Consejo de la Unión Europea

Bruselas, 23 de marzo de 2021
(OR. en)

7290/21

CYBER 80
TELECOM 124
COPEN 144
CODEC 443
COPS 107
COSI 50
CSC 119
CSCI 45
IND 70
RECH 117
ESPACE 21

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	22 de marzo de 2021
A:	Delegaciones
Asunto:	Conclusiones del Consejo sobre la Estrategia de Ciberseguridad de la UE para la Década Digital - Conclusiones del Consejo aprobadas por el Consejo en su sesión del 22 de marzo de 2021

Se remiten en anexo, a la atención de las delegaciones, las Conclusiones del Consejo sobre la Estrategia de Ciberseguridad de la UE para la Década Digital, aprobadas por el Consejo en su sesión del 22 de marzo de 2021.

ANEXO

Conclusiones del Consejo sobre la Estrategia de Ciberseguridad de la UE para la Década Digital

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],

- la gobernanza de Internet[2],

- 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»[3],

- el desarrollo de capacidades y competencias en materia de ciberseguridad en la UE[4],

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

- 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»[6],

- acciones complementarias para aumentar la resiliencia y luchar contra las amenazas híbridas[7],

- la configuración del futuro digital de Europa[8],

---

1 12109/13
2 16200/14
3 14435/17 + COR 1
4 7737/19
5 14517/19
6 9596/19
7 14972/19
8 8711/20

- la diplomacia digital[9],

- el refuerzo de la resiliencia y la lucha contra las amenazas híbridas, en particular la desinformación en el contexto de la pandemia de COVID-19[10],

- la ciberdiplomacia[11],

- la respuesta coordinada de la UE a los incidentes y crisis de ciberseguridad a gran escala[12],

- un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia»)[13],

- las directrices para el desarrollo de la capacidad cibernética exterior de la UE[14],

- una recuperación que haga avanzar en la transición hacia una industria europea más dinámica, resiliente y competitiva[15],

- la ciberseguridad de los dispositivos conectados[16],

- reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora[17],

- y la Resolución del Consejo sobre el cifrado: «La seguridad mediante el cifrado y a pesar del cifrado»[18],

---

9 12804/20
10 14064/20
11 6122/15 + COR 1
12 10086/18
13 10474/17
14 10496/18
15 13004/20
16 13629/20
17 14540/16
18 13084/1/20 REV 1

- así como la declaración de los Estados miembros de 15 de octubre de 2020 sobre el establecimiento de la nube de nueva generación para las empresas y el sector público de la UE,

RECORDANDO las Conclusiones del Consejo Europeo sobre la COVID-19, el mercado único, la política industrial, el ámbito digital y las relaciones exteriores de los días 1 y 2 de octubre de 2020[19] y las relativas a la desinformación y las amenazas híbridas y a una nueva agenda estratégica para 2019-2024, de 20 de junio de 2019[20],

RECORDANDO la Estrategia Global sobre Política Exterior y de Seguridad de la Unión Europea «Visión compartida, actuación conjunta: una Europa más fuerte», de 28 de junio de 2016,

RECORDANDO las Comunicaciones de la Comisión Europea sobre configurar el futuro digital de Europa, de 19 de diciembre de 2020[21], y sobre la Estrategia de la UE para una Unión de la Seguridad, de 24 de julio de 2020[22],

RECORDANDO la Comunicación conjunta de la Comisión Europea y el Alto Representante sobre una nueva agenda UE-EE. UU. para el cambio global, de 2 de diciembre de 2020[23],

1. DESTACA que la ciberseguridad es esencial para construir una Europa resiliente, ecológica y digital, y ACOGE CON SATISFACCIÓN la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «La Estrategia de Ciberseguridad de la UE para la Década Digital», en la que se presenta el nuevo marco para la acción de la UE en el ámbito de la «resiliencia, la soberanía tecnológica y el liderazgo», así como para proteger a sus ciudadanos, empresas e instituciones de incidentes y amenazas cibernéticos, al tiempo que se mejora la confianza de las personas y las organizaciones en la capacidad de la UE para promover las redes y los sistemas información, las infraestructuras y una conectividad seguros y fiables, y para fomentar y proteger un ciberespacio global, abierto, libre, estable y seguro basado en los derechos humanos, las libertades fundamentales, la democracia y el Estado de Derecho.

---

19 EUCO 13/20
20 EUCO 9/19
21 COM(2020) 67 final de 19.2.2020.
22 COM(2020) 605 final de 24.7.2020.
23 JOIN(2020) 22 final de 2.12.2020.

2. RECONOCE que la pandemia de COVID-19 ha puesto de relieve la importancia que han cobrado en nuestra vida diaria la creciente necesidad de confianza en las herramientas y los sistemas de las tecnologías de la información y la comunicación (TIC) y su seguridad. SUBRAYA que la ciberseguridad y una Internet global y abierta son vitales para el funcionamiento de la administración y las instituciones públicas tanto a escala nacional como de la UE, y para nuestra sociedad y la economía en su conjunto.

3. INCIDE en la necesidad de sensibilizar en mayor medida sobre las cuestiones cibernéticas en los ámbitos de decisión política y estratégica, proporcionando a los responsables de la toma de decisiones los conocimientos y la información pertinentes, y SUBRAYA la necesidad de aumentar la sensibilización del público en general y de promover la ciberhigiene.

4. ABOGA POR la promoción y protección de los valores esenciales de la UE, como la democracia, el Estado de Derecho, los derechos humanos y las libertades fundamentales, incluidos el derecho a la libertad de expresión e información, el derecho a la libertad de reunión y asociación y el derecho a la intimidad en el ciberespacio. ACOGE FAVORABLEMENTE, en este sentido, que se mantengan los esfuerzos constantes para proteger a los defensores de los derechos humanos y a los miembros de la sociedad civil y del mundo académico que trabajan en cuestiones como la ciberseguridad, la confidencialidad de los datos, la vigilancia y la censura en línea, ofreciendo directrices prácticas adicionales, promoviendo buenas prácticas y redoblando los esfuerzos de la UE para impedir las violaciones y los abusos de los derechos humanos y el uso indebido de las tecnologías emergentes, en particular mediante la adopción de medidas diplomáticas cuando sea necesario, así como el control de las exportaciones de dichas tecnologías. HACE HINCAPIÉ, en este contexto, en la importancia del Plan de Acción de la UE para los Derechos Humanos y la Democracia 2020-2024 y las Directrices de la UE sobre derechos humanos relativas a la libertad de expresión en Internet y fuera de Internet.

5. DESTACA que lograr la autonomía estratégica preservando al mismo tiempo una economía abierta es un objetivo clave de la Unión de cara a determinar por sí misma su trayectoria e intereses económicos. Para ello es necesario aumentar la capacidad de adoptar decisiones autónomas en el ámbito de la ciberseguridad con el objetivo de reforzar el liderazgo digital de la UE y sus capacidades estratégicas. RECUERDA que esto implica detectar y reducir las dependencias estratégicas y fortalecer la resiliencia en los ecosistemas industriales más sensibles y en ciertos ámbitos específicos. SUBRAYA que tal vez sea preciso diversificar las cadenas de producción y suministro, fomentar y atraer inversiones y producción en Europa, explorar soluciones alternativas y modelos circulares y promover una amplia cooperación industrial entre los Estados miembros.

6. Teniendo en cuenta la escasez de competencias digitales y de ciberseguridad de la población activa, DESTACA la importancia de satisfacer la demanda de mano de obra formada en el ámbito digital y de la ciberseguridad, en particular, desarrollando, reteniendo y atrayendo a los mejores talentos, por ejemplo, mediante la educación y la formación, para poder digitalizar nuestra sociedad de manera que se garantice la ciberseguridad. PROMUEVE una mayor participación de las mujeres y las niñas en la enseñanza de las ciencias, la tecnología, la ingeniería y las matemáticas, así como en el perfeccionamiento y el reciclaje profesional en materia de competencias digitales en los empleos del ámbito de las TIC, pues es uno de los medios para superar la brecha digital de género.

7. 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 su compromiso con la resolución de conflictos internacionales en el ciberespacio por vías pacíficas, y que todos los esfuerzos diplomáticos de la UE deben dirigirse, como prioridad, a promover la seguridad y la estabilidad en el ciberespacio mediante el refuerzo de la cooperación internacional, y a atenuar el riesgo de percepciones erróneas, escalada y conflicto que puede derivarse de los incidentes relacionados con las TIC, y APOYA el ulterior desarrollo y ejecución de medidas de fomento de la confianza a escala regional e internacional. REITERA el llamamiento de la Asamblea General de las Naciones Unidas, acordado por consenso, para que los Estados miembros de las Naciones Unidas se guíen por las recomendaciones de los informes del Grupo de Expertos Gubernamentales en su uso de las TIC, y REAFIRMA la aplicación del Derecho internacional, en particular de la Carta de las Naciones Unidas en su totalidad, en el ciberespacio.

8. REAFIRMA que resulta esencial seguir elaborando normas y estándares en el seno de la Unión, a través de un enfoque basado en la participación de múltiples partes interesadas, con vistas a configurar sustancialmente las normas y los estándares internacionales en el ámbito de las tecnologías emergentes y la infraestructura técnica y lógica esencial para la disponibilidad general y la integridad del núcleo público de Internet, de manera que dichas normas y estándares sean conformes con los valores universales y de la UE. Esto garantizará que Internet siga siendo global, abierta, libre, estable y segura, que el uso y el desarrollo de las tecnologías digitales respeten los derechos humanos, y que estas se utilicen de manera lícita, segura y ética. TOMA NOTA de la futura estrategia de normalización y SE COMPROMETE a llevar a cabo una difusión proactiva y coordinada para promover el liderazgo de la UE y los objetivos de la Unión a escala internacional, en particular en diversos organismos internacionales de normalización y mediante la cooperación con socios de ideas afines, la sociedad civil, el mundo académico y el sector privado.

9. APOYA FIRMEMENTE el modelo basado en múltiples partes interesadas para la gobernanza de Internet y la ciberseguridad, y se compromete a reforzar los intercambios periódicos y estructurados con partes interesadas, incluidos el sector privado, el mundo académico y la sociedad civil, en foros internacionales, también en el contexto del Llamamiento de París para la Confianza y la Seguridad en el Ciberespacio. PROMUEVE un acceso universal, asequible y equitativo a Internet que permita superar las brechas digitales y, en particular, el empoderamiento de mujeres, niñas y personas en situaciones vulnerables o marginadas, tanto en la formulación de políticas como en el uso de Internet.

10. DESTACA la necesidad de incluir la ciberseguridad en las inversiones y las iniciativas digitales en los próximos años, y de contribuir progresivamente a unas condiciones de competencia equitativas en materia de ciberseguridad, y TOMA NOTA del plan de la Comisión de elevar el gasto público y atraer la inversión privada en el ámbito de la ciberseguridad. DESTACA la importancia de las pequeñas y medianas empresas (pymes) en el ecosistema de la ciberseguridad y RECONOCE los instrumentos financieros pertinentes de que se dispone para hacer hincapié en la ciberseguridad dentro del ámbito de la transformación digital durante el marco financiero plurianual 2021-2027, así como en el Mecanismo de Recuperación y Resiliencia.

11. ESPERA CON INTERÉS la aplicación en breve del Reglamento 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, en particular la pronta creación y puesta en funcionamiento del Centro Europeo de Competencia en Ciberseguridad en Bucarest. La adopción sin demora del programa del Centro contribuirá a maximizar los efectos de las inversiones destinadas a reforzar el liderazgo y la autonomía estratégica de la Unión en materia de ciberseguridad y a respaldar las capacidades y competencias tecnológicas, así como a aumentar la competitividad global de la Unión con la aportación de las comunidades empresarial y académica en el ámbito de la ciberseguridad, incluidas las pymes y los centros de investigación, que se beneficiarán de una colaboración más sistemática, inclusiva y estratégica, teniendo en cuenta la cohesión de la Unión y de todos sus Estados miembros.

12. ACOGE CON SATISFACCIÓN el trabajo en curso dirigido por ENISA, junto con los Estados miembros y las partes interesadas, para proporcionar a la UE esquemas de certificación de productos, servicios y procesos de TIC que contribuyan a elevar el nivel general de ciberseguridad en el mercado único digital. En este contexto, ESPERA CON INTERÉS el programa de trabajo evolutivo de la Unión con vistas a desarrollar esquemas de certificación de la ciberseguridad de la UE en el marco del Reglamento de Ciberseguridad. RECONOCE, en este contexto, el papel fundamental de la UE en la elaboración de normas capaces de conformar el panorama de la ciberseguridad y que contribuyan a garantizar una competencia leal en la UE y a escala mundial, promoviendo el acceso al mercado y abordando los riesgos de seguridad al tiempo que se garantiza la aplicabilidad del marco legislativo de la Unión.

13. SUBRAYA que es importante evaluar si se precisa de una legislación horizontal, que especifique también las condiciones necesarias para la comercialización, con el fin de abordar a largo plazo todas las cuestiones pertinentes de la ciberseguridad de los dispositivos conectados, como la disponibilidad, la integridad y la confidencialidad. ACOGE FAVORABLEMENTE, a este respecto, la celebración de un debate para estudiar el ámbito de aplicación de dicha legislación y sus vínculos con el marco de certificación de la ciberseguridad que se define en el Reglamento de Ciberseguridad, con el objetivo de elevar el nivel de seguridad en el mercado único digital. SUBRAYA que los requisitos de ciberseguridad deben definirse con arreglo a la legislación pertinente de la Unión, incluidos el Reglamento de Ciberseguridad, el nuevo marco legislativo, el Reglamento sobre la Normalización Europea y la posible futura legislación horizontal, con el fin de evitar la ambigüedad y la fragmentación de la legislación.

14. RECONOCE la importancia de adoptar un enfoque global y horizontal sobre la ciberseguridad en la Unión, respetando plenamente las competencias y las necesidades de los Estados miembros, así como la importancia del apoyo continuo a la asistencia técnica y la cooperación para desarrollar la capacidad de los Estados miembros. Teniendo en cuenta la evolución del panorama de las ciberamenazas, TOMA NOTA de la nueva propuesta de Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, que se basa en la Directiva SRI, y reitera su apoyo al refuerzo y la armonización de los marcos nacionales de ciberseguridad y a la cooperación continua entre los Estados miembros. Además, SUBRAYA la necesidad de armonizar y articular la legislación sectorial en este ámbito.

15. TOMA NOTA de la propuesta de la Comisión de asistir a los Estados miembros en el establecimiento y el refuerzo de los centros de operaciones de seguridad (COS), con el fin de crear una red de COS en toda la UE para vigilar y anticipar mejor los indicios de ataque a las redes. En este contexto, ESPERA los planes detallados de la Comisión relativos a la red de COS, respetando al mismo tiempo las competencias de los Estados miembros. RECUERDA los esfuerzos dedicados por los Estados miembros, con el apoyo de la UE, a establecer equipos de respuesta a incidentes de seguridad informática (CSIRT) sectoriales, nacionales y regionales y centros de puesta en común y análisis de la información nacionales o europeos como parte de una red eficaz de asociaciones en materia de ciberseguridad en la Unión. ESPERA CON INTERÉS que se considere el potencial de esta red para reforzar los COS, así como su complementariedad y coordinación con las redes y los agentes existentes (en particular, la Red de CSIRT), con el fin de promover una cultura de intercambio de información eficiente, segura y fiable. DESTACA que este proceso se basará en la labor realizada en el contexto de las iniciativas de inteligencia artificial e informática de alto rendimiento y por los centros europeos de innovación digital.

16. TOMA NOTA del posible desarrollo de un sistema de conectividad seguro, basado en la infraestructura europea de comunicación cuántica (EuroQCI) y la comunicación gubernamental por satélite de la Unión Europea (Govsatcom), y RECONOCE que todo posible desarrollo futuro debe basarse en un marco de ciberseguridad sólido y ha de tener en cuenta toda la infraestructura de comunicaciones electrónicas, como los sistemas de redes espaciales, terrestres y submarinas.

17. ESPERA CON INTERÉS los debates con la Comisión, ENISA, los dos operadores de servidores raíz del DNS de la UE y la comunidad de múltiples partes interesadas para evaluar el papel de estos dos operadores a la hora de garantizar que Internet siga siendo accesible a escala mundial y no fragmentada. ACOGE CON SATISFACCIÓN que prosigan los debates sobre la intención de la Comisión de desarrollar un servicio europeo alternativo de acceso a la Internet mundial («iniciativa DNS4EU»), basado en un modelo transparente que se ajuste a las normas y reglas más recientes sobre seguridad, protección de datos y protección de la intimidad desde el diseño y por defecto, con el fin de contribuir a aumentar la resiliencia, manteniendo y mejorando al mismo tiempo la conectividad internacional para todos los Estados miembros.

18. RECONOCE la necesidad de un esfuerzo conjunto de la Comisión y los Estados miembros para acelerar la adopción de las principales normas de Internet, incluidas las relativas al IPv6, y de las normas de seguridad de Internet consolidadas, ya que son fundamentales para elevar el nivel global de seguridad, resiliencia, apertura e interoperabilidad de la Internet mundial, al tiempo que aumentan la competitividad de las empresas de la UE y, en particular, de los operadores de infraestructuras de Internet.

19. SUBRAYA la importancia de un enfoque coordinado, así como del desarrollo y la aplicación de medidas eficaces a escala nacional para reforzar la ciberseguridad de las redes 5G. APOYA los próximos pasos que deben darse en materia de ciberseguridad de las redes 5G, presentados en el apéndice de la Estrategia de Ciberseguridad de la UE y basados en los resultados del informe acerca del impacto de la Recomendación de la Comisión sobre la seguridad de las redes 5G, por ejemplo, en lo que respecta a la definición de un enfoque global y a largo plazo que tenga en cuenta toda la cadena de valor y el ecosistema de la 5G. Con vistas a reforzar aún más el enfoque coordinado de la seguridad de las redes 5G, INSTA a los Estados miembros, las instituciones de la UE y otras partes interesadas pertinentes a proseguir con su inventario periódico, así como con el intercambio de información y buenas prácticas en el marco del flujo de trabajo específico del Grupo de Cooperación SRI sobre la ciberseguridad de la 5G, y a informar periódicamente al Consejo de los avances logrados. DESTACA, al tiempo que hace hincapié en la responsabilidad de los Estados miembros en la protección de la seguridad nacional, su firme voluntad de aplicar y culminar con prontitud la ejecución de las medidas del conjunto de instrumentos de la UE para las redes 5G, y de seguir esforzándose por garantizar la seguridad de las redes 5G y el desarrollo de las futuras generaciones de redes. La estrecha cooperación entre los Estados miembros, la Comisión y ENISA en materia de seguridad de las redes 5G podría servir de ejemplo para otras cuestiones del ámbito de la ciberseguridad, respetando al mismo tiempo las competencias de los Estados miembros y los principios de subsidiariedad y proporcionalidad.

20. RECONOCE la importancia de seguir integrando la ciberseguridad en los mecanismos de la UE de respuesta a las crisis y de poner a prueba dichos mecanismos en los ejercicios pertinentes, y DESTACA la importancia de reforzar la cooperación y el intercambio de información entre las distintas comunidades informáticas dentro de la UE y de vincular las iniciativas, estructuras y procedimientos existentes (como el Dispositivo RPIC, la Red de CSIRT, el Grupo de Cooperación SRI, CyCLONe, el Centro Europeo contra la Ciberdelincuencia, el INTCEN y otros organismos pertinentes de la Unión) en caso de incidentes y amenazas cibernéticos a gran escala y transfronterizos. TENIENDO EN CUENTA los avances ya logrados en este ámbito, ESPERA la propuesta de la Comisión relativa al proceso, los hitos y el calendario para definir la unidad informática conjunta, con vistas a proporcionar valor añadido y un enfoque claro y a racionalizar el marco de gestión de crisis de ciberseguridad de la UE, en particular mediante la preparación, el conocimiento compartido de la situación, el refuerzo de la respuesta coordinada y los ejercicios, de una manera transparente y gradual, evitando al mismo tiempo la duplicación y el solapamiento y respetando las competencias de los Estados miembros.

21. SUBRAYA la importancia de promover la cooperación y el intercambio de información entre los agentes pertinentes del ámbito de la ciberseguridad y las autoridades competentes en materia de seguridad y justicia penal, como las autoridades policiales y judiciales, así como la necesidad de ampliar y mejorar la capacidad de estas autoridades para investigar y perseguir la ciberdelincuencia y para fomentar las negociaciones internacionales y las normas de la UE sobre el acceso transfronterizo a pruebas electrónicas. Con independencia del entorno tecnológico del momento, es esencial preservar las facultades de las autoridades competentes en los ámbitos de la seguridad y la justicia penal mediante un acceso legítimo que les permita llevar a cabo sus tareas, con arreglo a lo dispuesto y autorizado por la ley. Las leyes que establezcan las competencias ejecutivas siempre deben respetar plenamente la tutela judicial efectiva y otras garantías, así como los derechos fundamentales, en particular el derecho al respeto de la vida privada y la privacidad de las comunicaciones y el derecho a la protección de los datos personales.

22. REAFIRMA su apoyo al desarrollo, la aplicación y el uso de un cifrado sólido como medio necesario para proteger los derechos fundamentales y la seguridad digital de las personas, los gobiernos, las empresas y la sociedad y, al mismo tiempo, RECONOCE la necesidad de garantizar la capacidad de las autoridades competentes en el ámbito de la seguridad y la justicia penal, como las autoridades policiales y judiciales, para ejercer sus competencias legales, tanto en línea como fuera de línea, con el fin de proteger nuestras sociedades y a nuestros ciudadanos. Las autoridades competentes deben poder acceder a los datos de forma legítima y selectiva, respetando plenamente los derechos fundamentales y la legislación pertinente en materia de protección de datos y preservando al mismo tiempo la ciberseguridad. DESTACA que toda medida adoptada debe ponderar cuidadosamente estos intereses con los principios de necesidad, proporcionalidad y subsidiariedad.

23. APOYA y PROMUEVE el Convenio de Budapest sobre la Ciberdelincuencia y los trabajos en curso sobre el Segundo Protocolo adicional a dicho Convenio. Por otra parte, sigue participando en intercambios multilaterales sobre ciberdelincuencia, por ejemplo, en procesos relacionados con el Consejo de Europa, la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) y la Comisión de Prevención del Delito y Justicia Penal (CPDJP), con el fin de garantizar una cooperación internacional reforzada para luchar contra la ciberdelincuencia, que incluye el intercambio de buenas prácticas y conocimientos técnicos, y el apoyo a la creación de capacidades, respetando, promoviendo y protegiendo al mismo tiempo los derechos humanos y las libertades fundamentales.

24. Aunque la seguridad nacional sigue siendo responsabilidad exclusiva de cada Estado miembro, RECONOCE la importancia de la cooperación estratégica en materia de inteligencia sobre las amenazas y actividades cibernéticas, e INVITA a los Estados miembros, a través de sus autoridades competentes, a seguir contribuyendo a la labor del INTCEN, que es el eje de la UE para el conocimiento de la situación y la evaluación de amenazas relativas a cuestiones cibernéticas, y a considerar la propuesta sobre la posible creación de un grupo de trabajo de inteligencia cibernética de los Estados miembros, con el fin de reforzar la capacidad específica del INTCEN en este ámbito, sobre la base de las contribuciones voluntarias en materia de inteligencia de los Estados miembros, y sin perjuicio de sus competencias.

25. DESTACA la importancia de un marco de seguridad sólido y coherente para proteger a todo el personal, los datos, las redes de comunicación y los sistemas de información de la UE, así como de los procesos decisorios basados en normas exhaustivas, coherentes y homogéneas. En particular, esta tarea debe abordarse mediante el aumento de la resiliencia y la mejora de la cultura de seguridad de la UE frente a las ciberamenazas, y el refuerzo de la seguridad de las redes de la UE clasificadas y no clasificadas, al tiempo que se garantiza una gobernanza adecuada y la disposición de recursos y capacidades suficientes, también en el contexto del fortalecimiento del mandato del CERT-UE. ACOGE CON SATISFACCIÓN, en este contexto, los debates en curso acerca del establecimiento de normas comunes sobre seguridad de la información, teniendo debidamente en cuenta las normas de seguridad del Consejo para la protección de la información clasificada de la UE, así como la definición de normas comunes vinculantes sobre ciberseguridad para todas las instituciones, órganos y organismos de la Unión.

26. PARTIENDO de los esfuerzos de la UE en materia de ciberdiplomacia, SE COMPROMETE a elevar la eficacia y la eficiencia del conjunto de instrumentos de ciberdiplomacia, y ESPERA CON INTERÉS que se ahonde en los debates sobre su alcance y uso con arreglo a las enseñanzas extraídas de la aplicación de este instrumento hasta la fecha. Estos debates deben contribuir al fomento de la seguridad a escala internacional mediante la promoción del diálogo y de una visión compartida de las cuestiones de ciberseguridad, el refuerzo de la prevención, la estabilidad y la cooperación y el fomento de la confianza y la creación de capacidades y, en caso necesario, la aplicación de medidas restrictivas, con el fin de prevenir, desincentivar e impedir las actividades cibernéticas malintencionadas contra la integridad y la seguridad de la UE y sus Estados miembros y responder a ellas, contribuyendo así a la seguridad y la estabilidad internacionales y consolidando la posición de la UE en materia cibernética, de plena conformidad con las competencias y prerrogativas nacionales. En particular, debe prestarse especial atención a la prevención y la lucha contra ciberataques con efectos sistémicos que puedan afectar a nuestras cadenas de suministro, infraestructuras críticas y servicios esenciales, e instituciones y procesos democráticos, y socavar nuestra seguridad económica, como en caso de robo de propiedad intelectual facilitado por medios cibernéticos. Los Estados miembros y las instituciones de la UE también deben seguir reflexionando sobre la articulación entre el marco de gestión de crisis de ciberseguridad de la UE, el conjunto de instrumentos de ciberdiplomacia y las disposiciones del artículo 42, apartado 7, del TUE y del artículo 222 del TFUE, especialmente mediante el trabajo basado en supuestos para formular una interpretación común de las modalidades prácticas de aplicación del artículo 42, apartado 7, del TUE.

27. RECONOCE la importancia de reforzar la cooperación con las organizaciones internacionales y los países socios con el fin de avanzar en una interpretación compartida del panorama de las ciberamenazas, emprender diálogos y mecanismos de cooperación, determinar, cuando proceda, respuestas diplomáticas de cooperación, y mejorar el intercambio de información, también a través de la educación, la formación y diversos ejercicios. En particular, DESTACA que una sólida asociación transatlántica en el ámbito de la ciberseguridad contribuye a nuestra seguridad, estabilidad y prosperidad comunes, y TOMA NOTA de las disposiciones sobre cooperación en materia de ciberseguridad en el marco del Acuerdo de Comercio y Cooperación entre la UE y el Reino Unido. RECORDANDO los principales logros de la cooperación entre la UE y la OTAN en el ámbito de la ciberseguridad en el marco de la aplicación de las Declaraciones Conjuntas de Varsovia (2016) y Bruselas (2018), reitera la importancia de una cooperación reforzada, mutuamente enriquecedora y beneficiosa a través de la educación, la formación, la realización de ejercicios y la respuesta coordinada a las actividades cibernéticas malintencionadas, respetando plenamente la autonomía y los procedimientos decisorios de ambas organizaciones, sobre la base de los principios de transparencia, reciprocidad e inclusividad.

28. Con el fin de contribuir a un ciberespacio global, abierto, libre, estable y seguro, cada vez más importante para preservar la prosperidad, el crecimiento, la seguridad, el bienestar, la conectividad y la integridad de nuestras sociedades, SE COMPROMETE a participar de manera continua en los procesos de establecimiento de normas en las organizaciones internacionales, especialmente en los procesos relacionados con la Primera Comisión de las Naciones Unidas, promoviendo y contribuyendo al reconocimiento de la aplicación del Derecho internacional en el ciberespacio y a la adhesión a las normas, reglas y principios de comportamiento responsable de los Estados en el ciberespacio, en particular promoviendo el rápido establecimiento de un programa de acción para fomentar el comportamiento responsable de los Estados en el ciberespacio, en tanto que seguimiento constructivo, inclusivo y consensuado de los procesos en curso del Grupo de Expertos Gubernamentales y del Grupo de Trabajo de Composición Abierta de las Naciones Unidas.

29. RECUERDA su firme adhesión a un multilateralismo eficaz y a un orden mundial basado en normas con las Naciones Unidas como eje central, y su determinación de reforzar la cooperación y la coordinación con las organizaciones internacionales y regionales, a saber, el sistema de las Naciones Unidas, la OTAN, el Consejo de Europa, la OSCE, la OCDE, la Unión Africana, la Organización de los Estados Americanos, la ASEAN, el Foro Regional de la ASEAN, el Consejo de Cooperación del Golfo y la Liga de los Estados Árabes, en lo que respecta a los debates sobre cuestiones relacionadas con el ciberespacio, así como a la continuación y la ampliación de los ciberdiálogos estructurados de la UE y las consultas con terceros países. SUBRAYA su apoyo activo a las Naciones Unidas, en particular en lo que atañe a su Agenda 2030, incluidos los Objetivos de Desarrollo Sostenible, y ACOGE CON SATISFACCIÓN la hoja de ruta para la cooperación digital y la Agenda para el Desarme, ambas del secretario general de las Naciones Unidas, que fomentan la rendición de cuentas y la observancia de normas en el ciberespacio y contribuyen a la prevención y la resolución pacífica de conflictos derivados de actividades malintencionadas en el ciberespacio. ACOGE CON SATISFACCIÓN la propuesta del Alto Representante para Asuntos Exteriores y Política de Seguridad de establecer una red informal de ciberdiplomacia de la UE destinada a impulsar la participación y los conocimientos técnicos, tanto de la UE como de los Estados miembros, en cuestiones cibernéticas internacionales, con el fin de reforzar las actividades coordinadas de proyección exterior.

30. ESPERA CON INTERÉS la futura propuesta de revisión del marco político de ciberdefensa de la UE, y SE COMPROMETE a seguir esforzándose por reforzar las dimensiones de ciberseguridad y ciberdefensa con vistas a garantizar que estas se integren plenamente en el ámbito más amplio de la seguridad y la defensa, en particular en el contexto de la labor relativa a la Brújula Estratégica. CONSIDERA que la futura «Visión y estrategia militar en el ciberespacio como un dominio de operaciones» contribuirá a ahondar en estos debates. ACOGE CON SATISFACCIÓN la iniciativa de la Agencia Europea de Defensa de fomentar la cooperación entre los CERT militares y APOYA los esfuerzos dedicados a potenciar las sinergias cívico-militares y la coordinación en materia de ciberdefensa y ciberseguridad, concretamente en los aspectos relacionados con el espacio, también a través de los proyectos específicos de la Cooperación Estructurada Permanente.

31. ACOGE CON SATISFACCIÓN la propuesta de elaborar una agenda para el desarrollo de la capacidad cibernética exterior de la UE, la propuesta de crear un consejo para el desarrollo de la capacidad cibernética de la UE y el establecimiento y la implantación de la CyberNet de la UE (red para el desarrollo de la capacidad cibernética de la UE) con el fin de aumentar la ciberresiliencia y las cibercapacidades en todo el mundo. En este contexto, ACOGE FAVORABLEMENTE la cooperación con los Estados miembros, así como con los socios de los sectores público y privado, en particular con el Foro Mundial sobre Conocimientos Especializados en Ciberseguridad (*Global Forum on Cyber Expertise*) y otros organismos internacionales pertinentes, con el fin de garantizar la coordinación y evitar la duplicación. En particular, PROMUEVE la cooperación con socios de los Balcanes Occidentales y de la vecindad oriental y meridional de la UE.

32. Para garantizar que todos los países puedan aprovechar los beneficios sociales, económicos y políticos de Internet y del uso de las tecnologías, SE COMPROMETE —en consonancia también con los esfuerzos realizados en el marco del Plan de Acción para la Democracia Europea— a ayudar a los países socios a hacer frente al creciente desafío de las actividades cibernéticas malintencionadas, en particular las que perjudican el desarrollo de sus economías y sociedades y la integridad y la seguridad de los sistemas democráticos.

33. Con el fin de garantizar el desarrollo, la ejecución y el seguimiento de las propuestas presentadas en la Estrategia de Ciberseguridad de la UE, y teniendo en cuenta el carácter plurianual de algunas de las iniciativas, ANIMA a la Comisión y al Alto Representante para Asuntos Exteriores y Política de Seguridad a establecer un plan de ejecución detallado en el que se fijen las prioridades y el calendario de las acciones previstas. SUPERVISARÁ los avances en la aplicación de las presentes Conclusiones mediante un plan de acción que el Consejo revisará y actualizará periódicamente en estrecha colaboración con la Comisión Europea y el Alto Representante.