COMISIÓN
EUROPEA

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

Bruselas, 6.8.2021
JOIN(2021) 14 final/2

CORRIGENDUM
This document corrects document JOIN(2021) 14 final of 23.6.2021
Concerns all language versions.
Removal of the institutional reference 2021/0166 (NLE).
The text shall read as follows:

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO

Informe sobre la ejecución de la Estrategia de Ciberseguridad de la Unión Europea para la Década Digital

COMUNICACIÓN CONJUNTA AL PARLAMENTO EUROPEO Y AL CONSEJO

Informe sobre la ejecución de la Estrategia de Ciberseguridad de la Unión Europea para la Década Digital

I. La ciberresiliencia, la capacidad operativa y la apertura son más esenciales que nunca

La ciberseguridad es esencial para el despliegue de tecnologías más inteligentes y ecológicas en el mundo posterior a la pandemia. En términos generales, es indispensable para la seguridad de la Unión Europea (UE) y constituye uno de los pilares de la Unión de la Seguridad. Para lograr el desarrollo social, político y económico, es necesario que haya soberanía tecnológica y contar con un ciberespacio mundial, abierto y seguro cimentado sobre el Estado de Derecho y el respeto de los derechos humanos y las libertades fundamentales. Esta fue la premisa esencial de la Comunicación conjunta de la Comisión y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad sobre la Estrategia de Ciberseguridad de la UE para la Década Digital, adoptada el 16 de diciembre de 2020[1]. Todas las entidades críticas pueden ser objeto de ciberataques. Los acontecimientos de los últimos seis meses han justificado que la estrategia centre su atención en la intensificación de las reformas normativas, en la inversión y en la respuesta operativa colectiva.

Los ciberataques ocurridos recientemente han demostrado, en particular, que los programas de secuestro y las operaciones de ciberespionaje cada vez están más generalizados y entrañan un riesgo creciente para todos los sectores de la economía y la sociedad en su conjunto. La magnitud de los incidentes ha sido extraordinaria: los ataques a Microsoft Exchange afectaron a cientos de miles de servidores; la campaña contra la plataforma Orion de SolarWinds pudo afectar a 18 000 organizaciones; el ataque con programas de secuestro perpetrado contra el Servicio de Salud de Irlanda tuvo como consecuencia el robo de datos sensibles de cientos de pacientes y la interrupción de los servicios médicos; el ciberataque al sistema de facturación de Colonial Pipeline provocó una emergencia en el suministro de combustible y el robo masivo de datos; y se interrumpieron las operaciones del mayor proveedor de carne de vacuno del mundo[2]. Si bien se desconoce la magnitud real de los daños, cada incidente pone de relieve que la explotación malintencionada de las vulnerabilidades de los productos, servicios, sistemas y redes de las tecnologías de la información y de las comunicaciones puede tener consecuencias de gran alcance. Cabe esperar que estos ciberataques aumenten en términos de impacto y frecuencia, y socaven nuestra seguridad.

En consecuencia, resulta esencial que la Unión Europea acelere el avance en todos los frentes —legislativo, operativo, diplomático y en relación con las inversiones—, tal y como prevé la Estrategia. Es preciso aprobar cuanto antes las propuestas de una Directiva relativa a las medidas destinadas a

[1] Comunicación conjunta al Parlamento Europeo y al Consejo, «La Estrategia de Ciberseguridad de la UE para la Década Digital» [JOIN(2020) 18 final].

[2] SolarWinds, una importante empresa de tecnología de la información de los Estados Unidos, sufrió en 2020 un ciberataque que se extendió a sus clientes y no se detectó hasta meses después. Con él, los piratas informáticos tuvieron acceso a miles de empresas y oficinas gubernamentales que utilizaban su plataforma Orion, incluidos seis instituciones, organismos y agencias de la UE. Desde enero de 2021, se detectaron múltiples ataques de día cero contra Microsoft Exchange Server que afectaron a sistemas de correo electrónico de todo el mundo. En mayo, el Servicio de Salud de la República de Irlanda sufrió un ataque que tuvo un impacto considerable en la continuidad de los servicios. Colonial Pipeline, el mayor operador de oleoductos de los Estados Unidos, tuvo que detener sus operaciones el 7 de mayo tras descubrir un fallo de seguridad debido a un ciberataque que había afectado a sus principales sistemas informáticos. Por último, JBS USA Holdings Inc., la sucursal estadounidense del mayor proveedor cárnico del mundo en términos de ventas, sufrió en junio de 2021 un ataque con un programa de secuestro que provocó graves interrupciones en sus operaciones.

garantizar un elevado nivel común de ciberseguridad en toda la Unión (la «Directiva SRI 2»)[3], de una Directiva relativa a la resiliencia de las entidades críticas[4], así como de un Reglamento y una Directiva sobre la resiliencia operativa digital[5]. En este contexto, resulta esencial adoptar un enfoque ambicioso, principalmente en lo que respecta a las cadenas de suministro, en vista de que en los ciberataques recientes se determinó que las vulnerabilidades procedían de los proveedores de *software*, y tomar medidas encaminadas a garantizar la resiliencia de las administraciones públicas y la notificación rápida de incidentes. La necesidad de establecer una red de centros de operaciones de seguridad (COS) para la detección temprana de señales de ciberataques es más acuciante que nunca, como también lo es la necesidad de desarrollar una respuesta a escala de la UE creíble, efectiva y colectiva, también a nivel operativo, frente a los incidentes graves por medio de la unidad informática conjunta[6]. Debido al aumento de los ciberataques cometidos por agentes estatales o patrocinados por los Estados, es preciso seguir promoviendo que los Estados se comporten de forma responsable en las Naciones Unidas y mediante ciberdiálogos e intercambios estructurados con organizaciones regionales, tales como la Unión Africana, el Foro Regional de la ASEAN, la Organización de los Estados Americanos (OEA) y la Organización para la Seguridad y la Cooperación en Europa (OSCE), al tiempo que se emprenden acciones diplomáticas efectivas destinadas a prevenir, desalentar, disuadir y contrarrestar los comportamientos maliciosos en el ciberespacio. La cooperación con terceros países afines y las prioridades de la agenda transatlántica serán especialmente importantes. En concreto, conviene seguir explorando la cooperación entre la UE y los Estados Unidos en aspectos específicos de la ciberseguridad, tales como el intercambio de información y la lucha contra los programas de secuestro.

II. Visión general de los primeros seis meses de ejecución

Varias acciones estratégicas ya están muy avanzadas.

II.1 Resiliencia, soberanía tecnológica y liderazgo

En todo el mundo, las cadenas de suministros e infraestructuras críticas, como los hospitales que luchan contra la pandemia de COVID-19, se encuentran en un riesgo constante de sufrir ciberataques. La Comisión está prestando asistencia a los colegisladores con miras a garantizar la adopción rápida de la reforma de la Directiva SRI propuesta, que, en concreto, ampliará la cobertura del sector sanitario para incluir a los laboratorios de investigación y la fabricación de productos sanitarios esenciales y medicamentos, así como nuevas actividades del sector energético, tales como la producción de hidrógeno, los sistemas urbanos de calefacción, la producción de electricidad y el almacenamiento central de crudo.

El Reglamento por el que se establecen el Centro de Competencia en Ciberseguridad y la Red de Centros Nacionales de Coordinación fue adoptado el 20 de mayo de 2021[7]. Aunará los recursos de la UE, los Estados miembros y la industria con vistas a mejorar y fortalecer las capacidades tecnológicas e industriales en materia de ciberseguridad, con lo que incrementará la autonomía estratégica abierta de la Unión y brindará la posibilidad de consolidar parte de las actividades relacionadas con la

[3] Propuesta de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad y por la que se deroga la Directiva (UE) 2016/1148 [COM(2020) 823 final].
[4] Propuesta de Directiva relativa a la resiliencia de las entidades críticas [COM(2020) 829 final].
[5] Propuesta de Reglamento sobre la resiliencia operativa digital del sector financiero y por el que se modifican los Reglamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 y (UE) n.º 909/2014 [COM(2020) 595 final]; Propuesta de Directiva por la que se modifican las Directivas 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, 2013/36/UE, 2014/65/UE, (UE) 2015/2366 y (UE) 2016/2341 [COM(2020) 596 final].
[6] [Recomendación de la unidad informática conjunta].
[7] Reglamento (UE) 2021/887 del Parlamento Europeo y del Consejo, de 20 de mayo de 2021, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación.

ciberseguridad financiadas en el marco de Horizonte Europa, el programa Europa Digital y el Mecanismo de Recuperación y Resiliencia, y en total recibirá 4 500 millones EUR de financiación en los próximos seis años[8]. De este modo, favorecerá el desarrollo de aquí a 2023 de un escudo cibernético europeo para la detección temprana de los ciberataques, el cual estará compuesto por una red de centros de operaciones de seguridad que podrán ser públicos o privados y se servirán de herramientas basadas en inteligencia artificial. Varios Estados miembros han incluido el desarrollo de dichos centros nacionales en sus respectivos planes de recuperación y resiliencia. La Comisión complementará estos esfuerzos con financiación del programa Europa Digital y apoyará su conexión gradual. Los programas financieros también respaldarán la iniciativa EuroQCI de crear una infraestructura de comunicación cuántica segura que abarque toda la UE[9], incluidos sus territorios de ultramar, utilizando la mejor combinación posible de tecnologías terrestres y espaciales, y una línea presupuestaria específica destinada a fortalecer la ciberresiliencia en el sector de la salud.

Garantizar la ciberseguridad 5G es un proceso continuo que se desarrollará en paralelo a la implantación de la 5G y del conjunto de instrumentos de la UE para la seguridad de las redes 5G[10]. La mayoría de los Estados miembros ya han establecido —o lo harán en breve— marcos para imponer las restricciones oportunas a los proveedores de 5G. Se están reforzando los requisitos aplicables a los operadores de redes móviles mediante la transposición del Código Europeo de las Comunicaciones Electrónicas, y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) está preparando una propuesta de esquema europeo de certificación de la ciberseguridad para las redes de 5G[11]. En vista de las nuevas tendencias y de los avances en la cadena de suministro de la 5G, las autoridades de los Estados miembros han decidido iniciar un análisis exhaustivo de las implicaciones para la seguridad que tienen las soluciones de tecnología en red abiertas, desagregadas e interoperables («Open RAN») en el marco del conjunto de instrumentos de la UE. El resultado de esta labor contribuirá en mayor medida al enfoque concertado de la UE para la ciberseguridad 5G.

Es necesario redoblar los esfuerzos, en especial por medio del Plan de Acción de Educación Digital de la UE, para subsanar la enorme escasez de personal cualificado prevista, a fin de cubrir de aquí a 2022 los casi dos millones de puestos de ciberseguridad sin ocupar en todo el mundo, de los cuales 350 000 se encuentran en Europa, y la grave infrarrepresentación de las mujeres, que únicamente representan el 11 % del personal de ciberseguridad a escala mundial y un porcentaje todavía inferior (el 7 %) en Europa[12]. También se están llevando a cabo otras iniciativas políticas, como los trabajos de preparación de futuras iniciativas para la seguridad de la internet de las cosas y, en lo que respecta a las normas aplicables a internet, el desarrollo de un servicio de resolución de nombres de dominio no lucrativo («DNS4EU»).

[8] El Centro de Competencia en Ciberseguridad desempeñará estas funciones, en concreto, tomando decisiones sobre los fondos para ciberseguridad procedentes del programa Europa Digital, Horizonte Europa y los Estados miembros, que se encargará de gestionar.

[9] https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network.

[10] Informe, de 16 de diciembre de 2020, sobre las repercusiones de la Recomendación de la Comisión de 26 de marzo de 2019 sobre la ciberseguridad de las redes 5G [SWD(2020) 357 final].

[11] La preparación del esquema cuenta con el apoyo del Grupo de Cooperación SRI y es conforme al artículo 48 del Reglamento sobre la Ciberseguridad; Reglamento (UE) 2019/881, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.º 526/2013. https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-commission-requests-eu-cybersecurity-agency-develop-certification.

[12] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_es.

II.2 Desarrollo de la capacidad operativa para prevenir, disuadir y contrarrestar

Debido al auge de los ataques estatales, patrocinados por Estados, y delictivos contra redes y sistemas de información, así como a la dependencia cada vez mayor de bases de datos sensibles, la UE necesita que las comunidades cibernéticas estén más interconectadas. Estas deben responder de forma coherente a los aspectos civiles, penales, diplomáticos y de defensa asociados a los ciberataques a gran escala que han sufrido recientemente muchos sectores económicos sensibles. Por consiguiente, es necesario que todas las comunidades se esfuercen por completar los cuatro pasos contemplados en la Recomendación de la Comisión sobre la creación de la unidad informática conjunta, adoptada en paralelo al presente informe, como mecanismo para intensificar la coordinación y colmar las lagunas en la respuesta de la Unión a las ciberamenazas[13]. En el contexto de la lucha contra la ciberdelincuencia, se alcanzó un acuerdo político para la regulación temporal de los abusos sexuales de menores en línea, que se aprobará próximamente[14], y la nueva Estrategia de la UE contra la Delincuencia Organizada[15] se centra en la necesidad de dotar a los cuerpos de seguridad de las herramientas digitales que necesitan. Asimismo, la Comisión adoptó en febrero de 2020 el Plan de Acción sobre las sinergias entre las industrias civil, de la defensa y espacial, el cual define un nuevo proyecto emblemático para el establecimiento de un sistema global de conectividad segura de la UE basado en el espacio. Su objetivo es facilitar «el acceso generalizado a conectividad de alta velocidad en Europa» y proporcionar «un sistema de conectividad resiliente que permitirá a Europa mantenerse conectada en cualquier circunstancia»[16].

Desde el punto de vista internacional, y en consonancia con la ambición definida en la brújula estratégica[17], el Alto Representante está preparando la revisión del marco político de ciberdefensa que se presentará a los Estados miembros en el segundo semestre de 2021. El Alto Representante ha trabajado para mejorar la capacidad de la UE para prevenir, desalentar, disuadir y contrarrestar las actividades cibernéticas maliciosas, entre otras cosas mediante el fortalecimiento de la cooperación internacional. El 17 de mayo de 2021, el Servicio Europeo de Acción Exterior (SEAE), en cooperación con la Presidencia portuguesa y el Instituto de Estudios de Seguridad de la Unión Europea (IESUE), organizó un debate basado en escenarios con los Estados miembros de la UE y socios internacionales orientado a mejorar la comprensión mutua de los respectivos planteamientos diplomáticos para prevenir, desalentar, disuadir y contrarrestar las actividades cibernéticas malintencionadas y a encontrar oportunidades para reforzar en mayor medida la cooperación internacional a tal fin[18]. Con el objetivo de seguir fortaleciendo el conjunto de instrumentos de ciberdiplomacia de la Unión, el SEAE está recopilando las lecciones aprendidas y podría revisar las directrices para la aplicación del marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas.

Como se anunció en la Estrategia de Ciberseguridad de la UE para la Década Digital, la Comisión está poniendo en marcha un estudio para desarrollar herramientas de concienciación destinadas a mejorar la preparación y la resiliencia de las empresas de la UE contra el robo de propiedad

[13] [La unidad informática conjunta permitiría responder de forma coordinada a las crisis y los incidentes cibernéticos a gran escala, recuperarse de ellos y ayudar a asegurar la movilización de recursos con fines de asistencia. Estaría integrada por expertos de distintas comunidades de ciberseguridad, cuyo propósito sería generar un conocimiento compartido de la situación y garantizar la preparación necesaria. Del mismo modo, coordinaría los mecanismos de asistencia a petición de uno o varios Estados miembros.]

[14] https://www.europarl.europa.eu/news/es/press-room/20210430IPR03213/provisional-agreement-on-temporary-rules-to-detect-and-remove-online-child-abuse.

[15] Estrategia contra la Delincuencia Organizada 2021-2025 [COM(2021) 170 de 14.4.2021].

[16] COM (2021) 70 de 22.2.2021.

[17] Conclusiones del Consejo sobre seguridad y defensa, de 17 de junio de 2020 (8910/20).

[18] https://eeas.europa.eu/headquarters/headquarters-homepage/98588/cyberspace-strengthening-cooperation-promoting-security-and-stability_en.

intelectual por medios cibernéticos[19]. Asimismo, la Comisión intensificó las acciones coercitivas relacionadas con la Directiva 2013/40/UE, relativa a los ataques contra los sistemas de información, al iniciar en junio de 2021 procedimientos por incumplimiento adicionales contra varios Estados miembros[20]. La Comisión se planteará adoptar medidas adicionales según sea necesario. También será esencial mejorar la disponibilidad de capacidades en materia de ciberseguridad en la mano de obra de la UE. En este sentido, el Centro de Competencia en Ciberseguridad emprenderá acciones clave con el objetivo de mejorar sus conocimientos y capacidades y fomentar el desarrollo de habilidades interdisciplinarias en el ámbito de la ciberseguridad.

II.3 Fomentar un ciberespacio mundial y abierto

El panorama de amenazas se ve agravado por las tensiones geopolíticas en torno a la internet mundial y abierta y a las tecnologías en toda la cadena de suministro. Las restricciones de internet y sobre su uso, el aumento de las actividades cibernéticas malintencionadas y de aquellas que afectan a la seguridad y la integridad de los productos y servicios de tecnología de la información y de las comunicaciones constituyen una amenaza para el ciberespacio mundial y abierto, así como para el Estado de Derecho, los derechos humanos, las libertades fundamentales y los valores democráticos. En consecuencia, el Alto Representante está trabajando, en colaboración con los Estados miembros, para promover un comportamiento responsable de los Estados en el ciberespacio, fundamentalmente mediante el establecimiento de un Programa de acción para avanzar en la actuación responsable de los Estados en el ciberespacio en las Naciones Unidas, junto con los otros cincuenta y tres copatrocinadores, sobre la base de la recomendación formulada en el informe aprobado por consenso el 12 de marzo de 2021 por el Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional[21]. La UE se está dedicando a consolidar y ampliar las relaciones con terceros países, organizaciones internacionales y regionales y la comunidad de múltiples partes interesadas mediante ciberdiálogos, conforme a lo previsto en la estrategia, con la creación de una Red de Ciberdiplomacia informal de la UE. También se está creando el Consejo para el Desarrollo de la Capacidad Cibernética de la UE[22], con el que los organismos, las instituciones y las agencias de la Unión podrán coordinarse y cooperar mejor en las iniciativas de desarrollo de la capacidad cibernética exterior de la UE.

En el marco de las Naciones Unidas, el 26 de mayo de 2021, la Asamblea General aprobó las modalidades de trabajo del comité especial establecido con la Resolución 74/247 sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos[23]. Las modalidades finalmente aprobadas incluyen elementos importantes para garantizar que los procesos decisorios sean inclusivos y que la sociedad civil participe en mayor medida en las labores del comité especial. La primera sesión de negociación del proceso que dará lugar a un nuevo convenio de las Naciones Unidas tendrá lugar en Nueva York en enero de 2022.

En la sesión plenaria de 28 de mayo de 2021 del Comité de Estados Partes en el Convenio de Budapest sobre la Ciberdelincuencia del Consejo de Europa, los Estados partes finalizaron los debates y adoptaron un borrador del Segundo Protocolo Adicional al Convenio[24], que debe impulsar la cooperación en materia de ciberdelincuencia y pruebas electrónicas en las investigaciones penales. La

[19] COM(2020) 760 de 25.11.2020.
[20] Los Estados miembros en cuestión son Bélgica, Chequia, Estonia, Luxemburgo, Austria, Polonia y Suecia.
[21] https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.
[22] https://www.eucybernet.eu/.
[23] https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html.
[24] https://rm.coe.int/0900001680a2aa42.

Comisión participó en los debates en representación de la UE[25]. Este proceso debería sentar las bases para poner fin de manera oficial a las negociaciones durante el segundo semestre de 2021 y para posteriormente abrir para su firma el Segundo Protocolo Adicional a comienzos de 2022.

La UE y sus socios reiteraron en junio de 2021 su determinación de colaborar para abordar la apremiante y creciente amenaza que entrañan las redes delictivas de programas de secuestro que ponen en riesgo a nuestros ciudadanos y empresas; de fomentar un acuerdo común sobre cómo se aplica el Derecho internacional en vigor al ciberespacio y promover este enfoque en las Naciones Unidas y otros foros internacionales, instando a todos los Estados a que detecten y desmantelen con carácter urgente las redes delictivas de programas de secuestro que operan desde sus territorios; y de hacer que dichas redes rindan cuentas por sus acciones[26].

II.4 La ciberseguridad en las instituciones, agencias y organismos europeos

La UE está en proceso de mejorar las normas en materia de ciberseguridad y seguridad de la información en sus instituciones, agencias y organismos. La Comisión está celebrando consultas con las partes interesadas y estudiando las políticas actuales con miras a aprobar propuestas antes de que termine 2021.

III. Antecedentes

El 16 de diciembre de 2020, la Comisión y el Alto Representante adoptaron la Estrategia de Ciberseguridad de la UE, en la que se establecen prioridades y acciones clave para mejorar la resiliencia, la autonomía, el liderazgo y la capacidad operativa de Europa ante las crecientes y complejas amenazas a las que se enfrentan sus redes y sistemas de información, así como para promover un ciberespacio mundial y abierto y alianzas internacionales en este. La Comisión y el Alto Representante se comprometieron a hacer un seguimiento de los avances en la ejecución de la estrategia.

El Consejo Europeo, en su declaración de 26 de febrero de 2021, invitó a la Comisión y el Alto Representante a que presentasen un informe sobre la ejecución de la estrategia en junio de 2021 como tarde[27]. El Consejo, en sus conclusiones adoptadas el 9 de marzo de 2021, celebró la estrategia y puso de relieve que la ciberseguridad es esencial para construir una Europa resiliente, ecológica y digital, al tiempo que animó a la Comisión y el Alto Representante a que establezcan un plan de ejecución detallado donde figuren las prioridades y el calendario de las acciones previstas[28]. La Estrategia está siendo estudiada por los comités pertinentes del Parlamento Europeo que, entre otras cosas, están centrando la atención en el riesgo de fragmentación de la regulación y en la oportunidad de fortalecer la industria europea a medida que se digitaliza[29]. El Comité Económico y Social Europeo adoptó el 27

[25] El Segundo Protocolo Adicional del Convenio de Budapest sobre la Ciberdelincuencia incluye medidas y salvaguardias destinadas a mejorar la cooperación internacional entre los cuerpos de seguridad y las autoridades judiciales, así como entre las autoridades y los proveedores de servicios de otros países, para lo cual la Comisión participa en las negociaciones en representación de la UE; Decisión del Consejo de junio de 2019 (ref. 9116/19).
[26] Declaración de la Cumbre UE-EE. UU., 15 de junio de 2021; https://www.consilium.europa.eu/media/50758/eu-us-summit-joint-statement-15-june-final-final.pdf.
Comunicado de la Cumbre del G7 en la bahía de Carbis: *Our Shared Agenda for Global Action to Build Back Better* [«Nuestra agenda común para emprender acciones globales para reconstruir a mejor»], 13 de junio de 2021; https://www.consilium.europa.eu/media/50361/carbis-bay-g7-summit-communique.pdf.
[27] https://www.consilium.europa.eu/media/48649/2526-02-21-euco-statement-es.pdf.
[28] https://www.consilium.europa.eu/es/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/.
[29] 2021/2568(RSP).

de abril un Dictamen que acogía con beneplácito la estrategia como un paso positivo para protegerse frente a las ciberamenazas mundiales y para salvaguardar el crecimiento económico[30].

El presente informe responde a los avances mencionados y, en particular, a la invitación del Consejo Europeo.

[30] https://www.eesc.europa.eu/es/our-work/opinions-information-reports/opinions/communication-cybersecurity-strategy.