Consejo de la Unión Europea

Bruselas, 23 de mayo de 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	23 de mayo de 2022
A:	Delegaciones
Asunto:	Conclusiones del Consejo sobre la elaboración de la posición de la Unión Europea en materia cibernética - Conclusiones del Consejo aprobadas por el Consejo en su sesión del 23 de mayo de 2022

Adjunto se remite a las delegaciones las Conclusiones del Consejo sobre la elaboración de la posición de la Unión Europea en materia cibernética, aprobadas por el Consejo en su sesión del 23 de mayo de 2022.

ANEXO

Conclusiones del Consejo sobre la elaboración de la posición de la Unión Europea en materia cibernética

EL CONSEJO DE LA UNIÓN EUROPEA,

RECORDANDO sus Conclusiones sobre:

– la Comunicación conjunta de 25 de junio de 2013 al Parlamento Europeo y al Consejo sobre la Estrategia de Ciberseguridad de la Unión Europea: «Un ciberespacio abierto, protegido y seguro»[1],

– el marco político de ciberdefensa de la UE[2],

– la gobernanza de internet[3],

– la ciberdiplomacia[4],

– reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora[5],

– la Comunicación conjunta de 20 de noviembre de 2017 al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE»[6],

– un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»)[7],

– la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala[8],

– las directrices para el desarrollo de la capacidad cibernética exterior de la UE[9],

---

1 12109/13.
2 15585/14.
3 16200/14.
4 6122/15 + COR 1.
5 14540/16.
6 14435/17 + COR 1.
7 10474/17.
8 10086/18.
9 10496/18.

– la Decisión de Ejecución (UE) 2018/1993 del Consejo, de 11 de diciembre de 2018, sobre el Dispositivo de la UE de Respuesta Política Integrada a las Crisis[10],

– el desarrollo de capacidades y competencias en materia de ciberseguridad en la UE[11],

– la importancia de la tecnología 5G para la economía europea y la necesidad de mitigar los riesgos para la seguridad relacionados con la 5G[12],

– el futuro de una Europa altamente digitalizada más allá de 2020: «Impulsar la competitividad digital y económica en toda la Unión y la cohesión digital»[13],

– las acciones complementarias para aumentar la resiliencia y luchar contra las amenazas híbridas[14],

– la configuración del futuro digital de Europa[15],

– la ciberseguridad de los dispositivos conectados[16],

– la Estrategia de Ciberseguridad de la UE para la Década Digital[17],

– seguridad y defensa[18],

– la exploración del potencial de la iniciativa relativa a una Unidad Cibernética Conjunta como complemento de la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala[19],

– una Brújula Estratégica para la Seguridad y la Defensa – Por una Unión Europea que proteja a sus ciudadanos, defienda sus valores e intereses y contribuya a la paz y la seguridad internacionales[20],

---

10 DO L 320 de 17.12.2018, p. 28.
11 7737/19.
12 14517/19.
13 9596/19.
14 14972/19.
15 8711/20.
16 13629/20.
17 7290/21.
18 8396/21.
19 13048/21.
20 7371/22.

1. HACE HINCAPIÉ en que la conducta malintencionada en el ciberespacio, con origen tanto en agentes estatales como no estatales, se ha intensificado en los últimos años; en particular, se ha producido un acusado y constante aumento de las actividades malintencionadas dirigidas contra las infraestructuras críticas, las cadenas de suministro y la propiedad intelectual de la UE y sus Estados miembros, se ha incrementado el riesgo de efectos indirectos y han aumentado también los ataques con programas de secuestro contra nuestras empresas, organizaciones y ciudadanos. OBSERVA que, con el retorno de la política basada en las relaciones de poder, algunos países intentan cada vez más cuestionar y socavar el orden internacional basado en normas en el ciberespacio, por lo que el ciberespacio se está convirtiendo en un ámbito cada vez más disputado, al igual que la alta mar, el espacio aéreo y el espacio ultraterrestre. RECONOCE que los ciberataques a gran escala o los intentos de invadir, perturbar o destruir las redes y los sistemas de información con efectos sistémicos son ahora más frecuentes, podrían socavar nuestra seguridad económica y afectar a nuestras instituciones y procesos democráticos y muestran la voluntad de algunos agentes de poner en peligro la seguridad y la estabilidad internacionales. SUBRAYA que la agresión militar de Rusia contra Ucrania ha puesto de manifiesto que es posible realizar actividades cibernéticas ofensivas como parte de estrategias híbridas que combinan intimidación, desestabilización y perturbaciones económicas.

2. REITERA que, ante los actuales cambios geopolíticos, la fuerza de nuestra Unión reside en la unidad, la solidaridad y la determinación, y que la aplicación de la Brújula Estratégica reforzará la autonomía estratégica de la UE y su capacidad para trabajar con sus socios a fin de salvaguardar sus valores e intereses, también en el ámbito cibernético. SUBRAYA que una Unión más fuerte y más capaz en materia de seguridad y defensa contribuirá positivamente a la seguridad transatlántica y mundial y complementa a la OTAN, que sigue siendo la base de la defensa colectiva de sus miembros. REAFIRMA la intención de la UE de intensificar su apoyo al orden internacional basado en normas, con las Naciones Unidas como eje central.

3. REITERA, en consonancia con las Conclusiones del Consejo sobre la Estrategia de Ciberseguridad de la Unión Europea y la Brújula Estratégica, la necesidad de afianzar la posición de la Unión en materia cibernética, aumentando a tal fin nuestra aptitud para evitar ciberataques a través del desarrollo de capacidades y medios, la formación, los ejercicios y la mejora de la resiliencia, y respondiendo con firmeza a los ciberataques contra la Unión y sus Estados miembros mediante todas las herramientas que la UE tiene a su disposición. Para ello es necesario seguir mostrando la determinación de la UE de ofrecer respuestas inmediatas y a largo plazo a los agentes de riesgo que intentan negarnos un acceso seguro y abierto al ciberespacio y perjudicar nuestros intereses estratégicos, incluida la seguridad de nuestros socios. DESTACA, en ese contexto, que la posición en materia cibernética pretende combinar las diversas iniciativas que conforman la actuación de la UE destinada a consolidar la paz y la estabilidad en el ciberespacio, y a favorecer un ciberespacio abierto, libre, mundial, estable y seguro, al tiempo que mejora la coordinación de acciones a corto, medio y largo plazo para prevenir, desincentivar e impedir las ciberamenazas y los ciberataques y responder a ellos, y aprovecha las cibercapacidades. DESTACA que estos elementos deben incorporarse a la posición de la UE en materia cibernética, conforme a cinco funciones de la UE en el ámbito cibernético: fortalecer nuestra ciberresiliencia y nuestras capacidades de protección; mejorar la gestión solidaria e integral de las crisis; promover nuestra visión del ciberespacio; aumentar la cooperación con los países socios y las organizaciones internacionales, y prevenir los ciberataques, defenderse de ellos y darles respuesta.

I. REFORZAR NUESTRA CIBERRESILIENCIA Y NUESTRAS CAPACIDADES DE PROTECCIÓN

4. REITERA la necesidad de elevar el nivel general de ciberseguridad de la UE, AGUARDA CON INTERÉS la rápida adopción del proyecto de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en la Unión (Directiva SRI), del proyecto de Reglamento sobre la resiliencia operativa digital del sector financiero (Reglamento DORA) y del proyecto de Directiva relativa a la resiliencia de las entidades críticas (Directiva REC), y TOMA NOTA de la propuesta de Reglamento por el que se establecen medidas destinadas a garantizar un elevado nivel común de ciberseguridad en las instituciones, los órganos y los organismos de la Unión, con el fin de fomentar una Unión Europea que proteja a sus ciudadanos, servicios públicos y empresas en el ciberespacio. ANIMA a la Comisión a que concluya la adopción de propuestas clave destinadas a garantizar la seguridad de las infraestructuras, tecnologías, productos y servicios digitales, al objeto de transmitir un mensaje claro sobre la ambición de la UE en estos ámbitos y propiciar el apoyo a las empresas para que estén a la altura del desafío. INSTA a la Comisión a que proponga requisitos comunes de ciberseguridad de la Unión para los dispositivos conectados y los procesos y servicios asociados a través de la Ley de Ciberresiliencia, que la Comisión deberá presentar antes de finales de 2022, teniendo en cuenta la necesidad de aplicar un enfoque horizontal e integral que abarque todo el ciclo de vida de los productos digitales, así como la normativa vigente, especialmente en el ámbito de la ciberseguridad.

5. INVITA a las autoridades pertinentes, como el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), la Agencia de la Unión Europea para la Ciberseguridad (ENISA) y el Grupo de Cooperación sobre Seguridad de las Redes y la Información (Grupo de Cooperación SRI), junto con la Comisión Europea, a formular recomendaciones, basadas en una evaluación de riesgos, a los Estados miembros y a la Comisión Europea, con el fin de reforzar la resiliencia de las redes e infraestructuras de comunicaciones dentro de la Unión Europea, incluida la aplicación continuada del conjunto de instrumentos de la UE para las redes 5G.

6. INSTA a la UE y a sus Estados miembros a que redoblen sus esfuerzos por aumentar el nivel general de ciberseguridad, por ejemplo, facilitando la aparición de proveedores de servicios de ciberseguridad de confianza, y DESTACA que fomentar el desarrollo de dichos proveedores debe ser una prioridad para la política industrial de la UE en el ámbito de la ciberseguridad. INVITA a la Comisión a que, a fin de resistir y contrarrestar mejor los ciberataques con posibles efectos sistémicos y a partir de las enseñanzas extraídas de la gestión de las vulnerabilidades de Solarwinds, Microsoft Exchange y Apache Log4J, proponga opciones para impulsar la aparición de un sector de servicios de ciberseguridad de confianza, reforzar la ciberseguridad de la cadena de suministro de las TIC, abordar los posibles efectos de las vulnerabilidades de los programas informáticos para la UE y sus Estados miembros —también con miras a la futura Ley de Ciberresiliencia— y mejorar las capacidades de detección y puesta en común de ciberamenazas en los Estados miembros y entre unos Estados y otros.

7. REITERANDO que invertir en innovación y hacer un mejor uso de la tecnología civil es fundamental para aumentar nuestra soberanía tecnológica, también en el ámbito cibernético, PIDE a la Comisión que ponga en marcha rápidamente el Centro Europeo de Competencia en Ciberseguridad para desarrollar un ecosistema europeo sólido de investigación, industria y tecnología cibernéticas, y SUBRAYA la necesidad de impulsar la investigación y la innovación, invertir más en ámbitos civiles y de defensa para fortalecer la base industrial y tecnológica de la defensa europea, y desarrollar las cibercapacidades de la UE y sus Estados miembros, incluidas las capacidades de apoyo estratégico. DESTACA la importancia de hacer un uso intensivo de las nuevas tecnologías, en particular la informática cuántica, la inteligencia artificial y la inteligencia de datos, para lograr ventajas comparativas, también por lo que respecta a las operaciones de respuesta a los ciberataques.

8. RECONOCIENDO que mejorar nuestra ciberseguridad es una manera de aumentar la eficacia y la seguridad de nuestros esfuerzos en tierra, mar, aire y en el espacio ultraterrestre, DESTACA la importancia de integrar los aspectos relativos a la ciberseguridad en todas las políticas públicas de la UE, por ejemplo, en la legislación sectorial que complementa a la Directiva SRI 2, e INVITA a la Comisión a que estudie opciones para aumentar la ciberseguridad en toda la cadena de suministro de la base industrial y tecnológica de la defensa europea.

9. RECONOCE que, para elaborar la posición de la UE en materia cibernética, es esencial destinar recursos financieros y humanos suficientes a la ciberseguridad y a las medidas encaminadas a crear un entorno propicio a la competitividad del sector privado, y que también hay que abordar a escala de la UE la cuestión de la financiación estable y a largo plazo de la ciberseguridad, mediante el diseño y la aplicación de un mecanismo horizontal que combine múltiples fuentes de financiación, como el coste de unos recursos humanos altamente cualificados. INSTA a la Comisión, por tanto, a que estudie las opciones sobre un mecanismo de este tipo antes de finales de 2022, que se debatirán en los órganos pertinentes del Consejo.

10. HACE HINCAPIÉ en la necesidad de redoblar nuestros esfuerzos y aumentar la cooperación en la lucha contra la ciberdelincuencia internacional, en particular los programas de secuestro, mediante el mecanismo EMPACT (plataforma multidisciplinar europea contra las amenazas delictivas), los intercambios entre los sectores de la ciberseguridad, las fuerzas o cuerpos de seguridad y la diplomacia, y el refuerzo de las capacidades policiales en la investigación y el enjuiciamiento de la ciberdelincuencia. REITERA su compromiso de informar a la opinión pública sobre las ciberamenazas y las medidas adoptadas a escala nacional y de la UE contra estas amenazas fomentando la participación de la sociedad civil, el sector privado y el mundo académico, con el fin de sensibilizar e impulsar un nivel adecuado de ciberprotección y ciberhigiene. INSISTE en la necesidad de centrarse en las competencias y capacidades de los ciudadanos en materia de ciberseguridad en la UE y en los Estados miembros, y en la necesidad de fomentar activamente la participación de los usuarios en su propia protección.

II. MEJORAR LA GESTIÓN SOLIDARIA E INTEGRAL DE LAS CRISIS

11. A partir de la experiencia adquirida en los ciberejercicios anuales, otros ejercicios con una dimensión cibernética y el ejercicio EU CyCLES de 2022, DESTACA la importancia de establecer un programa de ciberejercicios intercomunitarios y multinivel periódicos para poner a prueba y definir la respuesta interna y externa de la UE a los ciberincidentes a gran escala, con la participación del Consejo, el SEAE, la Comisión y las partes interesadas pertinentes, como ENISA y el sector privado, y que se articulará y contribuirá a la política general de ejercicios de la UE. HACE HINCAPIÉ en la importancia de seguir profundizando en los ejercicios Cyber Europe y BlueOLEx, mediante la combinación de las respuestas a diferentes niveles. RECONOCE la necesidad de evaluar y consolidar los ejercicios existentes y de explorar la posibilidad de realizar otros ejercicios sobre segmentos específicos del ámbito cibernético, por ejemplo, un ejercicio de los CERT militares o uno dedicado a la cooperación en situaciones de crisis entre las instituciones, los órganos y los organismos de la UE. RECONOCE que la posición de la Unión en materia cibernética reforzará nuestra aptitud para prevenir los ciberataques a través de diversas acciones, como la formación, e INVITA, por tanto, a los Estados miembros a reforzar la cooperación civil y militar en formación de ciberseguridad y ejercicios conjuntos.

12. SUBRAYA la necesidad de seguir probando y reforzando la cooperación operativa y la conciencia situacional común entre los Estados miembros, también a través de redes establecidas, como la red de equipos de respuesta a incidentes de seguridad informática (CSIRT) y la red de organizaciones de enlace de crisis cibernéticas (CyCLONe), con el fin de avanzar en la preparación de la UE para hacer frente a ciberincidentes a gran escala. SUBRAYA la importancia de trabajar en el desarrollo de un lenguaje común entre los Estados miembros y con las instituciones, los órganos y los organismos de la UE, que esté adaptado al debate a nivel político, a fin de respaldar la puesta en marcha de una evaluación consolidada de la gravedad y el impacto de los ciberincidentes en cuestión, así como de las posibles hipótesis de evolución y las necesidades derivadas de dichas hipótesis, según proceda. SUBRAYA a este respecto la necesidad de mejorar la complementariedad de los informes de evaluación común de la situación, incluidos los informes de la red CyCLONe sobre el impacto y la gravedad de los ciberincidentes a gran escala en los Estados miembros de la UE, y las evaluaciones de amenazas facilitadas por el INTCEN en el marco del conjunto de instrumentos de ciberdiplomacia de la UE. INVITA a la Comisión, al Alto Representante y al Grupo de Cooperación SRI, en coordinación con los órganos y organismos civiles y militares pertinentes y las redes existentes, tales como la red CyCLONe, a que efectúen antes de finales de 2022 una evaluación de riesgos y elaboren hipótesis de riesgo desde una perspectiva de ciberseguridad en una situación de amenaza o posible ataque contra Estados miembros o países socios, y a que las presenten a los órganos pertinentes del Consejo. DESTACA la necesidad de una comunicación pública adecuada y coordinada sobre la respuesta de la UE a los ciberincidentes a gran escala.

13. DESTACA la necesidad que existe, en caso de ciberincidentes a gran escala, de reforzar la coordinación y, si procede, de aprovechar los avances logrados y el trabajo realizado por los equipos de respuesta telemática rápida de la CEP y, a partir de la labor de la red de CSIRT y la red CyCLONe, la puesta en común voluntaria entre los Estados miembros de nuestras capacidades de respuesta ante incidentes. RECONOCE que crear vínculos con el sector privado podría ampliar las capacidades públicas, en particular en un contexto de escasez de capacidades en toda la UE, y que identificar y coordinar a estos socios privados podría suponer una diferencia en caso de incidentes a gran escala. Con el fin de lograr una preparación plena frente a los ciberincidentes a gran escala, INVITA a la Comisión a que presente una propuesta sobre un nuevo Fondo de Respuesta a Emergencias en materia de Ciberseguridad antes de que finalice el tercer trimestre de 2022.

14. REITERA, de conformidad con la Brújula Estratégica, la necesidad de invertir en nuestra asistencia mutua, con arreglo al artículo 42, apartado 7, del Tratado de la Unión Europea, así como en la solidaridad, con arreglo al artículo 222 del Tratado de Funcionamiento de la Unión Europea, en particular mediante ejercicios frecuentes. DESTACA, en este marco, la necesidad de seguir trabajando en la prestación y coordinación del apoyo civil y militar bilateral —en particular explorando la posibilidad de que la UE preste ayuda a petición expresa de los Estados miembros— y en la definición de medidas de respuesta adecuadas, por ejemplo, mediante el diseño de una estrategia de comunicación coordinada, en el contexto de la aplicación del artículo 42, apartado 7. OBSERVA que, para ello, conviene también explorar los vínculos con los mecanismos existentes de gestión de crisis de la UE y con el Mecanismo de Protección Civil de la UE.

15. SUBRAYA que, para reforzar la posición de la UE en materia cibernética, será necesario mejorar la seguridad de las comunicaciones. A tal fin, REITERA las orientaciones formuladas en la Brújula Estratégica a este respecto e INVITA a la Comisión y a otras instituciones, órganos y organismos pertinentes a elaborar, antes del fin de 2022, un inventario de las herramientas existentes para una comunicación segura en el ámbito cibernético, que se debatirá en los órganos del Consejo y los grupos de cooperación pertinentes, como la red de CSIRT y la red CyCLONe.

III. PROMOVER NUESTRA VISIÓN DEL CIBERESPACIO

16. RECUERDA que el enfoque común y global de la UE en materia de ciberdiplomacia tiene por objeto contribuir a la prevención de conflictos, la mitigación de las amenazas a la ciberseguridad y una mayor estabilidad en las relaciones internacionales. En este contexto, REAFIRMA el compromiso de la UE con la resolución de conflictos internacionales en el ciberespacio por vías pacíficas y con la aplicación del Derecho internacional, en particular el Derecho internacional de los derechos humanos y el Derecho internacional humanitario, a las acciones de los Estados en el ciberespacio. SUBRAYA el compromiso de la UE y de sus Estados miembros de actuar conforme a las normas voluntarias y no vinculantes de conducta responsable de los Estados en el ciberespacio, acordadas por todos los Estados miembros de las Naciones Unidas. DESTACA la importancia de un ciberespacio abierto, libre, mundial, estable y seguro, en el que se apliquen plenamente los derechos humanos, las libertades fundamentales y el Estado de Derecho en apoyo del bienestar social, el crecimiento económico, la prosperidad y la integridad de nuestras sociedades libres y democráticas, y REAFIRMA el compromiso de la UE y de sus Estados miembros de seguir promoviendo tales valores y principios. Con miras a abrir canales para entablar un diálogo constructivo, franco y abierto con las principales partes interesadas del ciberespacio, DESTACA la importancia de que las cuestiones cibernéticas, en particular el conjunto de instrumentos de ciberdiplomacia de la UE, formen parte integral de las negociaciones de adhesión a la Unión y de los diálogos estratégicos y políticos de la UE con los socios y competidores internacionales, y, al mismo tiempo, PIDE al Alto Representante que revise los diálogos bilaterales existentes en materia cibernética y, en caso necesario, proponga iniciar una cooperación similar con otros países u organizaciones internacionales pertinentes.

17. RECUERDA la importancia de la cooperación multilateral, ya que otras partes interesadas también tienen responsabilidad en materia de ciberseguridad, en particular por lo que respecta a la aplicación de las recomendaciones y decisiones adoptadas en los foros internacionales y regionales. PIDE a la UE y a sus Estados miembros que sigan promoviendo nuestro modelo de ciberespacio y de internet a partir del enfoque multilateral y a través de iniciativas como el Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio y la Declaración sobre el futuro de internet, haciendo hincapié en los beneficios compartidos de la estabilidad en el ciberespacio y sensibilizando a nivel mundial sobre los peligros de una visión de internet autoritaria y centrada en el Estado, e INSTA a la UE y a sus Estados miembros a que continúen fortaleciendo la cooperación con la comunidad multilateral, por ejemplo, mediante el recurso a proyectos pertinentes, como la iniciativa de cyberdiplomacia de la UE del instrumento de política exterior de la UE.

18. SE COMPROMETE a participar de forma continuada en las organizaciones internacionales pertinentes, especialmente en los procesos relacionados con la Primera Comisión y la Tercera Comisión de las Naciones Unidas, al tiempo que hace hincapié en la aplicación sin reservas del Derecho internacional vigente, tanto en el ciberespacio como en relación con este ámbito. DESTACA la importancia de proseguir los esfuerzos encaminados a defender y promover el marco de las Naciones Unidas sobre la conducta responsable de los Estados, y SUBRAYA que la UE y sus Estados miembros trabajarán activamente para reforzar su aplicación, en particular mediante la creación del programa de acción para promover la conducta responsable de los Estados en el ciberespacio. HACE HINCAPIÉ en que la UE y sus Estados miembros participarán activamente en las negociaciones sobre un futuro convenio de las Naciones Unidas que sirva de instrumento eficaz a las autoridades policiales y judiciales en la lucha mundial contra la ciberdelincuencia, teniendo plenamente en cuenta el marco existente de instrumentos internacionales y regionales en este ámbito, en particular el Convenio de Budapest sobre la Ciberdelincuencia. DESTACA la importancia de seguir apoyando la elaboración y la puesta en práctica de medidas de fomento de la confianza a escala regional e internacional, y de continuar impulsando el uso de las cibermedidas de fomento de la confianza existentes en la OSCE, también en épocas de tensiones internacionales.

19. RECUERDA que adoptar un enfoque proactivo basado en los derechos humanos para garantizar normas internacionales en los ámbitos de las tecnologías emergentes y la arquitectura central de internet, en línea con los valores y principios democráticos, es esencial para garantizar que internet siga siendo un instrumento mundial, no fragmentado y abierto, y ABOGA por el principio de respeto al ser humano y atención a la privacidad en el uso y el desarrollo de tecnologías, y por que la utilización de dichas tecnologías sea legal, segura y ética. ANIMA al Alto Representante y a la Comisión a que desarrollen una visión estratégica sobre cuestiones técnicas en el ámbito digital que tengan implicaciones en materia de política exterior y puedan repercutir en la estabilidad del ciberespacio y de internet en particular, también en las organizaciones internacionales especializadas pertinentes (Unión Internacional de Telecomunicaciones, etc.).

IV. AUMENTAR LA COOPERACIÓN CON LOS PAÍSES SOCIOS Y LAS ORGANIZACIONES INTERNACIONALES

20. HACE HINCAPIÉ en la necesidad de vincular mejor la estrategia de desarrollo de las capacidades cibernéticas de la UE a las normas de las Naciones Unidas sobre la conducta responsable de los Estados en el ciberespacio, en particular mediante la elaboración de programas de cooperación y desarrollo de capacidades adaptados para ayudar a terceros Estados en sus esfuerzos de aplicación, y, de este modo, proseguir y ampliar nuestras iniciativas destinadas a impulsar el programa de acción de las Naciones Unidas para promover la conducta responsable de los Estados en el ciberespacio. DESTACA la importancia de integrar plenamente el desarrollo de las capacidades cibernéticas en la oferta de la UE como proveedor de seguridad, con una coordinación adecuada de los esfuerzos entre los Estados miembros y las instituciones, los órganos y los organismos de la UE, y, en particular, ACOGE CON SATISFACCIÓN la cooperación entre los Estados miembros, así como con los socios de los sectores público y privado, especialmente a través de la red para el desarrollo de las capacidades cibernéticas de la UE (CyberNet) y el Foro Mundial sobre Conocimientos Especializados en Ciberseguridad (GFCE), para garantizar la coordinación y evitar duplicaciones.

INSTA al Alto Representante y a la Comisión a establecer un consejo para el desarrollo de capacidades cibernéticas a más tardar en el tercer trimestre de 2022 y a mantener cambios de impresiones periódicos en el Grupo Horizontal «Cuestiones Cibernéticas». INSTA a la Comisión y al Alto Representante a que sigan movilizando recursos del Instrumento de Vecindad, Cooperación al Desarrollo y Cooperación Internacional, el Instrumento de Ayuda Preadhesión (IAP III) y otros instrumentos financieros, como el Fondo Europeo de Apoyo a la Paz (EPF) y la iniciativa Global Gateway, con el fin de contribuir a reforzar la resiliencia de nuestros socios y su capacidad para detectar y abordar las ciberamenazas y para investigar y

enjuiciar los ciberdelitos, y a crear proyectos de cooperación, también en el contexto de crisis, y, en particular, ABOGA por la cooperación con los socios de los Balcanes Occidentales y de la vecindad oriental y meridional de la UE, y por el despliegue de expertos de la UE y de los Estados miembros para ofrecer apoyo en caso de cibercrisis, teniendo en cuenta los mandatos jurídicos existentes.

21. DESTACA la necesidad de redoblar los esfuerzos encaminados a elaborar un enfoque de divulgación estructurado y abierto de la UE acerca del modo de promover un entendimiento común mundial de la aplicación del Derecho internacional en el ciberespacio y del marco de las Naciones Unidas sobre la conducta responsable de los Estados en el ciberespacio —en particular, la iniciativa de un programa de acción para promover la conducta responsable de los Estados en el ciberespacio—, así como acerca de la posición de la UE y sus Estados miembros en las negociaciones en curso en torno a un convenio de las Naciones Unidas sobre la ciberdelincuencia, y, como parte de estos esfuerzos, SOLICITA al Alto Representante que presente un plan de divulgación al Consejo antes de finales de 2022. ANIMA al Alto Representante y a los servicios de la Comisión a que hagan un uso pleno y sistemático de las 145 Delegaciones y emprendan una colaboración periódica y fructífera entre ellas y las embajadas de los Estados miembros en terceros países, bajo los auspicios de la red de ciberdiplomacia prevista de la UE. INSTA al Alto Representante a que ponga en marcha la red de ciberdiplomacia de la UE a más tardar en el tercer trimestre de 2022, contribuyendo al intercambio de información, a la organización de actividades de formación conjuntas para el personal de la UE y de los Estados miembros, a la realización de esfuerzos coherentes de desarrollo de capacidades y al refuerzo de la aplicación del marco de las Naciones Unidas sobre la conducta responsable de los Estados, así como a la adopción de medidas de fomento de la confianza entre los Estados.

22. DESTACA su compromiso de seguir cooperando con las organizaciones internacionales y los países socios para promover una interpretación común del panorama de las ciberamenazas, crear mecanismos de cooperación y determinar de forma proactiva respuestas diplomáticas de cooperación. RECORDANDO los principales logros de la cooperación UE-OTAN en el ámbito de la ciberseguridad en el marco de la aplicación de las Declaraciones conjuntas de Varsovia (2016) y Bruselas (2018), dentro del pleno respeto de la autonomía y los procesos decisorios de ambas organizaciones y conforme a los principios de transparencia, reciprocidad e inclusión, HACE HINCAPIÉ en la necesidad de seguir reforzando la cooperación cibernética con la OTAN mediante ejercicios, la puesta en común de información e intercambios entre expertos, en particular, por lo que respecta al desarrollo de capacidades, al desarrollo de capacidades para los socios, a las misiones y operaciones, a la aplicabilidad del Derecho internacional y de las normas de las Naciones Unidas de conducta responsable de los Estados en el ciberespacio y a las posibles respuestas coordinadas a las actividades informáticas malintencionadas.

V. PREVENIR LOS CIBERATAQUES, DEFENDERSE DE ELLOS Y DARLES RESPUESTA

23. RECONOCE que el ciberespacio se ha convertido en un escenario para la competencia geopolítica y, por lo tanto, REITERA que la UE debe ser capaz de responder rápida y enérgicamente a los ciberataques, como las actividades informáticas malintencionadas patrocinadas por Estados contra la UE y sus Estados miembros, por lo que debe reforzar el conjunto de instrumentos de ciberdiplomacia de la UE y aprovechar al máximo todos sus instrumentos, incluidos los instrumentos políticos, económicos, diplomáticos, jurídicos y de comunicación estratégica disponibles para prevenir, desincentivar e impedir las actividades informáticas malintencionadas y responder a ellas. SUBRAYA que los agentes hostiles deben ser conscientes de que los ciberataques contra los Estados miembros y las instituciones de la UE se detectarán en una fase temprana, se identificarán rápidamente y deberán hacer frente a todas las herramientas y políticas necesarias. Partiendo, en particular, de los elementos que contiene la posición en materia cibernética y de las enseñanzas extraídas de la aplicación del conjunto de instrumentos de ciberdiplomacia desde su creación y del ejercicio EU CyCLES, INVITA a los Estados miembros y al Alto Representante a que, con el apoyo de la Comisión, elaboren a más tardar a finales de 2023 una versión revisada de las directrices de aplicación del conjunto de instrumentos de ciberdiplomacia de la UE, en la que se estudien concretamente medidas de respuesta adicionales.

24. SUBRAYA la necesidad de mantener intercambios periódicos sobre el panorama de las ciberamenazas en los órganos y comités pertinentes del Consejo —colaborando también periódicamente con el sector privado y teniendo en cuenta la evaluación del impacto y de la gravedad de los incidentes recientes— a fin de aumentar la sensibilización general y la preparación para nuevas aplicaciones del conjunto de instrumentos de ciberdiplomacia de la UE, y de concebir nuevos instrumentos que contribuyan a su aplicación. Si bien la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro, OBSERVA la necesidad de reforzar el intercambio de inteligencia e información y la cooperación entre los Estados miembros, así como con el INTCEN, a fin de poder compartir inteligencia al inicio del proceso decisorio, en particular sobre la cuestión de la atribución, permitiendo así una respuesta rápida, eficaz y fundamentada a las actividades informáticas malintencionadas dirigidas contra la UE y sus socios. REITERA la importancia de reforzar la capacidad del INTCEN en el ámbito cibernético, sobre la base de las contribuciones voluntarias de inteligencia de los Estados miembros y sin perjuicio de sus competencias, y de estudiar la propuesta relativa a la posible creación de un grupo de trabajo de ciberinteligencia de los Estados miembros.

25. RECONOCIENDO que las declaraciones de la UE y las medidas restrictivas adoptadas en el marco del conjunto de instrumentos de ciberdiplomacia de la UE han transmitido un mensaje firme de que las actividades informáticas malintencionadas que constituyen una amenaza externa para la UE, sus Estados miembros y sus socios son inaceptables y que, por tanto, dichas actividades y medidas contribuyen a prevenir, desincentivar e impedir las actividades informáticas malintencionadas y a responder a ellas, REITERA su compromiso de utilizar estas medidas para recordar las obligaciones que se aplican al ciberespacio en virtud del Derecho internacional, como la Carta de las Naciones Unidas en su totalidad, y de fomentar el marco de las Naciones Unidas sobre la conducta responsable de los Estados en el ciberespacio —en particular la obligación de todos los Estados de actuar con la diligencia debida para no permitir a sabiendas que su territorio se utilice para cometer actos ilegítimos por medio de las TIC—, con miras a seguir elaborando y promoviendo la visión común de la UE sobre la aplicación del Derecho internacional en el ciberespacio. Observando que con mensajes adecuados y ágiles es posible mitigar los riesgos de escalada y disuadir a quienes dirigen sus ataques contra intereses europeos, INVITA al Alto Representante a que elabore una estrategia de comunicación coherente sobre el uso del conjunto de instrumentos de ciberdiplomacia de la UE, y a que la presente a los Estados miembros.

26. ABOGA por la elaboración de enfoques y respuestas graduales, selectivos y continuados respecto de las actividades informáticas malintencionadas, mediante el recurso a la gran variedad de herramientas que ofrece el conjunto de instrumentos de ciberdiplomacia de la UE, en particular el régimen de sanciones de la Unión contra los ciberataques, y la opción de recurrir a medidas adicionales. HACE HINCAPIÉ en la necesidad de aumentar la posibilidad de movilizar, caso por caso, todas las herramientas disponibles, internas y externas, para prevenir, desincentivar e impedir los ciberataques y responder a ellos, aplicándolas con un enfoque rápido, eficaz, gradual, selectivo y continuado, basado en un compromiso estratégico a largo plazo. INSTA al Alto Representante a que, en cooperación con la Comisión, determine posibles respuestas conjuntas de la UE a los ciberataques en todos los ámbitos —en particular la opción de imponer sanciones—, que permitan reaccionar con rapidez y eficacia cuando sea necesario, y a que las presente al Consejo antes del final del primer trimestre de 2023.

27. Observando que la ciberdefensa es principalmente una responsabilidad nacional, ANIMA a los Estados miembros a seguir desarrollando sus propias capacidades para llevar a cabo operaciones de ciberdefensa, en particular, medidas proactivas de protección, detención, defensa y disuasión frente a los ciberataques, y posiblemente en apoyo de otros Estados miembros y de la UE. Cada Estado miembro ha de mejorar, en caso necesario, sus propias capacidades para prestar y recibir ayuda y asistencia. HACE HINCAPIÉ en que seguir desarrollando estas capacidades debe ser uno de los principales objetivos de la futura política de ciberdefensa de la UE. SEÑALA que la política de ciberdefensa de la UE debe prestar más atención al papel que pueden desempeñar las instituciones y los órganos pertinentes de la UE en el refuerzo de la cooperación entre los actores de ciberdefensa pertinentes de la UE y de los Estados miembros y en el desarrollo de sus propias capacidades, de acuerdo con sus respectivos mandatos. INVITA al Alto Representante a que, junto con la Comisión, complemente la elaboración de una posición de la UE en materia cibernética presentando una ambiciosa propuesta sobre una política de ciberdefensa de la Unión en 2022, que allanará el camino al Consejo para la ulterior definición de la posición de la UE en materia de ciberseguridad.

28. HACE HINCAPIÉ en la necesidad de aumentar la interoperabilidad y el intercambio de información a través de la cooperación entre los equipos militares de respuesta a emergencias informáticas (CERT militares). INVITA a los Estados miembros a crear, a partir de la labor de la Agencia Europea de Defensa, una red de CERT militares destinada a afianzar la cooperación y a facilitar el intercambio de información —lo que también contribuiría a fomentar la coordinación con otras cibercomunidades—, así como una red de cibercomandantes militares para reforzar la cooperación estratégica entre los cibermandos de los Estados miembros de la UE u otras autoridades pertinentes. La creación de estas redes, junto con los ciberproyectos de la CEP, contribuiría a reforzar la ciberdefensa a escala de la UE. DESTACA la importancia de la cooperación entre la red de CERT militares propuesta y la red civil ya existente (CSIRT) para reforzar el intercambio de información y mejorar la conciencia situacional.

29. Partiendo de la visión y estrategia militar de la UE en el ciberespacio como ámbito de operación y teniendo en cuenta el desarrollo en curso del concepto militar de ciberdefensa para las operaciones y misiones militares dirigidas por la UE, REITERA la necesidad de integrar la dimensión cibernética en la planificación y ejecución de las misiones y operaciones de la PCSD, en particular reforzando sus cibercapacidades, y DESTACA que ello contribuirá a una mejor conciencia situacional cibernética a escala de la UE.

30. Para concluir, OBSERVA que la posición en materia cibernética constituirá un paso hacia el establecimiento de una doctrina de la UE para la acción en el ciberespacio, basada en el refuerzo de la resiliencia, las capacidades y las opciones de respuesta, así como una posición común sobre la aplicación del Derecho internacional en el ciberespacio. El Consejo HARÁ BALANCE de los progresos logrados en la aplicación de las presentes Conclusiones en 2023 con el fin de garantizar la ulterior definición de la posición de la UE en materia cibernética.