Consejo de la Unión Europea

Bruselas, 20 de noviembre de 2017
(OR. en)

14435/17

CYBER 183
TELECOM 303
ENFOPOL 534
JAI 1055
MI 845
COSI 283
JAIEX 101
RELEX 989
IND 317
CSDP/PSDC 643
COPS 360
POLMIL 145

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
Fecha:	20 de noviembre de 2017
A:	Delegaciones
N.º doc. prec.:	13943/17 + COR 1
N.° doc. Ción.:	12210/17, 12211/17
Asunto:	Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE» - Conclusiones del Consejo (20 de noviembre de 2017)

Adjunto se remite a las Delegaciones, en el anexo, el proyecto de Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE», adoptada por el Consejo de Asuntos Generales el 20 de noviembre de 2017.

ANEXO

Proyecto de Conclusiones del Consejo sobre la Comunicación conjunta al Parlamento Europeo y al Consejo titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE»

El Consejo de la Unión Europea,

1. RECONOCIENDO la importancia de la ciberseguridad, protectora del Estado de Derecho y de los derechos humanos y las libertades fundamentales de cada persona, para la prosperidad, el crecimiento y la seguridad de la UE y para la integridad de nuestras sociedades libres y democráticas y de los procesos en los que se apoyan en la era digital;

2. SUBRAYANDO la necesidad de abordar la ciberseguridad con un planteamiento coherente a escalas nacional, de la UE y mundial, pues las ciberamenazas pueden afectar a nuestra democracia, nuestra prosperidad, nuestra estabilidad y nuestra seguridad;

3. TOMANDO NOTA de que un alto nivel de ciberresiliencia en toda la UE es también importante para generar confianza en el mercado único digital y para seguir desarrollando una Europa digital;

4. REITERANDO que la UE no dejará de promover un ciberespacio abierto, global, libre, pacífico y seguro, en el que se apliquen y respeten plenamente, tanto dentro de la UE como a escala mundial, los derechos humanos y las libertades fundamentales, en particular los derechos a la libertad de expresión, al acceso a la información, a la protección de datos y a la intimidad y la seguridad, así como los valores y principios fundamentales de la UE y HACIENDO HINCAPIÉ en la importancia crucial de lograr un equilibrio adecuado entre los derechos humanos y las libertades fundamentales, por una parte, y el cumplimiento de los requisitos de la política de seguridad interior de la UE, por otra[1];

5. RECONOCIENDO que el Derecho internacional, en particular la Carta de las Naciones Unidas en todos sus elementos, el Derecho internacional de los derechos humanos y el Derecho internacional humanitario se aplican en el ciberespacio y, en consecuencia, SUBRAYANDO la necesidad de seguir esforzándose para garantizar el respeto del Derecho internacional en el ciberespacio;

---

[1] 12650/17.

6. RECORDANDO sus Conclusiones sobre la Estrategia de ciberseguridad de la UE[2], sobre la gobernanza de Internet[3], sobre el refuerzo de la ciberresiliencia de la UE[4], sobre la ciberdiplomacia[5] y sobre un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas[6], sobre la mejora de la justicia penal en el ciberespacio[7], sobre seguridad y defensa en el contexto de la Estrategia Global de la UE[8], el Marco común relativo a la lucha contra las amenazas híbridas[9] y las Conclusiones sobre la revisión intermedia de la Estrategia renovada de Seguridad Interior de la Unión Europea 2015-2020[10];

7. RECONOCIENDO que el marco que proporciona el Convenio sobre la Ciberdelincuencia del Consejo de Europa (el Convenio de Budapest) ofrece una base sólida a un grupo diverso de países para emplear una norma jurídica eficaz en el marco de las distintas legislaciones nacionales y en la cooperación internacional en la lucha contra la ciberdelincuencia;

8. RECONOCIENDO la necesidad de hacer mayor hincapié en la aplicación del marco político de ciberdefensa de la UE de 2014 y de actualizarlo para integrar aún más la ciberseguridad y la defensa en la política común de seguridad y defensa (PCSD) y en el programa sobre seguridad exterior y defensa en su conjunto;

9. RECONOCIENDO que una industria europea competitiva a nivel mundial es un elemento importante para alcanzar un nivel elevado de ciberseguridad a escala nacional y en toda la UE;

10. RECORDANDO que, de conformidad con el artículo 4, apartado 2, del TUE, la seguridad nacional es responsabilidad exclusiva de cada Estado miembro.

---

2 Docs. 12109/13 y 6225/13 (Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro (COM JOIN(2013) 1 final)).

3 Docs. 16200/14 y 6460/14 (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: La política y la gobernanza de Internet - El papel de Europa en la configuración de la gobernanza de Internet (COM(2014) 72 final)).

4 Docs. 14540/16 y 11013/16 (Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Reforzar el sistema de ciberresiliencia de Europa y promover una industria de la ciberseguridad competitiva e innovadora (COM(2016) 410 final).

5 6122/15.

6 9916/17.

7 10007/16.

8 9178/17.

9 7688/16 (Comunicación conjunta al Parlamento Europeo y al Consejo: Marco común relativo a la lucha contra las amenazas híbridas: una respuesta de la Unión Europea).

10 12650/17.

EN LAS PRESENTES CONCLUSIONES

11. AGOGE FAVORABLEMENTE la Comunicación conjunta al Parlamento Europeo y al Consejo titulada: «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE», que propone un objetivo ambicioso: aumentar la ciberseguridad en la UE. Dicha Comunicación también contribuye a la autonomía estratégica de la UE mencionada en las Conclusiones del Consejo relativas a la Estrategia Global sobre Política Exterior y de Seguridad de la Unión Europea[11], ya que propone el objetivo de construir una Europa digital más segura, generadora de confianza, consciente de sus puntos fuertes, competitiva, abierta al mundo y respetuosa de los valores comunes de la UE, que propugnan una Internet abierta, libre, pacífica y segura, y, así, alcanzar un nivel más elevado de resiliencia para poder responder de manera conjunta a las ciberamenazas en toda la UE, tener un efecto preventivo y disuasorio en lo que respecta a las ciberamenazas, detectarlas y responder a ellas.

12. INVITA a los Estados miembros y a las instituciones, órganos y organismos de la UE a que trabajen conjuntamente, respetando los ámbitos de competencia de cada uno y los principios de subsidiariedad y proporcionalidad, a modo de respuesta a los objetivos estratégicos que figuran en las presentes Conclusiones, y

13. SUBRAYA la necesidad de que la UE, sus Estados miembros y el sector privado garanticen una financiación suficiente, respetando los recursos disponibles, para apoyar el refuerzo de la ciberresiliencia y de los esfuerzos de investigación y desarrollo en materia de ciberseguridad en toda la UE, así como para reforzar la cooperación a fin de tener un efecto preventivo y disuasorio en lo que respecta a las ciberamenazas, detectarlas y responder a ellas, y poder responder de manera conjunta a los incidentes cibernéticos a gran escala y a las actividades cibernéticas malintencionadas en toda la UE;

[11] 13202/16.

Capítulo I

GARANTIZAR LA CIBERRESILIENCIA EFECTIVA DE LA UE Y LA CONFIANZA EN EL MERCADO ÚNICO DIGITAL

14. SUBRAYA que la responsabilidad principal en lo que se refiere a aumentar su ciberseguridad y a dar respuesta a los ciberincidentes y cibercrisis recae en cada Estado miembro, mientras que la UE puede aportar un importante valor añadido en lo que respecta a apoyar la cooperación entre los Estados miembros. En este contexto, DESTACA que todos los Estados miembros deben dotar a las autoridades nacionales encargadas de la ciberseguridad de los recursos necesarios para que en toda la UE se prevengan y detecten ciberamenazas y ciberincidentes y se responda a ellos;

15. SUBRAYA la necesidad de recurrir, cuando sea posible, a los mecanismos, estructuras y organizaciones existentes a escala de la UE;

16. ELOGIA:

- los avances realizados en la transposición de la Directiva SRI por parte de los Estados miembros y DESTACA la necesidad de que, antes de mayo de 2018, esta se aplique plena y efectivamente, de conformidad con dicha Directiva[12];
- la labor realizada por el Grupo de cooperación SRI para incrementar la cooperación estratégica y el intercambio de información entre los Estados miembros;
- la labor realizada por la red de equipos de respuesta a incidentes de seguridad informática, especialmente en lo que respecta a reforzar la cooperación operativa de los Estados miembros, a generar confianza, a intercambiar información, a gestionar incidentes de ciberseguridad a gran escala y, sobre la base de las conclusiones nacionales de los Estados miembros, a proporcionar elementos para un conocimiento de la situación compartido a escala europea;
- la labor realizada en el marco de la asociación público-privada contractual sobre seguridad cibernética.

[12] Sin perjuicio de la competencia de los Estados miembros relativa a la transposición de la Directiva SRI, especialmente en lo que respecta a los operadores de servicios esenciales.

17. ACOGE FAVORABLEMENTE que la Comunicación conjunta haya confirmado que un cifrado fuerte y fiable es de gran importancia para garantizar adecuadamente los derechos humanos y las libertades fundamentales en la UE, así como para generar entre el público confianza en el mercado único digital, teniendo a la vez en cuenta que las fuerzas o cuerpos de seguridad necesitan acceder a determinados datos en el marco de sus investigaciones, y que haya confirmado también que los sistemas seguros de identificación y comunicación digital desempeñan un papel clave para garantizar una ciberseguridad eficaz en la UE;

18. ACOGE FAVORABLEMENTE el ambicioso plan propuesto en la Comunicación conjunta para organizar, periódicamente, unos ejercicios paneuropeos de ciberseguridad sobre la base de la experiencia de los ejercicios CyberEurope. Dichos ejercicios combinarán respuestas a distintos niveles, un elemento importante para avanzar en la preparación de los Estados miembros y las instituciones de la UE para responder a ciberincidentes a gran escala;

19. PIDE a la UE y a sus Estados miembros que lleven a cabo de manera periódica ejercicios estratégicos de ciberseguridad en las distintas formaciones del Consejo, sobre la base de la experiencia adquirida durante el EU CYBRID 2017 y

20. Sin perjuicio del resultado del proceso legislativo:

- ACOGE FAVORABLEMENTE la propuesta de otorgar a la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA) un mandato claro y permanente; su objetivo principal será apoyar y desarrollar una cooperación más estrecha entre los Estados miembros, a fin de aumentar tanto sus capacidades como la confianza en una Europa digital;

- REAFIRMA que la futura ENISA deberá basarse en la experiencia y el conocimiento experto de los Estados miembros y la UE para apoyar la elaboración y la aplicación coherentes de las políticas y normativas de ciberseguridad de la UE, actuales y futuras, garantizando además que el objetivo del desarrollo de todas sus competencias es complementar las de los Estados miembros;

- REAFIRMA el objetivo de aumentar la confianza en una Europa digital reforzando la confianza en las soluciones y las innovaciones digitales, en particular en la «Internet de las cosas», el comercio electrónico y la gobernanza electrónica, y especialmente en lo que respecta a un marco europeo de certificación de la ciberseguridad de primer orden[13]. Se trata de un requisito clave para incrementar la confianza en los productos y servicios digitales, así como su seguridad, para proteger infraestructuras críticas y datos de los Gobiernos, las empresas y los ciudadanos e imprescindible para adoptar un enfoque de seguridad desde el diseño para productos, servicios y procesos en el mercado único digital;

- DESTACA que el trabajo legislativo para reforzar la certificación de la ciberseguridad a escala de la UE tendrá que responder a las necesidades del mercado y de los usuarios, basarse en experiencias de capacidades y procesos de certificación existentes en la UE (por ejemplo, en el marco del Grupo de altos funcionarios sobre seguridad de los sistemas de información) y tendría que proporcionar un marco capaz de adaptarse rápidamente a las evoluciones digitales futuras más sofisticadas;

- DESTACA que, al reforzar la certificación de la ciberseguridad en la UE, se deberá cubrir todo el abanico de requisitos de seguridad, hasta los más elevados, es decir aquellos en los que se debe demostrar resistencia frente a las capacidades de los atacantes. Hay una serie de factores clave para alcanzar el éxito: garantizar un proceso de certificación de la seguridad fiable, transparente e independiente, para promover la disponibilidad de aparatos, programas informáticos y servicios seguros y confiables en el mercado único y más allá de sus fronteras; reconocer, mediante normas europeas e internacionales[14], los conocimientos expertos de la industria, los Gobiernos y los especialistas europeos, respectivamente; respetar el papel de los Estados miembros en el proceso de certificación, en particular en lo que respecta a la evaluación en los niveles de seguridad más elevados y especialmente respecto a la evaluación de las necesidades y capacidades de seguridad esenciales. Dicho marco de certificación debe también garantizar que cualquier programa de certificación a escala de la UE sea proporcional al nivel de seguridad necesario para el uso de los productos, servicios o sistemas TIC afectados y permita el comercio transfronterizo para que empresas de todos los tamaños desarrollen y vendan nuevos productos, tanto dentro de la UE como fuera de sus mercados.

---

13 Mediante normas internacionales, elaboradas en consonancia con el espíritu del Código de Buena Conducta del acuerdo OMC-OTC.

14 Mediante normas europeas e internacionales elaboradas en consonancia con el espíritu del Código de Buena Conducta del acuerdo OMC-OTC.

21. ACOGE FAVORABLEMENTE la intención de establecer una red de centros de competencia en ciberseguridad, a fin de estimular el desarrollo y el despliegue de tecnologías de ciberseguridad y de ofrecer un impulso adicional a la innovación para la industria europea en la escena mundial en cuanto al desarrollo de tecnologías revolucionarias y de nueva generación, como la inteligencia artificial, la computación cuántica, las cadenas de bloques y las identidades digitales seguras;

22. DESTACA la necesidad de que la red de centros de competencia en ciberseguridad incluya a todos los Estados miembros y sus centros de excelencia y competencia existentes y, teniendo esto presente, preste especial atención a la complementariedad; TOMA NOTA de la decisión de crear un Centro Europeo de Investigación en Ciberseguridad, que, ante todo, deberá centrarse en garantizar la complementariedad y evitar duplicaciones en el seno de la red de centros de competencia en ciberseguridad y con otras agencias de la UE;

23. DESTACA que la red de centros de competencia en ciberseguridad deberá abordar toda una gama de cuestiones, desde la investigación hasta la industria, y, por lo tanto, deberá contribuir, entre otras cosas, a alcanzar el objetivo de una autonomía estratégica europea;

24. Teniendo presente la red de centros de competencia en ciberseguridad propuesta, REAFIRMA la necesidad de que la UE, a través de sus Estados miembros, desarrolle una capacidad europea para evaluar el grado de seguridad de la criptografía empleada en productos y servicios a disposición de los ciudadanos, las empresas y los Gobiernos en el marco del mercado único digital, reconociendo al tiempo que las políticas relativas a la criptografía son un aspecto esencial de la seguridad nacional y, en consecuencia, son competencia de los Estados miembros;

25. INVITA a todas las partes interesadas pertinentes a aumentar las inversiones en aplicaciones de las nuevas tecnologías al ámbito de la ciberseguridad, a fin de contribuir a garantizar la ciberseguridad en todos los sectores de la economía europea;

26. DESTACA la importancia de que se presten servicios de ciberseguridad coordinados y dignos de crédito y confianza a las instituciones de la UE, e INSTA a la Comisión y a las demás instituciones de la UE a que sigan desarrollando el CERT-UE conforme a dichas finalidades y garanticen asimismo para ese fin los recursos adecuados;

27. ACOGE FAVORABLEMENTE el llamamiento a reconocer el importante papel de los investigadores de seguridad externos a la hora de descubrir vulnerabilidades en los productos y servicios, e INSTA a los Estados miembros a que pongan en común las mejores prácticas para una revelación coordinada de las vulnerabilidades;

28. DESTACA que la ciberseguridad es responsabilidad de todos, e INVITA a la UE y a sus Estados miembros a que fomenten las aptitudes digitales y la alfabetización mediática, ayudando a los usuarios a proteger su información digital en línea y concienciándolos acerca de los riesgos que conlleva poner datos personales en Internet;

29. ACOGE FAVORABLEMENTE la atención que presta la Comunicación conjunta a la educación, la ciberhigiene y la concienciación cibernética en los Estados miembros y en la UE;

30. PIDE A LA COMISIÓN que proponga de aquí a mediados de 2018 los instrumentos jurídicos correspondientes para la aplicación de la iniciativa por la que se crea una red de centros de competencia en ciberseguridad y un Centro Europeo de Competencia e Investigación en Ciberseguridad, y que ofrezca con prontitud una evaluación de impacto sobre dichos instrumentos;

31. INVITA a los Estados miembros a que:

- den prioridad a la concienciación cibernética en las campañas de información y estimulen la ciberseguridad dentro de los planes de estudios académicos, educativos y de formación profesional. Debe prestarse especial atención a la educación de los jóvenes y al fomento de sus aptitudes digitales, para crear profesionales capacitados para el futuro y preparados para los desafíos existentes en la seguridad, la economía y los servicios;

- impulsen la labor destinada a poner en marcha programas especializados de alto nivel en materia de ciberseguridad, con objeto de colmar la actual carencia de profesionales de ciberseguridad en la UE;

- creen una red de cooperación efectiva de puntos de contacto educativos bajo la égida de la ENISA. La red de puntos de contacto ha de tener como finalidad mejorar la coordinación y el intercambio entre los Estados miembros de mejores prácticas sobre educación y concienciación cibernéticas, así como de formación, ejercicios y desarrollo de capacidades;

- consideren la posibilidad de aplicar las normas de la Directiva SRI también a las administraciones públicas que participan en actividades sociales o económicas cruciales, si estas ya no están reguladas por la legislación nacional y si se considera adecuado, y ofrezcan formación relacionada con la ciberseguridad también en las administraciones públicas, dada la función que estas desempeñan en nuestra sociedad y nuestra economía.

Capítulo II

DESARROLLO DE CAPACIDADES DE LA UE PARA PREVENIR, DISUADIR, DETECTAR Y RESPONDER A LAS ACTIVIDADES CIBERNÉTICAS MALINTENCIONADAS

32. DESTACA que un incidente o ataque cibernético particularmente grave podría constituir motivo suficiente para que un Estado miembro invoque las cláusulas de solidaridad[15] o de asistencia mutua[16] de la UE;

33. SE CONGRATULA de la adopción del «marco para una respuesta diplomática conjunta de la UE a actividades cibernéticas maliciosas», que contribuye a la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio al establecer medidas del ámbito de la PESC, en particular medidas restrictivas, que pueden utilizarse para prevenir y responder a las actividades cibernéticas malintencionadas, e INSTA al SEAE y a los Estados miembros a que realicen ejercicios periódicos en relación con dicho marco;

---

15 Artículo 222 del TFUE
16 Artículo 42.7 del TFUE

34. DESTACA la necesidad de aportar una respuesta eficiente a escala de la UE respecto de incidentes y crisis cibernéticos de gran envergadura, respetando las competencias de los Estados miembros, así como la necesidad de que la ciberseguridad se integre transversalmente en los mecanismos de gestión de crisis a escala de la UE[17]. Para lograr ese objetivo, PIDE que se ejercite periódicamente la respuesta a escala de la UE a los incidentes cibernéticos de gran envergadura (que abarca desde las respuestas diplomáticas y estratégicas a las respuestas técnicas), a partir de los marcos y procedimientos correspondientes y perfeccionándolos si es necesario[18];

35. DESTACA la importancia de contar con mecanismos bien integrados de respuesta e intercambio de información entre las distintas comunidades que son esenciales para garantizar la ciberseguridad en Europa, en particular entre los organismos pertinentes de la UE y las autoridades de los Estados miembros. Dichos mecanismos deberán probarse y verificarse en el marco de los ejercicios de ciberseguridad a escala de la UE, y deberán formalizarse en los acuerdos respectivos si es necesario;

36. SEÑALA la posibilidad de que, si la Comisión presenta una propuesta para la creación de un Fondo de respuesta a emergencias en materia de ciberseguridad, en paralelo a la actividad actual de los Estados miembros y respetando los recursos disponibles (especialmente dentro del marco financiero plurianual de la UE), se estudie la ayuda a los Estados miembros para responder y mitigar incidentes cibernéticos de gran envergadura, siempre que el Estado miembro haya instaurado un sistema prudente de ciberseguridad antes del incidente, lo que supone haber aplicado plenamente la Directiva SRI y contar con marcos bien desarrollados para la gestión de riesgos y la supervisión a nivel nacional;

37. RECONOCE la vinculación cada vez mayor entre ciberseguridad y defensa, e INSTA a que se incremente la cooperación en materia de defensa cibernética, en particular fomentando la cooperación entre las comunidades civil y militar de respuesta a incidentes, y a que se siga fortaleciendo la ciberseguridad de las misiones y operaciones de la PCSD;

---

17 C/2017/ 6100 final.

18 9916/17 y C/2017/6100 final.

38. DESTACA la necesidad de plantear la posibilidad de aprovechar plenamente las iniciativas de defensa propuestas para acelerar el desarrollo de las capacidades cibernéticas adecuadas en Europa, y RECONOCE las oportunidades que brinda la posibilidad de desarrollar proyectos de defensa cibernética mediante la cooperación estructurada permanente si lo estiman necesario los Estados miembros participantes en la misma, y RECONOCE la función desempeñada por la base tecnológica e industrial de la defensa europea y por la base industrial de ciberseguridad civil más amplia a la hora de ofrecer medios para que los Estados miembros defiendan sus intereses en materia de seguridad y defensa relacionados con la cibernética;

39. TOMA NOTA de la propuesta de la Comisión de crear una plataforma de formación y educación en materia de ciberdefensa de aquí al término de 2018, y DESTACA que la plataforma debe reforzar las oportunidades de formación y educación en los Estados miembros, así como garantizar la complementariedad con otros empeños e iniciativas de la UE, en particular con la EESD y la AED;

40. INSTA a la UE y a sus Estados miembros a que sean sensibles a la amenaza que supone el uso de TIC para la apropiación indebida de propiedad intelectual, en particular secretos comerciales y otra información comercial confidencial con el fin de ofrecer ventajas competitivas a empresas o sectores comerciales;

41. RECONOCE la necesidad de abordar la cuestión de los delitos en el ciberespacio, en particular los cometidos en la red oscura, la explotación sexual infantil en línea, así como el fraude y la falsificación de medios de pago distintos del efectivo, concretamente con el fin de crear una imagen de inteligencia mejorada, llevar a cabo investigaciones conjuntas y compartir apoyo operativo;

42. ACOGE FAVORABLEMENTE la labor realizada por la UE y sus Estados miembros a la hora de afrontar los desafíos planteados por los sistemas que permiten a los delincuentes y terroristas comunicarse por medios inaccesibles a las autoridades competentes, DESTACA que esta labor ha de tener en mente que un cifrado fuerte y confiable es de gran importancia para la ciberseguridad y para la confianza en el mercado único digital, así como para garantizar el respeto de los derechos humanos y las libertades fundamentales;

43. SUBRAYA la importancia de ofrecer a los servicios policiales instrumentos que permitan detectar, investigar y enjuiciar la ciberdelincuencia, de manera que los delitos cometidos en el ciberespacio no pasen desapercibidos ni queden impunes, y ACOGE FAVORABLEMENTE la contribución de la Red judicial europea sobre ciberdelincuencia a la lucha contra la delincuencia mediante la cooperación entre las autoridades judiciales;

44. DESTACA la importancia de garantizar una posición coordinada de la UE para definir eficientemente las decisiones de gobernanza en Internet a nivel europeo y mundial dentro de la comunidad de múltiples interesados, como puede ser la de garantizar unas bases de datos WHOIS de direcciones IP y de nombres de dominio que sean rápidamente accesibles y exactas, de modo que se defiendan las capacidades policiales y los intereses públicos;

45. DESTACA la importancia de adoptar el Protocolo Internet IPv6, que es vital para el desarrollo de la «Internet de las cosas» en su nivel, así como para mejorar la atribución de los delitos en el ciberespacio;

46. ALIENTA los actuales trabajos relativos al acceso transfronterizo a las pruebas electrónicas, a la retención de datos y a las dificultades que plantean para los procedimientos penales los sistemas que permiten a los delincuentes y terroristas comunicarse por medios inaccesibles a las autoridades competentes, teniendo presente la necesidad de respetar los derechos humanos y las libertades fundamentales, así como la protección de datos;

47. INSTA a la Comisión a que:

- presente de aquí a diciembre de 2017 un informe de situación sobre la aplicación de las medidas prácticas para mejorar el acceso transfronterizo a las pruebas electrónicas;
- presente a comienzos de 2018 una propuesta legislativa destinada a mejorar el acceso transfronterizo a las pruebas electrónicas;

48. INVITA a Europol, la ENISA y Eurojust a que:

- sigan fortaleciendo su cooperación en la lucha contra la ciberdelincuencia, tanto entre sí como con otras partes interesadas pertinentes, como la comunidad de los CSIRT, Interpol, el sector privado y el mundo universitario, creando sinergias y complementariedades, de conformidad con sus respectivos mandatos y competencias;

- contribuyan conjuntamente con los Estados miembros a un enfoque coordinado de la respuesta policial de la UE a los incidentes y crisis cibernéticos de gran envergadura con objeto de complementar los procedimientos expuestos en los marcos correspondientes[19];

49. INVITA a la UE y a sus Estados miembros a que sigan trabajando:

- para suprimir los obstáculos a la investigación del delito y a la justicia penal efectiva en el ciberespacio, así como para fomentar la cooperación y la coordinación internacionales en la lucha contra la delincuencia en el ciberespacio;

- para afrontar los desafíos que plantean las tecnologías de anonimización, teniendo en mente que un cifrado fuerte y confiable es de gran importancia para la ciberseguridad y para la confianza en el mercado único digital;

- para definir las decisiones de gobernanza en Internet que afectan a la capacidad policial para luchar contra la delincuencia en el ciberespacio.

[19] 9916/17 y C/2017/6100 final.

Capítulo III

REFUERZO DE LA COOPERACIÓN INTERNACIONAL EN FAVOR DE UN CIBERESPACIO MUNDIAL ABIERTO, LIBRE, PACÍFICO Y SEGURO

50. RECONOCE que garantizar la ciberseguridad es un desafío mundial, que exige una cooperación mundial efectiva entre todos los actores, y RECONOCE que ha de hacerse especial hincapié en defender los valores democráticos y los principios de un ciberespacio mundial abierto, libre, pacífico y seguro, y teniendo esto presente,

51. INSTA a la UE y a sus Estados miembros a que fomenten la creación de un marco estratégico para la prevención de conflictos, la cooperación y la estabilidad en el ciberespacio que esté basado en la aplicación del Derecho internacional vigente, y en particular de la Carta de las Naciones Unidas en su totalidad, y también el desarrollo y la aplicación de normas universales de comportamiento responsable del Estado y medidas regionales de fomento de la confianza entre Estados;

52. RECONOCE la función que corresponde a las Naciones Unidas a la hora de elaborar las normas de comportamiento responsable del Estado en el ciberespacio, y recuerda que los resultados de los debates mantenidos en el Grupo de Expertos Gubernamentales de las Naciones Unidas, a lo largo de los años, han ido configurando un conjunto de normas y recomendaciones consensuadas[20], que la Asamblea General ha refrendado en reiteradas ocasiones y que los Estados deben tomar como base para el comportamiento responsable del Estado en el ciberespacio;

53. RECONOCE que entre esas normas de comportamiento responsable del Estado en el ciberespacio se halla el que los Estados no permitan a sabiendas que su territorio se utilice para cometer actos ilícitos a nivel internacional, respondan a las solicitudes adecuadas de asistencia formuladas por otro Estado cuyas infraestructuras críticas sean objeto de actos malintencionados de TIC surgidos en su territorio y tomen las medidas adecuadas para proteger sus infraestructuras críticas de las amenazas de TIC;

54. RECONOCE las amenazas y riesgos cibernéticos comunes a que se enfrentan la UE, la OTAN y sus respectivos Estados miembros, y REITERA la importancia de proseguir la cooperación UE-OTAN en materia de ciberseguridad y defensa, respetando plenamente los principios de participación, reciprocidad y autonomía en el proceso decisorio de la UE, y de conformidad con sus Conclusiones de 6 de diciembre de 2016 sobre la aplicación de la Declaración conjunta del presidente del Consejo Europeo, el presidente de la Comisión Europea y el secretario general de la Organización del Tratado del Atlántico Norte[20];

55. INSTA a la UE y a sus Estados miembros a que apoyen y propicien el desarrollo de medidas regionales de fomento de la confianza, que constituyen un elemento esencial para aumentar la cooperación y la transparencia y reducir el riesgo de conflictos. Llevar a la práctica medidas de fomento de la confianza en materia de ciberseguridad en la OSCE y en otros contextos regionales hará que sea más predecible el comportamiento del Estado y contribuirá aún más a estabilizar el ciberespacio;

56. REAFIRMA que la UE seguirá defendiendo sus valores esenciales en la protección de los derechos humanos y las libertades fundamentales, basándose en las Directrices de la UE sobre derechos humanos relativas a la libertad de expresión en Internet. La UE destaca asimismo la importancia de que participen en la gobernanza de Internet todos los interesados, en particular el mundo universitario, la sociedad civil y el sector privado;

57. INSTA a la UE y a sus Estados miembros a que fomenten el desarrollo de las competencias cibernéticas en terceros países, dando especial prioridad a los vecinos de la UE y a los países en desarrollo que están experimentando una conectividad en rápido aumento, para afrontar la ciberdelincuencia y consolidar la ciberresiliencia, de acuerdo con los valores esenciales de la UE. Con objeto de impulsar los trabajos de la UE en este ámbito, debe crearse una red dedicada al desarrollo de las competencias cibernéticas de la UE y unas directrices para el desarrollo de la capacidad cibernética de la UE que han de ser complementarias respecto de los mecanismos y estructuras existentes;

---

[20] 15283/16.

58. PONE DE RELIEVE los avances logrados en la cooperación UE-OTAN en materia de defensa y seguridad cibernéticas, y el desarrollo de dicha cooperación en la formación, la educación y los conceptos, evitando la innecesaria duplicación de esfuerzos cuando coinciden necesidades, así como fomentando la interoperabilidad mediante requisitos y normas de defensa cibernética, e INSTA a que continúe la cooperación en los ejercicios de defensa cibernética (a nivel de personal) y se pongan en común las mejores prácticas en relación con la gestión de crisis, evitando la innecesaria duplicación de esfuerzos cuando coinciden necesidades, y respetando plenamente el marco estratégico de ejercicios de la UE y los principios de participación, reciprocidad y autonomía en el proceso decisorio de la UE;

59. RECONOCE que el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) ofrece una norma jurídica efectiva para configurar la legislación nacional en materia de ciberdelincuencia. INSTA s todos los países a que diseñen marcos jurídicos nacionales adecuados y lleven a cabo la cooperación dentro de ese marco internacional existente que ofrece el Convenio de Budapest;

60. RECUERDA los logros obtenidos con los diálogos bilaterales mantenidos por la UE en materia cibernética, y pide que se siga trabajando para facilitar la cooperación con terceros países en materia de ciberseguridad;

61. RECUERDA que la UE cuenta con un mecanismo de control de las exportaciones, sólido y jurídicamente vinculante, basado en las decisiones y mejores prácticas establecidas en los sistemas internacionales de no proliferación, y TOMA NOTA de los debates que actualmente tienen lugar en el Consejo para hallar el mejor modo de mejorar aún más el funcionamiento de dichos controles, e INVITA a los Estados miembros a seguir estudiando, en los regímenes internacionales pertinentes de control de las exportaciones (por ejemplo, el Arreglo de Wassenaar), las aplicaciones críticas de ciberseguridad de las nuevas tecnologías, con objeto de garantizar un control efectivo de las tecnologías criticas de ciberseguridad del mañana.

62. En aplicación de las Conclusiones del Consejo Europeo de 19 de octubre de 2017[21], las presentes Conclusiones se llevarán a la práctica mediante un plan de acción que será adoptado por el Consejo antes del término de 2017. El plan de acción será un documento vivo que el Consejo revisará y actualizará periódicamente.

---

[21] EUCO 14/17.