CONSEJO DE LA UNIÓN EUROPEA

Bruselas, 22 de julio de 2013
(OR. en)

12109/13

POLGEN 138
JAI 612
TELECOM 194
PROCIV 88
CSC 69
CIS 14
RELEX 633
JAIEX 55
RECH 338
COMPET 554
IND 204
COTER 85
ENFOPOL 232
DROIPEN 87
CYBER 15
COPS 276
POLMIL 39
COSI 93
DATAPROTECT 94

RESULTADO DE LOS TRABAJOS

De:	Secretaría General del Consejo
A:	Delegaciones
N.º doc. prec.:	11357/13
Asunto:	Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro"

Se remiten adjuntas, a la atención de las Delegaciones, las conclusiones del Consejo sobre la comunicación conjunta de la Comisión y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad titulada "Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro", acordadas por el Consejo de Asuntos Generales el 25 de junio de 2013.

ANEXO

Conclusiones del Consejo sobre la comunicación conjunta de la Comisión y de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad, titulada "Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro"

El Consejo de la Unión Europea,

1. RECONOCIENDO que el ciberespacio, que tiene una naturaleza inherentemente transnacional, consta de una serie de redes e infraestructuras interdependientes, por ejemplo, entre otras, la Internet y las redes de telecomunicación, constituye uno de los canales presentes y futuros más importantes para satisfacer las necesidades, intereses y derechos de los ciudadanos de la UE y de sus Estados miembros y constituye un activo indispensable del crecimiento económico de la UE.

2. SUBRAYANDO la importancia del papel y los derechos de los ciudadanos individuales, del sector privado y de la sociedad civil en las cuestiones relacionadas con el ciberespacio, así como el importante cometido de la UE para apoyar y mantener un ciberespacio resiliente, abierto y seguro basado en los valores fundamentales de la UE, como la democracia, los derechos humanos y el Estado de Derecho, para nuestras economías, las administraciones y la sociedad en general, así como para el correcto funcionamiento del mercado interior.

3. RECONOCIENDO la necesidad de mejorar la confidencialidad, disponibilidad e integridad de las redes y la infraestructura de la información contenida en ellas.

4. RECONOCIENDO que deben crearse salvaguardias y adoptarse medidas para evitar las amenazas asociadas a las redes interdependientes o perjudiciales para las mismas y para las infraestructuras de la información, así como proteger el ciberespacio, tanto en el ámbito civil como el militar

5. REAFIRMANDO la posición de la UE de que las mismas normas, principios y valores que propugna la UE en todos los demás terrenos, en particular en su Carta de los Derechos Fundamentales de la Unión Europea, deberán aplicarse asimismo en el ciberespacio.

6. RECONOCIENDO que el Derecho internacional, incluidos convenios internacionales como el Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) y los correspondientes convenios en materia de Derecho humanitario y derechos humanos, como el Pacto Internacional de Derechos Civiles y Políticos, el Pacto internacional relativo a los derechos económicos, sociales y culturales, proporcionan un marco jurídico aplicable al ciberespacio. Por todo ello, deberá procurarse que dichos instrumentos sean también de aplicación en el ciberespacio; en consecuencia, la UE no defiende la creación de nuevos instrumentos jurídicos internacionales para abordar las cuestiones relacionadas con el ciberespacio.

7. AFIRMANDO que la ciberseguridad debe abordarse de un modo integrado, multidisciplinar y horizontal y que tales medias deberán abarcar un amplio rango de asuntos que afectan al ciberespacio.

8. RECORDANDO las numerosas iniciativas de la UE e internacionales en el ámbito del ciberespacio, por ejemplo las que figuran en el Anexo del presente documento,

9. RECORDANDO las disposiciones del artículo 222 del Tratado de Funcionamiento de la Unión Europea y tiene en cuenta los debates en curso sobre su aplicación,

10. CONSCIENTE de que tanto los esfuerzos para aumentar la ciberseguridad como la lucha contra la ciberdelincuencia deben desplegarse no solo en el interior de la Unión Europea sino también en terceros países, por ejemplo en aquellos desde los que operan las organizaciones de ciberdelincuentes,

EN LAS PRESENTES CONCLUSIONES

11. SE FELICITA por la comunicación conjunta de la Comisión y el Alto Representante de la UE sobre una Estrategia de ciberseguridad de la Unión Europea,

12. CONSIDERA esencial y urgente impulsar y aplicar un planteamiento general de la política ciberespacial de la UE que:

- proteja y promueva el disfrute de los derechos humanos y esté basado en los valores fundamentales de la democracia, los derechos humanos y el Estado de Derecho,

- permita aumentar la prosperidad europea y las ventajas sociales y económicas del ciberespacio, por ejemplo la Internet,

- promueva una ciberseguridad eficaz y mejorada en toda la UE y más allá de sus fronteras,

- permita avanzar en el empeño por colmar la brecha digital mundial y promover la cooperación internacional en materia de ciberseguridad,

- refleje el papel y los derechos de los ciudadanos individuales, del sector privado y la sociedad civil en cuestiones del ciberespacio, inclusive una mejora de la cooperación pública-privada y el intercambio de información,

E

13. INVITA a los Estados miembros, la Comisión y el Alto Representantes a trabajar conjuntamente, respetando las correspondientes competencias de los demás y el principio de subsidiariedad, en respuesta a los objetivos estratégicos que figuran en las presentes conclusiones.

Valores

14. SUBRAYA que los derechos humanos de los individuos, entre ellos el derecho a la libertad de expresión y el derecho a la intimidad, deben respetarse en todo momento cuando se pongan a punto la política y las prácticas relativas al ciberespacio, así como en la correspondiente legislación, y toma nota de las negociaciones en curso para acordar un marco jurídico de la UE sobre protección de datos personales que puedan funcionar de forma efectiva en el ciberespacio,

15. RECONOCE que los valores e intereses promovidos y protegidos en el seno de la Unión deberían también impulsarse en sus políticas exteriores relacionadas con cuestiones del ciberespacio,

16. LLAMA a la UE y a sus Estados miembros a:

- defender una posición única y firme en relación con la aplicabilidad universal de los derechos humanos y las libertades fundamentales, inclusive las libertades de opinión, expresión, información, reunión y asociación en el ciberespacio,

- establecer el modo en que deberán aplicarse las obligaciones existentes en el ciberespacio,

17. INVITA a la UE y a sus Estados miembros a fomentar la alfabetización digital y a ayudar a los usuarios a mejorar su grado de sensibilización con sus responsabilidad individual cuando coloquen datos personales en la Internet.

18. SUBRAYA el importante papel de la UE en el mantenimiento del modelo multisectorial de gestión de la Internet,

19. INVITA a los Estados miembros a adoptar todas las medidas razonables para garantizar que todos los ciudadanos de la UE estén en condiciones de acceder a la Internet y disfrutar de sus ventajas.

Prosperidad

20. INVITA a la Comisión a desplegar un esfuerzo especial para promover el mercado único digital y hacer avanzar las cuestiones conexas en el seno de la Unión y en los foros internacionales (por ejemplo, la Organización Mundial del Comercio y las negociaciones sobre el Acuerdo sobre Tecnología de la Información) así como garantizar el acceso al mercado en dichos sectores cuando se negocien acuerdos de libre comercio con terceros países,

21. SUBRAYA la importancia de que la legislación en este sector sea tecnológicamente neutra y anima a propiciar la neutralidad en la red en la mayor medida posible, con el fin de no obstaculizar la competencia al discriminar el comercio transfronterizo en línea y los nuevos modelos de negocio,

22. SE FELICITA por el reconocimiento concedido a la necesidad de invertir en investigación y desarrollo en el ámbito del ciberespacio, como un sector importante que podría aportar la creación de empleos de calidad y crecimiento económico,

23. SUBRAYA:

- la importancia fundamental de que la UE posea un sector de las tecnologías de la información y la comunicación (TIC) y un sector de seguridad de las TIC dinámicos y que refuercen la ciberseguridad e INVITA a los Estados miembros y a la Comisión a explorar y comunicar qué tipo de medidas podrían adoptarse para apoyar su desarrollo,

- la legislación en apoyo de la ciberseguridad debería fomentar la innovación y el crecimiento, centrándose en la protección de las infraestructuras y funciones vitales que los Estados miembros consideren esenciales,

- la economía digital debe ser un motor esencial de crecimiento, innovación y empleo, y la ciberseguridad es esencial para proteger la economía digital,

- la importancia a escala nacional de la protección de infraestructuras críticas de información(CIIP).

Lograr la ciberresiliencia

24. SE FELICITA de los objetivos de la propuesta de Directiva de la Comisión por la que establecen medidas para mejorar:

    - la seguridad de las redes y de la información en la UE,
    - la preparación en materia de ciberseguridad y las capacidades a escala nacional,
    - la cooperación entre los Estados miembros y en la UE y el impulso de unos hábitos de gestión del riesgo en los sectores público y privado,

25. ANIMA a todas las instituciones, órganos y organismos de la UE, en cooperación con los Estados miembros, a que tomen las medidas necesarias para garantizar su propia ciberseguridad, reforzando su seguridad de acuerdo con sus normas pertinentes en la materia, en cooperación con ENISA con el fin de introducir las mejores prácticas, de conformidad con el Reglamento (UE) n.° 526/2013[1],

26. RECUERDA que se ha creado un equipo de respuesta a emergencias informáticas (CERT) para las instituciones, órganos y organismos de la UE tras una fase piloto de un año en la que se evaluó satisfactoriamente su cometido y su eficacia,

27. SUBRAYA la importancia esencial de ENISA para apoyar los esfuerzos de los Estados miembros y de la Unión por lograr un elevado nivel de seguridad de la red y la información, en particular apoyando el desarrollo de capacidades de los Estados miembros e impulsando sólidas capacidades nacionales de resiliencia cibernética, los ejercicios ciberespaciales europeos y los esfuerzos de la Unión en materia de I&D y de normalización, e INVITA a ENISA a cooperar con otras instituciones, órganos y organismos de la UE en materias relacionadas con el NIS, de conformidad con el Reglamento (UE) n.° 526/2013,

[1] DO L 165 de 18.6.2013.

28. SUBRAYA la necesidad de aumentar la resiliencia de las infraestructuras vitales a escala de la UE y de reforzar una estrecha cooperación y coordinación entre los principales interesados, incluso entre los agentes civiles y militares, en particular entre el sector público y privado, para responder a incidentes y desafíos en materia de ciberseguridad, mediante iniciativas como la creación de normas comunes, el aumento de la sensibilización, la formación y la educación y revisiones y ensayos permanentes (o desarrollo) de mecanismos de alerta y respuesta precoz. Para enfrentarse con eficacia a los retos cibernéticos y en particular la gestión de los incidentes es también importante estrechar la cooperación y la coordinación a la hora de actuar ante incidentes cibernéticos por parte de los agentes de defensa, de los cuerpos de seguridad, del sector privado y de las autoridades de ciberseguridad;

29. INVITA a los Estados miembros:

- a dar los pasos necesarios para garantizar el logro de un nivel nacional de ciberseguridad eficiente, impulsando y aplicando las adecuadas medidas y capacidades organizativas y operativas con el fin de proteger el sistema de información en el ciberespacio, en particular las consideradas esenciales,

- a comprometerse con la industria y la Universidad a estimular la confianza como componente esencial de la ciberseguridad nacional, por ejemplo estableciendo asociaciones público-privadas,

- a apoyar la mejora en la sensibilización sobre la naturaleza de las amenazas y los elementos fundamentales de unas adecuadas prácticas digitales a todos los niveles,

- a ayudar a los propietarios y proveedores de sistemas TIC a que protejan sus propios sistemas y los servicios vitales que prestan,

- a fomentar la cooperación paneuropea en materia de ciberseguridad, en particular impulsando el desarrollo de ejercicios paneuropeos en la materia,

- a garantizar una cooperación y coordinación efectivas entre los Estados miembros a escala de la UE para conseguir establecer una evaluación común de las amenazas,

- a reforzar y ampliar la cooperación entre los Estados miembros y los usuarios de la UE, aprovechando las estructuras existentes,

- a tener en cuenta los problemas ligados a la ciberseguridad a la luz de los trabajos en curso sobre la cláusula de solidaridad.

La ciberdelincuencia

30. RECONOCE las conclusiones del Consejo, adoptadas en la sesión del Consejo JAI del 6 y 7 de junio de 2013, en las que se determinaban las prioridades de la UE para la lucha contra la delincuencia grave y organizada entre 2014 y 2017 y se establecía como una prioridad la lucha contra la ciberdelincuencia.

31. SUBRAYA que la evaluación de la amenaza de la delincuencia grave y organizada (SOCTA) de 2013 de Europol considera la ciberdelincuencia como un ámbito delictivo que plantea una amenaza cada vez mayor a la UE en forma de violación de datos, fraude en línea y explotación sexual de menores a gran escala, al tiempo que los beneficios procedentes de la ciberdelincuencia se está convirtiendo en un factor clave para otras actividades delictivas.

32. ELOGIA la creación del Centro Europeo de Ciberdelincuencia en Europol e INVITA a los Estados miembros a utilizar dicho Centro como un medio para reforzar la cooperación entre las agencias nacionales en el marco de sus mandatos.

33. INVITA a Europol y a Eurojust a que continúen reforzando su colaboración con todas las partes afectadas, en particular las agencias de la UE, Interpol, la comunidad de equipos de respuesta a emergencias informáticas (CERT) y el sector privado en la lucha contra la ciberdelincuencia, haciendo especial hincapié en las sinergias y complementariedades de acuerdo con sus respectivos mandatos y competencias.

34. PREVÉ la rápida ratificación del Convenio de Budapest sobre la Ciberdelincuencia por todos los Estados miembros.

35. PIDE a la Comisión, a Europol, a CEPOL y a la ENISA que ayuden a la formación y mejora de las competencias de los Estados miembros en los que es necesario reforzar las capacidades cibernéticas de las autoridades gubernamentales y fuerzas de seguridad para combatir la ciberdelincuencia.

36. INVITA a la Comisión a que:

- ayude a los Estados miembros que así lo pidan a detectar las lagunas y reforzar su capacidad para investigar y combatir la ciberdelincuencia.

- utilice el Fondo de Seguridad Interior (FSI), dentro de sus límites presupuestarios (teniendo en cuenta el resto de sus prioridades), para apoyar a las autoridades competentes en la lucha contra la ciberdelincuencia;

- utilice el Instrumento de Estabilidad para reforzar la lucha contra la ciberdelincuencia, así como las iniciativas de consolidación de las capacidades, en particular la cooperación policial y judicial en países terceros a partir de los cuales operan las organizaciones dedicadas a la ciberdelincuencia:

- facilite la coordinación de los programas de consolidación de las capacidades para evitar las duplicaciones y mejorar las sinergias;

- proporcione información sobre el avance de la Alianza Mundial contra el abuso sexual de menores en línea;

- siga facilitando el seguimiento del marco político de la UE relacionado con la lucha contra la ciberdelincuencia, en particular a la luz de los resultados y de la información estratégica proporcionada por Europol (EC3);

- siga facilitando la cooperación transcomunitaria, en particular apoyando a Europol (EC3).

Política común de seguridad y defensa (PCSD)

37. En el marco de la PCSD, DESTACA:

- la necesidad urgente de aplicar y hacer avanzar la PCSD en relación con los aspectos de ciberdefensa de la estrategia para desarrollar un marco de ciberdefensa, si procede, y definir las medidas concretas al respecto, también con miras al debate del Consejo Europeo sobre seguridad y defensa previsto para diciembre de 2013. Se debería de designar un único punto de contacto en el SEAE para guiar estos esfuerzos;

- la necesidad de mejorar las capacidades de ciberdefensa de los Estados miembros, en particular mediante el desarrollo de normas comunes, y de la concienciación a través de la formación y educación en ciberseguridad, utilizando los recursos de la Escuela Europea de Seguridad y Defensa y mejorando las oportunidades de formación y de prácticas para los Estados miembros;

- utilizar los mecanismos existentes de aprovechamiento común y compartido y las sinergias con las políticas a escala de la UE para consolidar las capacidades necesarias de ciberdefensa en los Estados miembros de las manera más eficaz posible;

- la necesidad de investigación y desarrollo. Es prioritario alentar a los Estados miembros a desarrollar tecnologías seguras y resistentes respecto de la ciberdefensa, con una importante participación del sector privado y del mundo académico, y a reforzar los aspectos de ciberdefensa en los proyectos de investigación de la Agencia Europea de Defensa (AED) basándose en un enfoque de colaboración y como un ejemplo ilustrativo de una capacidad de doble uso que ha de coordinarse entre la AED y la Comisión en el marco europeo de cooperación;

- se deberán revisar los mecanismos de alerta y respuesta precoz y verificar a la luz de las nuevas amenazas cibernéticas, mediante el diálogo entre el SEAE, la ENISA, EC3. AED, la Comisión y los Estados miembros con vistas a procurar sinergias y enlaces con la comunidad de defensa.

- la necesidad de procurar y reforzar la cooperación entre la UE y la OTAN sobre ciberdefensa, determinando las prioridades de una cooperación continua sobre ciberdefensa UE-OTAN en el marco existente, en particular participando los miembros de una institución en los ejercicios y en la formación de ciberdefensa de la otra institución y a la inversa.

- incluír los aspectos de ciberdefensa en una política más general de ciberespacio.

Industria/Tecnología

38. RECONOCIENDO la necesidad de que Europa siga desarrollando sus recursos industriales y tecnológicos para lograr un nivel suficiente de diversidad y confianza en el marco de sus redes y sistemas TIC, el Consejo ACOGE CON GRAN SATISFACCIÓN el llamamiento en la estrategia de ciberseguridad de la UE de que Europa apoye una firme política industrial, para promover la fiabilidad de las TIC europeas y de la industria de la ciberseguridad e impulsar el mercado interior a través de la I&D.

39. INVITA a los Estados miembros, la Comisión y la ENISA a redoblar sus esfuerzos en investigación y desarrollo en el ámbito de las TIC y la ciberseguridad, así como la disponibilidad de buenos profesionales sobre ciberseguridad, cosa que es esencial para promover la competitividad de las tecnologías de la información y la comunicación europeas (TIC), las industrias de servicios y seguridad, y su capacidad para desarrollar soluciones fiables y seguras, por ello el Consejo ALIENTA a la Comisión a impulsar el Programa Marco de Investigación e Innovación ("Horizonte 2020").

40. HACE HINCAPIÉ en que el desarrollo de asociaciones público-privadas será un instrumento importante para mejorar las capacidades de ciberseguridad; y, por ello, PIDE a la Comisión que fomente las sinergias en el marco de H2020 entre los operadores de infraestructuras críticas, las TIC y la investigación de seguridad en el ámbito de la ciberseguridad y la ciberdelincuencia y con las políticas de la Unión relativas a la seguridad interna y externa.

41. PIDE a los Estados miembros y a la Comisión que adopten medidas específicas para apoyar la ciberseguridad en las empresas pequeñas y medianas, las cuales son especialmente vulnerables a ataques informáticos, y alienta a los Estados miembros a desarrollar tecnologías seguras y resilientes de ciberseguridad con la colaboración del sector privado y del mundo académico.

42. INVITA a la Comisión a que tome en consideración las normas existentes en el ámbito de la ciberseguridad y SUBRAYA que la cooperación y el intercambio de información sobre normas -por ejemplo, sobre gestión de riesgos- debe seguir desarrollándose en cooperación con los Estados miembros y la industria y otros agentes pertinentes.

Cooperación internacional en el ámbito del ciberespacio

43. REITERA el compromiso de la UE de apoyar el desarrollo de medidas de fomento de la confianza en la ciberseguridad, de aumentar la transparencia y reducir el riesgo de que se malinterprete la manera de actuar de los Estados promoviendo el establecimiento de normas internacionales en este ámbito.

44. PIDE a la Comisión y a la Alta Representante que de conformidad con los procedimientos establecidos en los Tratados:

- a) promuevan el Convenio de Budapest como modelo para la elaboración de la legislación nacional sobre ciberdelincuencia y base de la cooperación internacional en este ámbito; b) promuevan el respeto de los derechos fundamentales en el ciberespacio y c) aprovechen plenamente todos los instrumentos de cooperación internacional disponibles para desarrollar la lucha contra la ciberdelincuencia así como la cooperación policial y judicial al respecto con países terceros a partir de los cuales operan las organizaciones dedicadas a la ciberdelincuencia.

- procurarse los conocimientos especializados en política de ciberseguridad de los Estados miembros y sus experiencias de los compromisos o de la cooperación bilateral para elaborar mensajes de la UE comunes sobre el ciberespacio y trabajar estrechamente con los Estados miembros sobre los aspectos operativos.

- en cooperación con los Estados miembros y las organizaciones privadas pertinentes y la sociedad civil, hacer pleno uso de los instrumentos de ayuda de la UE para la capacitación en TIC, en particular en ciberseguridad.

45. PIDE a los Estados miembros, la Comisión y la Alta Representante que se esfuercen en lograr una política internacional en materia de ciberespacio de la UE coherente, de conformidad con los procedimientos pertinentes establecidos en los Tratados:

- reforzando su compromiso con los socios y las organizaciones internacionales clave de tal manera que se garantice que todos los Estados miembros pueden beneficiarse plenamente de dicha cooperación.

- integrando las cuestiones de ciberseguridad en la PESC.

- mejorando la coordinación de las cuestiones mundiales de la ciberseguridad e integrándolas en el resto de las políticas, en particular mediante medidas de creación de confianza y de transparencia en el marco general de las relaciones con terceros países y con organizaciones internacionales, en particular mediante una coordinación reforzada entre los Estados miembros, la Comisión y el SEAE respecto al mantenimiento de diálogos y otras actividades sobre ciberseguridad.

- mejorando la coordinación a través de los órganos preparatorios pertinentes del Consejo (incluido el Grupo de Amigos de la Presidencia (FoP) sobre cuestiones cibernéticas).

- respaldando el desarrollo de capacidades en terceros países, mediante la formación y asistencia para la creación de las políticas, estrategias e instituciones nacionales pertinentes, con miras a permitir el desarrollo pleno del potencial económico y social de las TIC, respaldando el desarrollo de sistemas resilientes en esos países y reduciendo los riesgos cibernéticos pare las instituciones de la UE y los Estados miembros, haciendo uso al mismo tiempo de las redes y foros existentes para la coordinación política y el intercambio de información.

Funciones y responsabilidades respectivas

46. PIDE a los demás agentes (el sector privado, las comunidades técnicas y académicas, la sociedad civil y al ciudadano particular), que asuman sus respectivas funciones y responsabilidades para lograr un ciberespacio abierto, libre y seguro.

47. PIDE a la Comisión y a la Alta Representante que las actividades europeas se conciban de manera que sean compatibles con las estructuras, el Derecho constitucional y las iniciativas nacionales relativas a la ciberseguridad, a fin de garantizar un enfoque integrado y de evitar duplicaciones.

Y

48. PIDE a la Comisión y a la Alta Representante que elaboren un informe de situación sobre la estrategia de ciberseguridad que deberá presentarse en la Conferencia de alto nivel que se celebrará en febrero de 2014. y PROPONE que se mantengan reuniones periódicas de los órganos preparatorios competentes del Consejo (en particular del Grupo "Amigos de la Presidencia" sobre cuestiones cibernéticas) para ayudar al establecimiento de las prioridades cibernéticas y los objetivos estratégicos de la UE, como parte del marco político general, y para revisar y respaldar la aplicación en curso de la estrategia.

49. Para la aplicación de las presentes conclusiones del Consejo únicamente se utilizarán los fondos y los programas financieros existentes, sin perjuicio de las negociaciones sobre el futuro marco financiero y, por ello, el Consejo INVITA a la Comisión a presentar la financiación de la estrategia, teniendo en cuenta las próximas negociaciones con el Parlamento Europeo.

ANEXO DEL ANEXO

Referencias

1. Parlamento Europeo, Consejo y Comisión

   – Carta de los Derechos Fundamentales de la Unión Europea[2]

2. Parlamento Europeo y Consejo

   – Reglamento (CE) no 460/2004 del Parlamento Europeo y del Consejo de 10 de marzo de 2004 por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información[3]

   – Directiva 2002/21/CE del Parlamento Europeo y del Consejo de 7 de marzo de 2002 relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (Directiva marco), modificada por la Directiva 2009/140/CE[4]

3. Parlamento Europeo

   – Resolución del Parlamento Europeo, de 11 de diciembre 2012, sobre una Estrategia de libertad digital en la política exterior de la UE

   – el informe del Parlamento Europeo sobre Informe sobre ciberseguridad y ciberdefensa de 2012

4. Consejo

   – Programa de Estocolmo – Una Europa abierta y segura que sirva y proteja al ciudadano[5]

   – Una Europa segura en un mundo mejor – Estrategia Europea de Seguridad, 12 de diciembre de 2003[6]

---

2 DO C 364 de 18.12.2010, p. 1.
3 DO L 077 de 13.03.2004.
4 DO L 108 de 24.4.2002 y DO L 337/37 de 18.12.2009
5 Doc. 17024/09 CO EUR PREP 3 JAI 896 POLGEN 229
6 Doc. 15849/03 PESC 783

– Estrategia de Seguridad Interior de la Unión Europea: "Hacia un modelo europeo de seguridad"[7]

– Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección[8]

– Conclusiones del Consejo sobre la Comunicación de la Comisión titulada "La Estrategia de Seguridad Interior de la UE en acción"[9]

– Conclusiones del Consejo sobre la Comunicación de la Comisión sobre la protección de infraestructuras críticas de información: ("Logros y próximas etapas: hacia la ciberseguridad global"´)[10]

– Conclusiones del Consejo sobre la determinación de las prioridades de la UE para la lucha contra la delincuencia grave y organizada entre 2014 y 2017[11]

– Conclusiones del Consejo sobre la creación de un Centro Europeo de Ciberdelincuencia[12]

7 Doc. 5842/2/10 JAI 90
8 DO L 345 de 23.12.2008.
9 Doc. 6699/11 JAI 124
10 Doc. 10299/11 TELECOM 71 DATAPROTECT 55 JAI 332 PROCIV 66 Esta comunicación es posterior a la Comunicación de la Comisión sobre Protección de Infraestructuras Críticas de Información "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia" (doc. 8375/09).
11 Doc. 9849/13 JAI 407 COSI 62 ENFOPOL 151 CRIMORG 77 ENFOCUSTOM 89 PESC 569 RELEX 434.
12 Doc. 10603/12 ENFOPOL 154 TELECOM 116

– Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a los ataques contra los sistemas de información, por la que se sustituye la Decisión marco 2005/222/JAI 89 del Consejo. Aprobación del texto transaccional definitivo con vistas a un acuerdo con el Parlamento Europeo en primera lectura[13]

– Conclusiones del Consejo relativas a la Estrategia europea en favor de una Internet más adecuada para los niños[14]

– Conclusiones del Consejo sobre la lucha contra el abuso sexual y la explotación sexual de los niños y la pornografía infantil en internet - Mejora de la eficacia de la actuación policial en los Estados miembros y en terceros países[15]

– Conclusiones del Consejo sobre una Alianza Mundial contra el abuso sexual de menores en línea[16]

– Conclusiones del Consejo relativas a una estrategia de trabajo concertada y a medidas concretas contra la delincuencia informática[17] y conclusiones del Consejo sobre un plan de acción para aplicar la estrategia concertada contra la delincuencia informática[18]

– Orientación general parcial del Consejo sobre la propuesta de Reglamento de la Comisión por el que se establece Horizonte 2020, Programa Marco de Investigación e Innovación (2014-2020)[19]

– Acción Común del Consejo relativa a la creación de la Agencia Europea de Defensa[20]

---

13 Doc. 11399/12 DROIPEN 79 TELECOM 126 CODEC 1673

14 Doc. 15850/12 AUDIO 111 JEUN 95 EDUC 330 TELECOM 203 CONSOM 136 JAI 766 GENVAL 81

15 Doc. 15783/2/11 REV 2 GENVAL 108 ENFOPOL 368 DROPIEN 119 AUDIO 53

16 Doc. 10607/12 +COR 1 GENVAL 39 ENFOPOL 155 DROIPEN 69 AUDIO 62 JEUN 46

17 Doc. 15569/08 ENFOPOL 224 CRIMORG 190

18 Doc. 5957/2/10 REV 2 CRIMORG 22 ENFOPOL 32

19 Doc. 10663/12 RECH 207 COMPET 364 IND 102 MI 398 EDUC 152 TELECOM 118 ENER 233 ENV 446 REGIO 75 AGRI 362 TRANS 187 SAN 134 CODEC 1511.

20 Doc 10556/04 COSDP 374 POLARM 17 IND 80 RECH 130 ECO 121

– Propuesta conjunta de Decisión del Consejo relativa a las modalidades de aplicación por la Unión de la cláusula de solidaridad[21]

– Conclusiones del Consejo sobre la alfabetización mediática en el entorno digital[22]

– Derechos humanos y democracia: Marco estratégico y Plan de acción de la UE[23]

– Informe sobre la aplicación de la Estrategia Europea de Seguridad[24]

5. Comisión

– La Agenda digital para Europa[25] que es una de las siete iniciativas emblemáticas de Europa 2020, una estrategia para un crecimiento inteligente, sostenible e integrador[26] y la Agenda Digital para Europa – Motor del crecimiento europeo[27] que reorienta la Agenda Digital

– Comunicación sobre la protección de la privacidad en un mundo interconectado - Un marco europeo de protección de datos para el siglo XXI[28]

– Comunicación "a represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia"[29]

---

21 Doc. 18124/12 CAB 39 POLGEN 220 CCA 13 JAI 946 COSI 134 PROCIV 225 ENFOPOL 430 COPS 485 COSDP 1123 PESC 1584 COTER 125 COCON 45 COHAFA 165

22 Doc. 15441/09 AUDIO 47 EDUC 173 TELECOM 233 RECH 380

23 Doc. 11855/12 COHOM 163 PESC 822 COSDP 546 FREMP 100 INF 110 JAI 476 RELEX 603

24 Doc. 17104/08 CAB 66 PESC 1687 POLGEN 139

25 Doc. 9981/1/10 TELECOM 52 AUDIO 17 COMPET 165 RECH 193 MI 168 DATA PROTECT 141.

26 Doc. 7110/10 CO EUR-PREP 7 POLGEN 28 AG 3 ECOFIN 136 UEM 55 SOC 174 COMPET 82 RECH 83 ENER 63 TRANS 55 MI 73 IND 33 EDUC 40 ENV 135 AGRI 74.

27 Doc. 17963/12 TELECOM 262 MI 839 COMPET 786 CONSOM 161 DATAPROTECT 149 RECH 472 AUDIO 137 POLGEN 216

28 Doc. 5852/12 DATAPROTECT 8 JAI 43 MI 57 DRS 10 DAPIX 11 FREMP 6

29 Doc. 8543/12 ENFOPOL 94 TELECOM 72

– Comunicación de la Comisión titulada "liberar el potencial de la computación en nube en Europa"[30]

– Comunicación de la Comisión sobre la protección de infraestructuras críticas de información "logros y próximas etapas: hacia la ciberseguridad global"[31]

– Comunicación de la Comisión sobre Protección de Infraestructuras Críticas de Información "Proteger Europa de ciberataques e interrupciones a gran escala: aumentar la preparación, seguridad y resistencia"[32]

6. Naciones Unidas

– Resolución de la Asamblea General de las Naciones Unidas (A/RES 57/239) relativa a la creación de una cultura mundial de seguridad cibernética

– Resolución del Consejo de Derechos Humanos de las Naciones Unidas (A/HR/20/L.13), de 29 de junio de 2012, sobre la Promoción, protección y disfrute de los derechos humanos en Internet

– Resolución de la Asamblea General de las Naciones Unidas (A/RES 67/27) relativa a los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

– Creación de un grupo intergubernamental de expertos de composición abierta sobre el delito cibernético junto con la Oficina de las Naciones Unidas contra la Droga y el Delito, de conformidad con la Resolución de la Asamblea General 65/230

7. Consejo de Europa

– Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981

– Convenio del Consejo de Europa sobre la ciberdelincuencia de 23 de noviembre de 2001

30 Doc. 14411/12 TELECOM 170 MI 586 DATAPROTECT 112 COMPET 585
31 Doc. 8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38
32 Doc. 8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46

8. Organización para la Seguridad y la Cooperación en Europa (OSCE)

   – Decisión del Consejo Permanente n.° 1039, de 26 de abril de 2012, relativa al desarrollo de medidas de confianza para reducir los riesgos de conflictos provocados por el uso de las tecnologías de la comunicación y la información

   – Decisión Ministerial n.° 4/12, de 7 de diciembre de 2012, esfuerzos de la OSCE para responder a las amenazas transnacionales

   – Grupo informal y abierto de la OSCE cuya misión es elaborar un proyecto de conjunto de medidas de creación de confianza para reforzar la cooperación interestatal, la transparencia, la predictibilidad y la estabilidad, y reducir el riesgo de malas interpretaciones, escaladas de tensión y conflictos que pueden producir el uso de las TIC (Decisión del Consejo permanente de la OSCE n.° 1039 de 26 de abril de 2012)

9. Conferencias, iniciativas y actos

   – Conferencia Internacional sobre el Ciberespacio, celebrada en Londres el 1 y 2 de noviembre de 2011 y seguida por la Conferencia Internacional sobre el Ciberespacio celebrada el 4 y 5 de octubre de 2012 en Budapest

   – Ejercicio de simulación conjunto UE-EEUU para hacer frente a un incidente cibernético "Cyber Atlantic 2011" y ejercicio paneuropeo con la participación de todos los Estados miembros ("ciber Europa 2010" y "Ciber Europa 2012")

   – Un Grupo ad hoc sobre seguridad nuclear que debatió sobre la Seguridad informática/Ciberseguridad y elaboró su informe final sobre esta cuestión[33]-

[33] Doc. 10616/12 AHGS 20 ATO 84

10. Otros:

– Evaluación de la amenaza de la delincuencia grave y organizada (SOCTA)[34]

– Política de seguridad en materia de defensa de la red para proteger la información[35]y Directrices sobre Defensa de la Red[36]

---

[34] Doc. 7368/13 JAI 200 COSI 26 ENFOPOL 75 CRIMORG 41 CORDROGUE 27 ENFOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211

[35] Doc. 8408/12 CSCI 11 CSC 20

[36] Doc. 10578/12 CSCI 20 CSC 34