerabilidades[25] en los

---

[22] Por ejemplo, la Directiva (UE) 2016/1148, el Reglamento (UE) 2016/679, la Directiva (UE) 2015/2366 y otras normativas propuestas, como el Código Europeo de las Comunicaciones Electrónicas, exigen que las organizaciones pongan en práctica medidas de seguridad adecuadas para afrontar los riesgos de ciberseguridad pertinentes.

[23] Los sectores incluidos en el ámbito de aplicación de la 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.

[24] Cybersecurity in the European Digital Single Market («Ciberseguridad en el Mercado único Digital Europeo»), Grupo de Alto Nivel de Asesores Científicos, marzo de 2017.

[25] La revelación coordinada de las vulnerabilidades constituye una forma de cooperación que facilita y permite a los investigadores de seguridad notificar las vulnerabilidades al propietario o al vendedor del sistema de información, brindando a la empresa la posibilidad de diagnosticarlas y solucionarlas de manera correcta y oportuna antes de que se revele información detallada sobre estas vulnerabilidades a terceros o al público.

distintos Estados miembros, tomando como base las mejores prácticas[26] y las normas pertinentes[27].

Al mismo tiempo, **sectores específicos** se enfrentan a problemas concretos y deben desarrollar sus propios métodos. De este modo, las estrategias generales de ciberseguridad se complementarían con estrategias de ciberseguridad específicas para sectores como los servicios financieros[28], la energía, el transporte y la salud[29].

La Comisión ya ha destacado los aspectos específicos relativos a la **responsabilidad** asociada a las nuevas tecnologías digitales[30] y se está trabajando para analizar sus repercusiones; los siguientes pasos concluirán en junio de 2018. La ciberseguridad plantea cuestiones relativas a la imputación de daños a las empresas y las cadenas de suministro, por lo que la falta de respuesta a dichas cuestiones obstaculizará el desarrollo de un mercado único sólido de productos y servicios de ciberseguridad.

Por último, el desarrollo del mercado único de la UE también depende de la incorporación de la ciberseguridad a las políticas de comercio e inversión. El efecto de las adquisiciones extranjeras sobre tecnologías críticas, de las cuales la ciberseguridad es un ejemplo importante, constituye un aspecto clave en el marco de **la evaluación de la inversión extranjera directa en la Unión Europea**[31], cuyo objetivo es examinar las inversiones de terceros países por razones de seguridad y de orden público. Del mismo modo, los requisitos de ciberseguridad han creado ya barreras comerciales para los bienes y servicios de la UE en sectores importantes de varias economías de terceros países. El marco de certificación de la ciberseguridad de la UE reforzará aún más la posición internacional de Europa, y debería complementarse con esfuerzos continuos para desarrollar normas globales de alta seguridad y acuerdos de reconocimiento mutuo.

2.3 Aplicación plena de la Directiva relativa a la seguridad de las redes y sistemas de información

Dado que las principales herramientas de ciberseguridad se encuentran hoy en manos nacionales, la UE ha reconocido la necesidad de potenciar las normas. Debido a la naturaleza cada vez más globalizada, digitalmente dependiente e interconectada de sectores clave como la banca, la energía o el transporte, los incidentes de ciberseguridad a gran escala rara vez afectan a un único Estado miembro.

La Directiva relativa a la seguridad de las redes y sistemas de información (la «Directiva SRI») fue la primera ley de ciberseguridad a escala de la UE[32]. Fue concebida para aumentar la resiliencia mediante la mejora de las capacidades nacionales de ciberseguridad, el fomento de una mayor cooperación entre los Estados miembros y la exigencia a las empresas de los

---

[26] Por ejemplo, la «Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations» («Guía de buenas prácticas sobre revelación de vulnerabilidades. De los desafíos a las recomendaciones»), ENISA, 2016.

[27] ISO/IEC 29147:2014 «Information Technology— Security Techniques— Vulnerability Disclosure» («Tecnología de la información — Técnicas de seguridad —Revelación de vulnerabilidades»).

[28] El próximo trabajo de la Comisión sobre tecnología financiera tratará la ciberseguridad del sector financiero.

[29] Por ejemplo, en el sector de la energía, que combina tecnologías de la información muy antiguas y de vanguardia, particularmente para cumplir los requisitos en tiempo real de la red eléctrica.

[30] COM(2017) 228.

[31] COM(2017) 478.

[32] 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.

sectores económicos principales de que adopten prácticas eficaces de gestión de riesgos e informen a las autoridades nacionales sobre los incidentes graves. Estas obligaciones también se aplican a tres tipos de proveedores clave de servicios de Internet: servicios de computación en la nube, motores de búsqueda y mercados en línea. Tiene como objetivo un enfoque más sólido y sistemático, así como un mejor flujo de información.

La plena aplicación de la Directiva por todos los Estados miembros en mayo de 2018 resulta esencial para la ciberresiliencia de la UE. El proceso está siendo respaldado por el trabajo colectivo de los Estados miembros, que en otoño de 2017 se traducirá en la publicación de directrices de apoyo a una aplicación más armonizada, especialmente en lo relativo a los operadores de servicios esenciales. Además, la Comisión está preparando una Comunicación[33], como parte de este paquete de ciberseguridad, con el fin de apoyar sus esfuerzos, proporcionando las mejores prácticas de los Estados miembros pertinentes para la implementación de la Directiva, así como orientaciones sobre la aplicación práctica de esta última.

Un ámbito en el que la Directiva deberá recibir apoyo es el flujo de información. Por ejemplo, la Directiva solo abarca los sectores estratégicos clave pero, como es lógico, sería necesario un enfoque similar de todas las partes afectadas por ciberataques para realizar una evaluación sistemática de las vulnerabilidades y los puntos de entrada de los ciberatacantes. Además, la cooperación y el intercambio de información entre los sectores público y privado se enfrentan a una serie de obstáculos. Los gobiernos y las autoridades públicas son reacios a compartir información relevante en materia de ciberseguridad por temor a comprometer la seguridad nacional o la competitividad. Las empresas privadas suelen mostrarse reticentes a compartir datos sobre sus vulnerabilidades cibernéticas y las pérdidas resultantes por temor a revelar información comercial delicada, poner en riesgo su reputación o infringir las normas de protección de datos[34]. Es necesario fortalecer la confianza para que las asociaciones público-privadas apoyen una cooperación más amplia y el intercambio de información en un mayor número de sectores. El papel de los Centros de Puesta en Común y Análisis de la Información es particularmente importante para crear la confianza necesaria que permita compartir información entre los sectores privado y público. Se han dado algunos primeros pasos en sectores críticos específicos, como la aviación, mediante la creación del Centro Europeo de Ciberseguridad en la Aviación[35], y la energía, con la creación de Centros de Puesta en Común y Análisis de la Información[36]. La Comisión contribuirá en todo lo posible a este enfoque con el apoyo de ENISA, dando especial prioridad a los sectores que prestan servicios esenciales, tal y como se definen en la Directiva SRI.

2.4 Resiliencia mediante una respuesta rápida de emergencia

---

33 COM(2017) 476.

34 Cybersecurity in the European Digital Single Market («Ciberseguridad en el Mercado único Digital Europeo»), Grupo de Alto Nivel de Asesores Científicos, marzo de 2017. Un motivo particular de preocupación son los secretos comerciales, respecto a los cuales la Comunicación de julio de 2016 «Reforzar el sistema de ciberresiliencia de Europa» señala la reticencia a informar sobre el robo cibernético de secretos comerciales y la importancia de que existan canales de información fiables que garanticen la confidencialidad.

35 https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

36 Se trata de organizaciones sin ánimo de lucro, dirigidas por sus miembros y constituidas por entidades públicas y privadas con el objetivo de compartir información sobre ciberamenazas, riesgos, prevención, mitigación y respuesta. Véanse, p. ej., los Centros Europeos de Puesta en Común y Análisis de la Información sobre Energía (http://www.ee-isac.eu).

Cuando se produce un ataque cibernético, una respuesta rápida y eficaz puede atenuar su impacto. De este modo se puede demostrar también que las autoridades públicas no son impotentes ante los ciberataques, y contribuir a crear confianza. En lo que se refiere a la respuesta de las propias instituciones de la UE, en primer lugar, los aspectos cibernéticos deben integrarse en los mecanismos de gestión de crisis de la UE ya existentes: la respuesta integrada a crisis políticas de la UE, coordinada por la Presidencia del Consejo[37], y los sistemas generales de alerta rápida de la UE[38]. La necesidad de responder a un incidente o ataque cibernético particularmente grave podría constituir un motivo suficiente para que un Estado miembro invoque la cláusula de solidaridad de la UE[39].

Una respuesta rápida y eficaz también depende de la existencia de un mecanismo rápido de intercambio de información entre todos los actores clave a nivel nacional y de la UE, lo que a su vez requiere claridad sobre sus respectivas funciones y responsabilidades. La Comisión ha consultado a las instituciones y los Estados miembros sobre un «plan director» que asegure un proceso eficaz de respuesta operativa a nivel de la Unión y de los Estados miembros ante un incidente cibernético a gran escala. El **plan director**, presentado en una Recomendación[40] en este paquete, explica cómo se integra la ciberseguridad en los mecanismos de gestión de crisis ya existentes a nivel de la UE, y establece los objetivos y los modos de cooperación entre los Estados miembros, así como entre los Estados miembros y las instituciones, los servicios, las agencias y los organismos pertinentes de la UE[41], a la hora de dar respuesta a incidentes y crisis de ciberseguridad a gran escala. La Recomendación también pide a los Estados miembros y a las instituciones de la UE que establezcan un marco de respuesta a las crisis de ciberseguridad de la UE para operativizar el plan director. Este plan se someterá periódicamente a pruebas de gestión de crisis cibernéticas y de otro tipo[42], actualizándose cuando sea necesario.

Dado que los incidentes de ciberseguridad podrían afectar sustancialmente al funcionamiento de las economías y la vida cotidiana de las personas, una opción sería investigar la posibilidad de crear un **Fondo de respuesta a las emergencias de ciberseguridad**, siguiendo el ejemplo de otros mecanismos de crisis de este tipo en otros ámbitos políticos de la UE. Esto permitiría a los Estados miembros solicitar ayuda a nivel de la UE durante o tras un incidente grave, siempre que el Estado miembro haya establecido un sistema prudente de ciberseguridad antes de dicho incidente, que incluya la plena aplicación de la Directiva SRI, una gestión de riesgos madura y estructuras de supervisión a nivel nacional. Dicho Fondo, que complementaría los mecanismos existentes de gestión de crisis a nivel de la UE, podría desplegar una capacidad de respuesta rápida en aras de la solidaridad y financiar acciones específicas de respuesta de emergencia, tales como la sustitución de los equipos afectados o el despliegue de instrumentos de mitigación o respuesta, aprovechando los conocimientos nacionales, en la línea del Mecanismo de Protección Civil de la Unión.

2.5 Una red de competencias en ciberseguridad con un Centro Europeo de Competencia e Investigación en Ciberseguridad

---

37 Esto permite coordinar al más alto nivel político las respuestas a crisis intersectoriales graves.

38 Se permite así el intercambio de información y la coordinación internas en casos de crisis multisectoriales emergentes o amenazas previsibles o inminentes que requieran medidas a nivel de la UE.

39 En virtud del artículo 222 del Tratado de Funcionamiento de la Unión Europea.

40 C(2017) 6100.

41 Incluidos Europol, ENISA, el Equipo de Respuesta a Emergencias Informáticas de la UE para las instituciones, los organismos y las agencias de la UE (CERT-UE) y el Centro de Análisis de Inteligencia de la UE (INTCEN).

42 Por ejemplo, las que lleva a cabo ENISA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

Las herramientas tecnológicas de ciberseguridad son activos estratégicos, así como tecnologías clave para el futuro crecimiento. Es de interés estratégico para la UE garantizar que se conserven y desarrollen las capacidades esenciales para garantizar su economía, sociedad y democracia digitales, proteger los equipos y programas informáticos críticos y proporcionar servicios clave de ciberseguridad.

La asociación público-privada sobre ciberseguridad[43] creada en 2016 fue un primer paso importante que generará 1 800 millones EUR de inversión hasta 2020. Sin embargo, la magnitud de la inversión en curso en otras partes del mundo[44] indica que la UE debe hacer más en términos de inversión y superar la fragmentación de las capacidades repartidas por toda la UE.

Dada la sofisticación de la tecnología de ciberseguridad, la inversión a gran escala necesaria y la necesidad de soluciones que funcionen en todo su territorio, la UE tiene un valor añadido que ofrecer. Tomando como base la labor de los Estados miembros y de la asociación público-privada, la capacidad de ciberseguridad de la UE se seguirá reforzando a través de una **red de centros de competencia en ciberseguridad**[45], cuyo eje será un **Centro Europeo de Competencia e Investigación en Ciberseguridad**. Esta red y su centro estimularían el desarrollo y el despliegue de tecnología de la ciberseguridad y complementarían los esfuerzos de capacitación en este ámbito a nivel nacional y de la UE La Comisión iniciará una evaluación de impacto para examinar las opciones disponibles, incluida la posibilidad de crear una empresa común, con vistas a establecer esta estructura en 2018.

Como primer paso y para orientar futuras reflexiones, la Comisión propondrá que se lance una fase piloto en el marco del programa Horizonte 2020 para ayudar a reunir a los centros nacionales en una red y así crear un nuevo impulso en materia de competencia cibernética y desarrollo tecnológico. Prevé proponer una inyección financiera a corto plazo de 50 millones EUR para este fin. Esta actividad complementará la implementación en curso de la asociación público-privada sobre ciberseguridad.

La puesta en común y la configuración de los esfuerzos de investigación constituirían el núcleo de la red y el enfoque inicial del Centro. Para apoyar el desarrollo de capacidades industriales, el Centro podría actuar como un gestor de proyectos de capacidades apto para administrar proyectos multinacionales. Esto también daría un nuevo impulso a la innovación y la competitividad de la industria de la UE en la escena mundial en el desarrollo de las tecnologías digitales de la próxima generación, incluida la inteligencia artificial, la computación cuántica, las cadenas de bloques y las identidades digitales seguras, así como garantizaría el acceso de las empresas a datos masivos, todo ello fundamental para la ciberseguridad en el futuro. El Centro también se basaría en el trabajo de la UE para ampliar la infraestructura de computación de alto rendimiento: esto es esencial para el procesamiento de grandes cantidades de datos, el cifrado y el descifrado rápido de datos, la comprobación de identidades, la simulación de ciberataques y el análisis de material de vídeo[46].

La red de centros de competencia también podría tener capacidad para apoyar a las empresas mediante pruebas y simulaciones que respalden la certificación de ciberseguridad descrita en el apartado 2.2. Su participación en toda la gama de actividades de ciberseguridad de la UE

[43] C (2016) 4400 final.

[44] Estados Unidos invertirá 19 000 millones USD en ciberseguridad solo en 2017, un 35 % más que en 2016. La Casa Blanca, Oficina del Secretario de Prensa: 'Fact Sheet: Cybersecurity National Action Plan («Hoja informativa: Plan nacional de acción de ciberseguridad)»', 9 de febrero de 2016

[45] La red incluiría los centros de ciberseguridad existentes y futuros creados en los Estados miembros, cuyos miembros serían, por lo general, centros de investigación y laboratorios públicos.

[46] COM(2012) 45 final y COM(2016) 178 final.

garantizaría una actualización continua de sus objetivos según las necesidades. El Centro tendría como objetivo elevar las normas de ciberseguridad, no solo en los sistemas de tecnología y ciberseguridad, sino también en el desarrollo de competencias de alto nivel para los profesionales, a través del suministro de soluciones y plantillas para los esfuerzos nacionales de desarrollo de destrezas digitales. En este sentido, también mejoraría las capacidades de ciberseguridad a escala de la UE y se basaría en sinergias, en particular con ENISA, el CERT-UE, Europol, el posible futuro Fondo de respuesta a emergencias en materia de ciberseguridad y los CSIRT nacionales.

La red de competencias debe prestar especial atención a la falta de capacidad europea para evaluar el **cifrado** de los productos y servicios utilizados por los ciudadanos, las empresas y los gobiernos dentro del Mercado Único Digital. Una encriptación fuerte es la base de los sistemas seguros de identificación digital que desempeñan un papel clave en la eficacia de la ciberseguridad[47]; también protege la propiedad intelectual de las personas y garantiza derechos fundamentales, como la libertad de expresión y la protección de los datos personales, además de garantizar un comercio en línea seguro[48].

Dado que los mercados civil y militar de la ciberseguridad de la UE comparten desafíos comunes[49] y que la tecnología de doble uso requiere una estrecha colaboración en áreas críticas, se podría desarrollar una segunda fase de la red y su Centro con una dimensión de ciberdefensa, respetando plenamente las disposiciones del Tratado relativas a la política común de seguridad y defensa. Además de su enfoque tecnológico, esta dimensión de defensa podría contribuir a la cooperación entre los Estados miembros en el ámbito de la ciberdefensa, en particular mediante el intercambio de información, la sensibilización sobre la situación, la acumulación de experiencias y las reacciones coordinadas, así como al desarrollo de capacidades comunes de los Estados miembros. También podría servir de plataforma que permita a los Estados miembros identificar las prioridades de la ciberdefensa de la UE, investigar soluciones comunes, contribuir al desarrollo de estrategias compartidas y facilitar la realización de actividades de formación, ejercicios y pruebas conjuntas en el ámbito de la ciberseguridad a nivel europeo, así como dar respaldo al trabajo sobre las categorías y normas de ciberdefensa, desempeñando el Centro un papel consultivo y de apoyo. Para llevar a cabo las actividades mencionadas, el Centro deberá trabajar en estrecha colaboración y de forma plenamente complementaria con la Agencia Europea de Defensa en el ámbito de la ciberdefensa, así como con ENISA en el ámbito de la ciberresiliencia. Esta dimensión de la defensa tendría en cuenta el proceso iniciado por el documento de reflexión sobre el futuro de la defensa europea.

El alto nivel de resiliencia requerido en la defensa cibernética exige que se definan objetivos específicos para los esfuerzos en investigación y tecnología. Los proyectos de defensa cibernética o las tecnologías desarrolladas por las empresas podrían beneficiarse de la financiación del Fondo Europeo de Defensa en las fases de investigación y desarrollo[50]. Áreas específicas tales como los sistemas de cifrado basados en tecnologías cuánticas, la

---

[47] La Comisión tiene previsto convocar, en el marco del programa Horizonte 2020, un nuevo Premio Horizonte que concederá 4 millones EUR a la mejor solución innovadora de métodos de autenticación electrónica eficaces.

[48] Cybersecurity in the European Digital Single Market («Ciberseguridad en el mercado único digital europeo»), Grupo de Alto Nivel de Asesores Científicos, marzo de 2017.

[49] «Study on synergies between the civilian and the defence cybersecurity markets» («Estudio de las sinergias entre los mercados civil y militar de la ciberseguridad») (Optimity; SMART 2014-0059).

[50] En adelante, el Programa Europeo de Desarrollo Industrial en materia de Defensa dará prioridad a los proyectos de ciberdefensa, siendo este uno de los temas de la convocatoria de propuestas que se lanzará en 2018.

sensibilización de la situación cibernética, los sistemas biométricos de control de acceso, la detección avanzada de amenazas persistentes o la recopilación de datos podrían ser particularmente relevantes en este contexto. El Alto Representante, la Agencia Europea de Defensa y la Comisión apoyarán a los Estados miembros en la determinación de los ámbitos en los que podría considerarse la posibilidad de que el Fondo Europeo de Defensa financiara proyectos comunes de ciberseguridad.

2.6 Creación de una base sólida de competencias cibernéticas de la UE

Existe una fuerte dimensión educativa en la ciberseguridad. La ciberseguridad efectiva depende en gran medida de las competencias de las personas involucradas. Sin embargo, según las previsiones, en el sector privado europeo se necesitarán 350 000 profesionales competentes en ciberseguridad para 2022[51]. La educación en materia de ciberseguridad debe desarrollarse a todos los niveles, empezando por la formación regular de profesionales de la cibernética, una formación adicional en ciberseguridad de todos los especialistas en TIC y nuevos programas específicos de ciberseguridad. Deberían crearse centros de competencia académica sólidos con los que satisfacer las crecientes exigencias en materia de educación y formación; podrían crearse bajo la tutela de un Centro Europeo de Investigación y Competencia en Ciberseguridad y de ENISA. El objetivo sería conseguir que, en el diseño de productos y sistemas de TIC, se incorporen desde las fases iniciales y de forma natural los principios de seguridad. La educación en ciberseguridad no debe limitarse a los profesionales de la TI, sino que debe ser integrada en los planes de estudios de otras áreas, como la ingeniería, la gestión empresarial o el Derecho, así como en las ramas de educación sectoriales. Por último, como parte de la adquisición de competencias digitales en los centros educativos, se debe sensibilizar a los docentes y los alumnos de enseñanza primaria y secundaria sobre la ciberdelincuencia y la ciberseguridad.

La UE, junto con los Estados miembros, debería contribuir también a esta labor, aprovechando el trabajo de la Coalición de empleos y capacidades digitales[52], mediante la creación de programas de aprendizaje en ciberseguridad para las pymes, por ejemplo.

2.7 Promover la ciberhigiene y la ciberconcienciación

Dado que el 95 % de los incidentes se atribuye a «algún tipo de error humano, intencionado o no»[53], el papel que desempeñan las personas resulta evidente. Así pues, la ciberseguridad es responsabilidad de todos. Esto significa que el comportamiento personal, corporativo y de la administración pública, debe cambiar para garantizar que todo el mundo entiende la amenaza y cuenta con las herramientas y las habilidades necesarias para detectar rápidamente y protegerse activamente frente a los ataques. Los ciudadanos necesitan desarrollar hábitos de ciberhigiene, y las empresas y las organizaciones deben adoptar programas adecuados de ciberseguridad basados en el riesgo y actualizarlos regularmente para reflejar el panorama de riesgo en evolución.

La Directiva SRI no solo establece la obligación de los Estados miembros de intercambiar información sobre los ciberataques a nivel de la UE, sino también de establecer estrategias y sistemas nacionales maduros de ciberseguridad para los sistemas de red y de información. Las

[51] Global Information Security Workforce Study 2017 («Estudio del personal de seguridad global de la información»). El déficit total asciende a 1,8 millones.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] «The Cybersecurity Intelligence Index» 2014 de IBM, publicado en Securitymagazine.com el 19 de junio de 2014.

administraciones públicas nacionales y de la UE deberían asumir un liderazgo en la promoción de estos esfuerzos.

En primer lugar, los Estados miembros deberían maximizar la disponibilidad de herramientas de ciberseguridad para las empresas y los ciudadanos. En particular, debería hacerse más para prevenir y atenuar los efectos de la ciberdelincuencia sobre los usuarios finales. Ya existe un ejemplo en la labor de Europol con la campaña «NoMoreRansom»[54], lanzada gracias a la estrecha colaboración entre los servicios policiales y las empresas de ciberseguridad para ayudar a los usuarios a prevenir infecciones por «ransomware» y descifrar datos si son víctimas de un ataque. Esos planes deberían aplicarse a otros tipos de programas maliciosos («malware») en otros ámbitos, y la UE debería desarrollar un **portal único para reunir todas esas herramientas en una ventanilla única**, ofreciendo asesoramiento a los usuarios en materia de prevención y detección de programas maliciosos y enlaces a mecanismos de información.

En segundo lugar, los Estados miembros deberían acelerar el **uso de herramientas cibernéticas más seguras en el desarrollo de la administración electrónica**, y aprovechar al máximo la red de competencias. Debe promoverse la adopción de medios seguros de identificación, tomando como base el marco comunitario de la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior, vigente desde 2016 y que ofrece un entorno regulador predecible en el que poder realizar interacciones electrónicas seguras y transparentes entre empresas, ciudadanos y autoridades públicas[55]. Además, las instituciones públicas, especialmente las que prestan servicios esenciales, deben garantizar que su personal esté capacitado en áreas relacionadas con la ciberseguridad.

En tercer lugar, los Estados miembros deben otorgar a la sensibilización cibernética una prioridad en las **campañas de concienciación**, incluidas las dirigidas a las escuelas, las universidades, la comunidad empresarial y los organismos de investigación. El mes de la ciberseguridad, que se celebra cada año en octubre bajo la coordinación de ENISA, se ampliará para lograr un mayor alcance como parte de un esfuerzo de comunicación común a nivel nacional y de la UE. Igualmente importante es la concienciación sobre las **campañas de desinformación y las noticias falsas** en las redes sociales, destinadas específicamente a socavar los procesos democráticos y los valores europeos. Si bien la responsabilidad primordial sigue estando a nivel nacional (incluso en el caso de las elecciones al Parlamento Europeo), la puesta en común de conocimientos especializados y el intercambio de experiencias a nivel europeo ha demostrado su valor añadido al proporcionar un enfoque orientado hacia la acción[56].

También se reserva un papel importante a la **industria** en general, especialmente los proveedores y fabricantes de servicios digitales. Debe apoyar a los usuarios (ciudadanos, empresas y administraciones públicas) con herramientas que les permitan asumir la responsabilidad de sus propias acciones en línea, dejando claro que el mantenimiento de la

---

54 https://www.nomoreransom.org/.

55 Reglamento (UE) n.º 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (Reglamento «eIDAS»), de 23 de julio de 2014. Por otra parte, la Comisión Europea está proporcionando los fundamentos y las herramientas para la interoperabilidad de la identificación y la firma electrónicas (por ejemplo, los navegadores de listas de confianza) a través del Mecanismo «Conectar Europa».

56 Un ejemplo es el grupo de trabajo East StratCom, puesto en marcha en 2015 por los Estados miembros y el Alto Representante para hacer frente a las campañas de desinformación lanzadas por Rusia. El equipo se dedica al desarrollo de productos de comunicación y campañas centradas en explicar las políticas de la UE en la región de la Asociación Oriental.

ciberhigiene es una parte indispensable de la oferta a los consumidores[57]. Para detectar y eliminar las vulnerabilidades, el sector empresarial debe esforzarse por desarrollar procesos internos que cubran la investigación, la clasificación y la resolución de vulnerabilidades, con independencia del carácter externo o interno de la fuente de vulnerabilidad.

Medidas clave

- Aplicación plena de la Directiva relativa a la seguridad de las redes y sistemas de información.
- Rápida adopción por el Parlamento Europeo y el Consejo del Reglamento por el que se establece un nuevo mandato para ENISA y un marco europeo de certificación[58].
- Iniciativa conjunta de la Comisión y el sector empresarial para definir un principio de «deber de diligencia» a fin de reducir las vulnerabilidades del producto/programa informático y promover la «seguridad mediante el diseño».
- Rápida aplicación del plan director de respuesta a incidentes transfronterizos graves.
- Evaluación de impacto que estudie las posibilidades de una propuesta de la Comisión en 2018 de crear una red de centros de competencia en materia de ciberseguridad y un Centro Europeo de Competencia e Investigación en Ciberseguridad sobre la base de una fase piloto inmediata.
- Apoyo a los Estados miembros en la identificación de los ámbitos en los que podrían considerarse proyectos comunes de ciberseguridad con financiación del Fondo Europeo de Defensa.
- Ventanilla única en toda la UE para ayudar a las víctimas de ciberataques, proporcionando información sobre las últimas amenazas y reuniendo consejos prácticos y herramientas de ciberseguridad.
- Medidas adoptadas por los Estados miembros para incorporar la ciberseguridad a los programas de capacitación, la administración electrónica y las campañas de sensibilización.
- Acciones del sector empresarial para aumentar la formación en ciberseguridad de su personal y adoptar un enfoque de «seguridad mediante el diseño» para sus productos, servicios y procesos.

3. CREAR UNA CIBERDISUASIÓN EFECTIVA EN LA UE

Una disuasión efectiva significa poner en marcha un marco de medidas que sean a la vez creíbles y disuasorias para posibles ciberdelincuentes y ciberatacantes. Mientras que los autores de ciberataques –tanto estatales como no estatales– solo teman al fracaso, carecerán de motivos para dejar de intentarlo. Una respuesta coercitiva más eficaz, centrada en la detección, la rastreabilidad y el emprendimiento de acciones penales contra los ciberdelincuentes, es fundamental para fomentar una disuasión efectiva. A esto se suma la necesidad de que la UE apoye a sus Estados miembros en el desarrollo de capacidades de doble uso en ciberseguridad. Solo comenzaremos a contrarrestar la creciente ola de ciberataques cuando aumentemos las posibilidades de detener y condenar a aquellos que los llevan a cabo. Los ciberataques deben ser investigados con prontitud y sus responsables juzgados, o bien se deben tomar medidas que permitan una respuesta política o diplomática adecuada. En caso de una grave crisis con una significativa dimensión internacional y de

[57] Algunos fabricantes ya están familiarizados con este concepto, ya que ciertas leyes europeas sobre productos (como la Directiva 2006/42/CE sobre maquinaria) imponen principios de «seguridad mediante el diseño».

[58] COM(2017) 477.

defensa, el Alto Representante podría presentar al Consejo alternativas para una respuesta adecuada.

En 2013 se dio un paso hacia la mejora de la respuesta del Derecho penal a los ciberataques con la adopción de la Directiva relativa a los ataques contra los sistemas de información[59]. Esta Directiva estableció normas mínimas relativas a la tipificación de los delitos y penas en el ámbito de los ataques contra los sistemas de información, así como medidas operativas para mejorar la cooperación entre las autoridades. La Directiva ha dado lugar a avances sustanciales en la penalización de los ciberataques a un nivel comparable en todos los Estados miembros, lo que facilita la cooperación transfronteriza de las autoridades policiales que investigan este tipo de delitos. No obstante, todavía queda margen para que la Directiva alcance todo su potencial si los Estados miembros aplican plenamente todas sus disposiciones[60]. La Comisión seguirá prestando apoyo a los Estados miembros en la aplicación de la Directiva, y en la actualidad no considera necesario proponer modificaciones.

3.1 Identificar a los actores maliciosos

Con el fin de aumentar las posibilidades de llevar a sus autores ante la justicia, necesitamos mejorar urgentemente nuestra capacidad para identificar a los responsables de los ciberataques. La búsqueda de información útil para las investigaciones de delitos cibernéticos, sobre todo en forma de rastros digitales, supone un gran reto para los servicios policiales. En consecuencia, necesitamos desarrollar nuestra capacidad tecnológica para investigar de forma eficaz, reforzando al mismo tiempo la unidad de ciberdelincuencia de Europol con expertos cibernéticos. Europol se ha convertido en un agente clave en el apoyo a las investigaciones plurijurisdiccionales de los Estados miembros. Debería convertirse en un centro de conocimientos especializados para los servicios policiales de los Estados miembros en las investigaciones en línea y las técnicas ciberforenses.

La práctica generalizada de colocar a múltiples usuarios, a veces miles de ellos, tras una dirección IP hace que sea técnicamente muy difícil investigar un comportamiento malicioso en línea. En algunos casos, por ejemplo, delitos graves como los abusos sexuales infantiles, es incluso necesario investigar a un gran número de usuarios con el fin de identificar a un agente malicioso. Por ello, la UE fomentará la adopción del nuevo protocolo (IPv6), que permite la asignación de un único usuario por dirección IP, lo que supone una gran ventaja para los servicios policiales y las investigaciones de ciberseguridad. Como primer paso para fomentar dicha adopción, la Comisión incorporará el requisito de pasar al IPv6 en todas sus políticas, incluidos los requisitos en materia de contratación y financiación de proyectos e investigaciones, además de fomentar el uso de los materiales de formación necesarios. Asimismo, los Estados miembros deberían considerar la posibilidad de establecer acuerdos voluntarios con los proveedores de servicios de Internet para impulsar la adopción del IPv6.

Bélgica es el país líder a nivel mundial[61] en porcentaje de adopción del IPv6, resultado de la cooperación de los sectores público y privado. Las partes interesadas pertinentes consideraron la posibilidad de limitar el uso de una dirección IP a un máximo de 16 usuarios

[59] Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información.

[60] COM(2017) 474.

[61] https://www.google.com/intl/es/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

como parte de una medida voluntaria de autorregulación, lo que incentivó la transición al IPv6[62].

En términos más generales, debería existir una promoción aún mayor de la responsabilidad en línea. Esto significa promover medidas para prevenir el abuso de los nombres de dominio para la distribución de mensajes no solicitados o ataques de suplantación de identidad («phishing»). Con este fin, la Comisión trabajará para mejorar el funcionamiento, la disponibilidad y la exactitud de la información en los sistemas de nombres de dominio e IP WHOIS[63], en consonancia con los esfuerzos de la Corporación para la Asignación de Nombres y Números en Internet[64].

3.2 Reforzar la respuesta policial

La **investigación** y el **emprendimiento de acciones penales** eficaces contra la ciberdelincuencia son fundamentales para desalentar los ataques. Sin embargo, el marco procesal actual debe adaptarse mejor a la era de Internet[65]. Nuestros procedimientos pueden verse superados por la velocidad de los ciberataques, que pueden crear la necesidad de una rápida cooperación transfronteriza. Tal y como se anunció en el marco de la Agenda Europea de Seguridad a principios de 2018, la Comisión presentará con este fin propuestas para **facilitar el acceso transfronterizo a las pruebas electrónicas**. Al mismo tiempo, la Comisión está aplicando medidas prácticas para mejorar el acceso transfronterizo a las pruebas electrónicas en las investigaciones penales, lo que incluye la financiación de la formación en materia de cooperación transfronteriza, el desarrollo de una plataforma electrónica para el intercambio de información en la UE y la normalización de las formas de cooperación judicial utilizadas entre los Estados miembros.

Otro obstáculo para el emprendimiento de acciones penales eficaces son los diferentes procedimientos forenses para la recopilación de pruebas electrónicas en las investigaciones de ciberdelincuencia en los Estados miembros. Esta situación podría remediarse mediante el establecimiento de estándares forenses comunes. Además, para mejorar la rastreabilidad y la imputación se han de reforzar las capacidades forenses. Un paso adelante sería desarrollar una mayor capacidad forense en Europol, adaptando los recursos presupuestarios y humanos existentes en el Centro Europeo de Ciberdelincuencia de Europol para satisfacer la creciente necesidad de apoyo operativo en las investigaciones transfronterizas sobre ciberdelincuencia. Otro avance sería replicar el enfoque tecnológico expuesto anteriormente sobre encriptación, observando cómo su abuso por parte de los delincuentes genera desafíos significativos en la lucha contra delitos graves como el terrorismo y la ciberdelincuencia. La Comisión presentará los resultados de las actuales reflexiones sobre el **papel del cifrado en las investigaciones penales**[66] en octubre de 2017[67].

---

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

63 Protocolo de consulta y respuesta ampliamente utilizado para consultar bases de datos que almacenan los usuarios registrados o asignados de un recurso de Internet.

64 La Corporación para la Asignación de Nombres y Números en Internet (ICANN) es una organización sin ánimo de lucro encargada de coordinar el mantenimiento y los procedimientos de varias bases de datos relacionadas con los espacios nominales de Internet.

65 Por citar un ejemplo, el servidor central (virtual) de mando y control de la red infectada («botnet») Avalanche cambió de servidores físicos y dominios cada cinco minutos.

66 Presidencia del Consejo, «Conclusiones del Consejo de Justicia y Asuntos de Interior de 8 y 9 de diciembre de 2016», n.º 15391/16.

67 Octavo informe de evolución hacia una Unión de la Seguridad genuina y efectiva, de 29 de junio de 2017, COM(2017) 354 final.

Dado que Internet carece de fronteras, el marco de cooperación internacional proporcionado por el Consejo de Europa en el **Convenio de Budapest sobre la Ciberdelincuencia**[68] ofrece la posibilidad de utilizar, en un grupo diverso de países, un estándar legal óptimo para las diferentes legislaciones nacionales que regulan la ciberdelincuencia. Se está estudiando la posible adición de un protocolo al Convenio[69], que también podría ofrecer una oportunidad útil para regular la cuestión del acceso transfronterizo a las pruebas electrónicas en un contexto internacional. En lugar de crear nuevos instrumentos jurídicos internacionales para las cuestiones relacionadas con la ciberdelincuencia, la UE pide a todos los países que elaboren una legislación nacional adecuada y traten de cooperar dentro del marco internacional vigente.

La disponibilidad generalizada de herramientas de anonimización hace que sea más fácil para los delincuentes ocultarse. La «**red oscura**»[70] ha abierto nuevas vías para que los delincuentes accedan a materiales de abuso sexual infantil, drogas o armas de fuego, a menudo con poco riesgo de ser detenidos[71]. En la actualidad es también una fuente clave de instrumentos utilizados en delitos cibernéticos, como los programas maliciosos («malware») y las herramientas de pirateo informático («hacking»). La Comisión, junto con las partes interesadas pertinentes, analizará los enfoques nacionales con el fin de identificar nuevas soluciones. Europol debe facilitar y apoyar las investigaciones sobre la red oscura, evaluar las amenazas y ayudar a determinar la jurisdicción, así como dar prioridad a los casos de alto riesgo, por lo que la UE puede desempeñar un papel destacado en la coordinación de la acción internacional[72].

Un tipo de ciberdelincuencia creciente es el uso fraudulento de datos de tarjetas de crédito u otros medios electrónicos de pago. Las credenciales de pago obtenidas mediante ciberataques contra vendedores en línea u otras empresas legítimas se ponen posteriormente a la venta en línea y pueden ser utilizadas por delincuentes para cometer fraudes[73]. La Comisión presentará una propuesta para fomentar la disuasión a través de una **Directiva sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo**[74]. El objetivo es actualizar las normas vigentes en este ámbito y reforzar la capacidad de las fuerzas policiales para hacer frente a esta forma de delincuencia.

---

[68] El Convenio es el primer tratado internacional sobre los delitos cometidos a través de Internet y otras redes informáticas, que regula en particular las infracciones de los derechos de autor, el fraude informático, la pornografía infantil y las violaciones de la seguridad de las redes.
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
En 2017, 55 gobiernos habían ratificado o se habían adherido al Convenio sobre ciberdelincuencia del Consejo de Europa.

[69] Mandato para la preparación del proyecto de un segundo protocolo adicional al Convenio de Budapest sobre la Ciberdelincuencia, T-CY (2017) 3.

[70] La red oscura está formada por contenidos en redes superpuestas que utilizan Internet, pero requieren programas informáticos, configuraciones o autorizaciones de carácter específico para el acceso. La red oscura constituye una pequeña parte de la web profunda, esto es, la parte de la web no indexada por los motores de búsqueda.

[71] Una notable excepción es el reciente desmantelamiento de dos de los mercados criminales más grandes de la red oscura, AlphaBay y Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[72] Europol ya desempeña un papel importante en este ámbito. Para un ejemplo reciente, véase: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

[73] Los productos del fraude suponen una importante fuente de ingresos para la delincuencia organizada y, por tanto, constituyen un facilitador de otras actividades delictivas, como el terrorismo, el tráfico de drogas y la trata de seres humanos.

[74] COM(2017) 489.

También es necesario mejorar las capacidades de investigación de la ciberdelincuencia de los servicios policiales de los Estados miembros, así como la comprensión de la ciberdelincuencia y las opciones de investigación por parte de los fiscales y del poder judicial. Eurojust y Europol contribuyen a este objetivo y a una mayor coordinación, en estrecha colaboración con los grupos asesores especializados del Centro de Ciberdelincuencia de Europol y con las redes de jefes de las unidades de ciberdelincuencia y de fiscales especializados en esta. La Comisión dedicará 10,5 millones EUR a la financiación de la lucha contra la ciberdelincuencia en el marco del **Programa de fondos de la UE para las políticas de seguridad interior**. La formación es un elemento importante y el Grupo Europeo de Formación y Educación en Ciberdelincuencia ha preparado una serie de materiales útiles. En adelante, dichos materiales deberán distribuirse entre las fuerzas policiales con el apoyo de la Agencia de la Unión Europea para la Formación Policial (CEPOL).

3.3 Cooperación de los sectores público y privado contra la ciberdelincuencia

La eficacia de los mecanismos policiales tradicionales es cuestionada por las características del mundo digital, formado principalmente por infraestructuras de propiedad privada y numerosos actores diferentes en una gran variedad de jurisdicciones. Como resultado, la cooperación con el sector privado, incluidas la industria y la sociedad civil, es fundamental para que las autoridades públicas puedan luchar eficazmente contra la delincuencia. En este contexto, el sector financiero también es clave y se debe intensificar la cooperación con el mismo. Por ejemplo, debería reforzarse el papel de las unidades de información financiera[75] en el contexto de la ciberdelincuencia.

Algunos Estados miembros ya han adoptado medidas clave. En los Países Bajos, las instituciones financieras y los servicios policiales trabajan codo con codo para hacer frente al fraude en línea y la ciberdelincuencia en el Grupo de Trabajo sobre Delitos Electrónicos. El Centro de Competencia contra la Ciberdelincuencia de Alemania ofrece a sus miembros un centro operativo en el que intercambiar información, en estrecha colaboración con la Oficina de la Policía Federal alemana, y desarrollar medidas destinadas a garantizar la protección contra la ciberdelincuencia. Dieciséis Estados miembros[76] han creado centros de excelencia para delitos cibernéticos a fin de facilitar la cooperación entre los servicios policiales, el mundo académico y los socios privados para el desarrollo y el intercambio de buenas prácticas, métodos de capacitación y desarrollo de competencias.
La Comisión apoya el establecimiento de asociaciones público-privadas y mecanismos de cooperación a través de proyectos específicos, tales como el Cibercentro y la Red de Expertos en el Fraude en Línea[77], que aplican modelos y estándares de intercambio de información para analizar y atenuar los riesgos de delitos electrónicos y fraudes en línea.

En el contexto de la ciberdelincuencia, las empresas privadas deben poder compartir información sobre incidentes concretos con los servicios policiales, incluida la información

[75] Las unidades de información financiera funcionan como centros nacionales de recepción y análisis de informes sobre transacciones sospechosas y otra información relacionada con el lavado de dinero, los delitos subyacentes asociados y la financiación del terrorismo, además de la difusión de los resultados de dicho análisis.

[76] Austria, Bélgica, Bulgaria, Chipre, República Checa, Estonia, Francia, Alemania, Grecia, Irlanda, Lituania, Polonia, Rumanía, Eslovenia, España y Reino Unido.

[77] La iniciativa EU-OF2CEN tiene por objeto permitir el intercambio sistemático, a nivel de la UE, de información relacionada con el fraude en Internet entre los bancos y los servicios policiales para evitar los pagos a los estafadores y las «mulas de dinero», además de investigar y emprender acciones penales contra los responsables. Es una iniciativa cofinanciada por la UE (Programa de fondos de la UE para las políticas de seguridad interior).

personal, respetando plenamente las normas de protección de datos. La reforma de la protección de datos de la UE, que entrará en vigor en mayo de 2018, establece un conjunto común de normas que determinan las condiciones en las que los servicios policiales y las entidades privadas pueden cooperar. La Comisión Europea colaborará con la Junta Europea de Protección de Datos y con las partes interesadas pertinentes para determinar las mejores prácticas en este ámbito y, cuando proceda, proporcionar orientación.

3.4 Reforzar la respuesta política

El marco adoptado recientemente para una **respuesta diplomática conjunta de la UE a las actividades cibernéticas maliciosas**[78] (el «conjunto de instrumentos de la ciberdiplomacia») se servirá plenamente de las medidas previstas en la política exterior y de seguridad común, incluidas las medidas restrictivas, que pueden utilizarse para reforzar la respuesta de la UE a las actividades que perjudican sus intereses políticos, de seguridad y económicos. El marco constituye un paso importante en el desarrollo de las capacidades de señalización y reacción de la UE y de los Estados miembros. Aumentará nuestra capacidad para identificar actividades cibernéticas maliciosas, con el fin de influir en el comportamiento de los agresores potenciales, teniendo en cuenta la necesidad de garantizar respuestas proporcionadas. Su atribución a un agente estatal o no seguirá siendo una decisión política soberana basada en información procedente de todo tipo de fuentes. El marco se está aplicando junto con los Estados miembros y se llevará adelante en estrecha coordinación con el plan director para responder a los incidentes cibernéticos a gran escala[79]. El INTCEN[80] debería fusionar, analizar y compartir la sensibilización de la situación necesaria para el uso de las medidas dentro del marco, trabajando estrechamente con los Estados miembros y las instituciones de la UE.

3.5 Aumentar la disuasión de la ciberseguridad a través de la capacidad de defensa de los Estados miembros

Los Estados miembros ya están desarrollando capacidades de defensa cibernética. Asimismo, dada la falta de definición de la frontera entre ciberdefensa y ciberseguridad y el doble uso de las herramientas y tecnologías cibernéticas, así como las grandes diferencias entre los enfoques de los Estados miembros, la UE se encuentra bien situada para ayudar a promover sinergias entre los esfuerzos militares y civiles[81].

Los Estados miembros con capacidades de ciberseguridad más avanzadas y dispuestos a aunar esfuerzos podrían considerar, con el apoyo del Alto Representante, la Comisión y la Agencia Europea de Defensa, la posibilidad de incluir la ciberdefensa en el marco de una «cooperación estructurada permanente» (PESCO). Podría respaldarse con el trabajo expuesto anteriormente para fomentar las capacidades industriales y la autonomía estratégica de la UE. La UE también puede promover la interoperabilidad, incluso facilitando el desarrollo de capacidades, la coordinación de la formación y la educación y los esfuerzos de normalización del doble uso.

También debe aprovecharse plenamente el marco común para responder a las amenazas híbridas, que a menudo implican ciberataques, en particular a través de la célula de fusión de

---

78 http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

79 C(2017) 6100.

80 JOIN(2016) 018 final.

81 La UE equipara el ciberespacio a otros escenarios de operaciones como la tierra, el aire y el mar. Los esfuerzos en ciberdefensa también incluyen la protección y la resiliencia de activos espaciales y las infraestructuras terrestres relacionadas.

la UE contra las amenazas híbridas y el recientemente creado Centro Europeo para la Lucha contra las Amenazas Híbridas de Helsinki, cuya misión es fomentar el diálogo estratégico y realizar investigaciones y análisis.

La UE pondrá un énfasis renovado en el marco político de ciberdefensa de la UE de 2014[82], empleándolo como una herramienta para integrar aún más la ciberseguridad y la defensa en la política común de seguridad y defensa (PCSD). La ciberresiliencia de las misiones y operaciones de la PCSD es esencial: se desarrollarán procedimientos normalizados y capacidades técnicas que podrían servir de apoyo tanto para las misiones y operaciones civiles y militares desplegadas como para sus respectivas estructuras de Capacidad de Planificación y Ejecución y los proveedores de servicios de TI del SEAE. La Agencia Europea de Defensa y el SEAE, en colaboración con los servicios de la Comisión, facilitarán el compromiso estratégico entre los responsables políticos de los Estados miembros en materia de defensa cibernética a fin de promover la cooperación de los Estados miembros y orientar mejor las actividades de la UE en este ámbito. La UE también apoyará el desarrollo de soluciones europeas de ciberseguridad como parte de sus esfuerzos en favor de una base tecnológica e industrial de la defensa europea, incluido el fomento de las agrupaciones regionales de excelencia en ciberseguridad y defensa.

Los servicios de la Comisión, en estrecha colaboración con el SEAE, los Estados miembros y otros órganos pertinentes de la UE, pondrán en marcha para 2018 **una plataforma de formación y educación en materia de ciberdefensa** para solucionar la falta de profesionales competentes en este ámbito. Esta medida complementará el trabajo de la Agencia Europea de Defensa, ayudando a resolver el actual déficit de competencias en ciberseguridad y ciberdefensa.

Medidas clave

- Iniciativa de la Comisión para el acceso transfronterizo a pruebas electrónicas (a principios de 2018).
- Rápida adopción por el Parlamento Europeo y el Consejo de la propuesta de Directiva sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo.
- Introducción de requisitos para el IPv6 en la contratación, la investigación y la financiación de proyectos de la UE; acuerdos voluntarios entre los Estados miembros y los proveedores de servicios de Internet para impulsar la adopción del IPv6.
- Enfoque renovado/ampliado de Europol sobre la investigación forense cibernética y el control de la red oscura.
- Aplicación del marco para una respuesta diplomática conjunta de la UE a actividades cibernéticas maliciosas.
- Aumento del apoyo financiero a los proyectos nacionales y transnacionales que mejoren la justicia penal en el ciberespacio.
- Plataforma de educación relacionada con la ciberseguridad para reducir el actual déficit de competencias en ciberseguridad y ciberdefensa en 2018.

4. FORTALECIMIENTO DE LA COOPERACIÓN INTERNACIONAL EN MATERIA DE CIBERSEGURIDAD

Guiada por los valores y los derechos fundamentales de la UE, como la libertad de expresión, el derecho a la privacidad, la protección de los datos personales y la promoción de un ciberespacio abierto, libre y seguro, la política internacional de ciberseguridad de la UE

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

pretende hacer frente al desafío de promover la estabilidad cibernética mundial, así como de contribuir a la autonomía estratégica de Europa en el ciberespacio.

4.1 La ciberseguridad en las relaciones exteriores

Los datos señalan que los ciudadanos de todo el mundo identifican los ciberataques de otros países como una de las principales amenazas a la seguridad nacional[83]. Dada la naturaleza global de la amenaza, es fundamental crear y mantener fuertes alianzas y asociaciones con terceros países para prevenir y disuadir de la realización de ciberataques, cuyo papel es cada vez más relevante en la estabilidad y la seguridad internacionales. La UE dará prioridad al establecimiento de un marco estratégico para la prevención de conflictos y la estabilidad en el ciberespacio en sus compromisos bilaterales, regionales, múltiples y multilaterales.

La UE cree firmemente que el Derecho internacional, y en particular la Carta de las Naciones Unidas, es de aplicación en el ciberespacio. Como complemento del Derecho internacional vinculante, la UE respalda las normas voluntarias no vinculantes, las reglas y los principios de comportamiento responsable del Estado formulados por el Grupo de Expertos Gubernamentales de las Naciones Unidas[84], y alienta el desarrollo y la aplicación de medidas regionales de fomento de la confianza, tanto en la Organización para la Seguridad y la Cooperación en Europa como en otras regiones.

A nivel bilateral, se intensificarán los diálogos cibernéticos[85] y se complementarán con los esfuerzos destinados a facilitar la cooperación con terceros países para reforzar los principios de diligencia debida y responsabilidad del Estado en el ciberespacio. La UE dará prioridad a las cuestiones de seguridad internacional en el ciberespacio en sus compromisos internacionales, garantizando asimismo que la ciberseguridad no se convierta en un pretexto para la protección del mercado y la limitación de los derechos y las libertades fundamentales, incluida la libertad de expresión y el acceso a la información. Un enfoque integral de la ciberseguridad exige el respeto de los derechos humanos, por lo que la UE seguirá manteniendo sus valores fundamentales a nivel mundial, tomando como base las Directrices de la UE sobre derechos humanos relativas a la libertad de expresión en Internet[86]. A este respecto, la UE hace hincapié en la importancia de la participación de todas las partes interesadas en la gobernanza de Internet.

La Comisión ha presentado también una propuesta[87] de modernización de los controles de las exportaciones de la UE, incluida la introducción de controles de las exportaciones de tecnologías críticas de vigilancia cibernética que puedan causar violaciones de los derechos humanos o ser utilizadas indebidamente contra la propia seguridad de la UE, y abrirá un diálogo con terceros países para promover la convergencia mundial y un comportamiento responsable en este ámbito.

4.2 Capacitación en ciberseguridad

La estabilidad cibernética mundial depende de la capacidad local y nacional de todos los países para prevenir y reaccionar frente a los incidentes cibernéticos e investigar y emprender

---

83 Spring 2017 Global Attitudes Survey («Encuesta de actitudes globales, primavera de 2017»), Pew Research Centre.

84 A/68/98 y A/70/174.

85 En septiembre de 2017, la UE mantuvo diálogos cibernéticos con Estados Unidos, China, Japón, la República de Corea y la India.

86 Directrices de la Unión Europea sobre derechos humanos relativas a la libertad de expresión en Internet y fuera de Internet.

87 COM(2016) 616.

acciones penales en los casos de ciberdelincuencia. Apoyar los esfuerzos para aumentar la resiliencia nacional en los terceros países incrementará el nivel de ciberseguridad en todo el mundo, con consecuencias positivas para la UE. La lucha contra las amenazas cibernéticas de rápida evolución apunta a la necesidad de formación, desarrollo de políticas y legislación, así como de equipos de respuesta a emergencias informáticas y unidades de ciberdelincuencia eficaces en todos los países del mundo.

Desde 2013, la UE ha liderado el fomento de la capacidad internacional en materia de ciberseguridad y ha vinculado sistemáticamente estos esfuerzos con su cooperación al desarrollo. La UE seguirá promoviendo un modelo de creación de capacidad basado en los derechos, en consonancia con el enfoque de desarrollo Digital4Development[88]. Las prioridades para la creación de capacidad serán los países vecinos y en desarrollo de la UE que experimenten una creciente conectividad y un rápido crecimiento de las amenazas. Los esfuerzos de la UE serán un complemento al programa de desarrollo de la UE a la luz de la Agenda para el Desarrollo Sostenible de 2030 y de los esfuerzos generales para el desarrollo de capacidad institucional.

Con el fin de mejorar la competencia de la UE para movilizar su experiencia colectiva en apoyo de la creación de capacidad, debería crearse una red dedicada al desarrollo de las competencias cibernéticas de la UE, que reúna al SEAE, las autoridades cibernéticas de los Estados miembros, las agencias de la UE y la sociedad civil. Se elaborarán directrices para el desarrollo de la capacidad cibernética de la UE con el fin de mejorar la orientación política y la priorización de los esfuerzos de la UE para ayudar a los terceros países.

La UE colaborará también con otros donantes en este ámbito a fin de evitar la duplicación de esfuerzos y facilitar el desarrollo de capacidades más específicas en las distintas regiones.

4.3 Cooperación UE-OTAN

Tomando como base los progresos sustanciales ya alcanzados, la UE profundizará en su cooperación con la OTAN en materia de ciberseguridad, amenazas híbridas y defensa, tal como se prevé en la Declaración Conjunta de 8 de julio de 2016[89]. Las prioridades incluyen fomentar la interoperabilidad mediante requisitos y normas coherentes de defensa cibernética, reforzar la cooperación en el ámbito de la formación y los ejercicios, y armonizar los requisitos de formación.

La UE y la OTAN también fomentarán la cooperación en materia de investigación e innovación en el ámbito de la ciberseguridad y se basarán en el actual acuerdo técnico sobre el intercambio de información en materia de ciberseguridad entre sus respectivos órganos de ciberseguridad[90]. Los recientes esfuerzos conjuntos para contrarrestar las amenazas híbridas, en particular la cooperación entre la célula de fusión de la UE contra las amenazas híbridas y la sección de análisis híbrido de la OTAN, deberían aprovecharse aún más para fortalecer la resiliencia y la respuesta a las crisis cibernéticas. Se fomentará una mayor cooperación entre la UE y la OTAN mediante ejercicios de defensa cibernética, con la participación del SEAE y otras entidades de la UE y sus homólogos de la OTAN, incluido el Centro de Excelencia de Cooperación en Ciberdefensa de la OTAN, situado en Tallin. Por primera vez, la OTAN y la UE llevarán a cabo ejercicios paralelos y coordinados en respuesta a un escenario híbrido en el que la OTAN asumirá el liderazgo en 2017, a lo que la UE corresponderá de manera similar en 2018. El próximo informe sobre la cooperación entre la UE y la OTAN, que se presentará a

[88] SWD(2017) 157.
[89] http://www.consilium.europa.eu/es/press/press-releases/2016/07/08-eu-nato-joint-declaration/.
[90] Capacidad de respuesta a incidentes informáticos, CERT-UE y OTAN (NCIRC).

sus respectivos Consejos en diciembre de 2017, ofrecerá la oportunidad de estudiar las posibilidades de seguir ampliando esta cooperación, en particular garantizando medios de comunicación comunes, seguros y sólidos entre todas las instituciones y órganos competentes, incluida ENISA.

Medidas clave

- Impulso del marco estratégico para la prevención de conflictos y la estabilidad en el ciberespacio.
- Desarrollo de una nueva red de creación de capacidad en los terceros países para hacer frente a las amenazas cibernéticas, así como de las directrices de la UE para crear capacidad en materia de ciberseguridad a fin de dar prioridad a los esfuerzos de la UE.
- Mayor cooperación entre la UE y la OTAN, incluida la participación en ejercicios paralelos y coordinados y una mayor interoperabilidad de las normas de ciberseguridad.

5. CONCLUSIÓN

La preparación cibernética de la UE es fundamental, tanto para el Mercado Único Digital como para la Unión de Seguridad y Defensa. Es imprescindible mejorar la ciberseguridad europea y hacer frente a las amenazas contra objetivos civiles y militares.

La próxima Cumbre Digital, organizada por la Presidencia estonia el 29 de septiembre de 2017, ofrece la oportunidad de mostrar una voluntad común de situar la ciberseguridad como prioridad de la UE en tanto que sociedad digital. Como parte de este esfuerzo común, la Comisión solicita a los Estados miembros que garanticen sus formas de actuación en ámbitos de los que son los principales responsables. Esto incluiría el fortalecimiento de la ciberseguridad, para lo cual se debe:

- Garantizar la aplicación plena y efectiva de la Directiva SRI antes del 9 de mayo de 2018, así como la dotación de los recursos necesarios para que las autoridades públicas responsables de la ciberseguridad puedan desempeñar eficazmente sus tareas.
- Aplicar las mismas reglas a las administraciones públicas, dada la función que desempeñan en la sociedad y en la economía en su conjunto.
- Ofrecer formación relacionada con la ciberseguridad en la administración pública.
- Dar prioridad a la concienciación cibernética en las campañas de información e incluir la ciberseguridad como parte de los planes de estudios académicos y de formación profesional.
- Aprovechar las iniciativas de la «cooperación estructurada permanente» (PESCO) y el Fondo Europeo de Defensa para apoyar el desarrollo de proyectos de ciberdefensa.

La presente Comunicación conjunta ha establecido la magnitud del reto y la gama de medidas que puede adoptar la UE. Necesitamos una Europa resiliente, que pueda proteger eficazmente a sus ciudadanos anticipándose a posibles incidentes de ciberseguridad, protegiendo sólidamente sus estructuras y funcionamiento, recuperándose rápidamente de cualquier ciberataque y disuadiendo a sus responsables. Esta Comunicación presenta medidas selectivas que reforzarán las estructuras y capacidades de ciberseguridad de la UE de manera coordinada, con la plena colaboración de los Estados miembros y de las diferentes estructuras de la UE interesadas, y que respetan sus competencias y responsabilidades. Su aplicación ofrecerá una clara demostración de que la UE y los Estados miembros colaboran para establecer un estándar de ciberseguridad que esté a la altura de los retos cada vez mayores a los que se enfrenta Europa en la actualidad.