PARLAMENTO EUROPEO 2009 - 2014

Documento de sesión

6.9.2013 B7-0386/2013

PROYECTO DE PROPUESTA DE RESOLUCIÓN

tras una declaración de la Comisión

presentada de conformidad con el artículo 110, apartado 2, del Reglamento

sobre una Estrategia de ciberseguridad de la Unión Europea: «Un ciberespacio abierto, protegido y seguro»
(2013/2606(RSP))

Malcolm Harbour, Andreas Schwab
en nombre de la Comisión de Mercado Interior y Protección del Consumidor
Elmar Brok, Tunne Kelam
en nombre de la Comisión de Asuntos Exteriores

B7-0386/2013

Resolución del Parlamento Europeo sobre una «Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro»
(2013/2606(RSP))

El Parlamento Europeo,

– Vista la Comunicación conjunta, de 7 de febrero de 2013, de la Comisión Europea y la Alta Representante de la Unión Europea para Asuntos Exteriores y Política de Seguridad titulada «Estrategia de ciberseguridad de la Unión Europea: un ciberespacio abierto, protegido y seguro» (JOIN(2013)1),

– Vista la propuesta de Directiva del Parlamento Europeo y del Consejo, de 7 de febrero de 2013, relativa a medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión (COM(2013)0048),

– Vistas las comunicaciones de la Comisión «Una agenda digital para Europa», de 19 de mayo de 2010 (COM (2010)0245), y «La agenda digital para Europa – Motor del crecimiento europeo», de 18 de diciembre de 2012 (COM(2012)0784),

– Vista la Comunicación de la Comisión, de 27 de septiembre de 2012, titulada «Liberar el potencial de la computación en nube en Europa» (COM(2012)0529),

– Vista la Comunicación de la Comisión, de 28 de marzo de 2012, titulada «La represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia», y vistas las conclusiones del Consejo al respecto, de 7 de junio de 2012,

– Vista la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013 , relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo[1],

– Vista 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[2],

– Vista la Directiva 2011/92/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil y por la que se sustituye la Decisión marco 2004/68/JAI del Consejo[3],

– Vistos el Programa de Estocolmo en el ámbito de la libertad, la seguridad y la justicia[4], las comunicaciones de la Comisión tituladas «Garantizar el espacio de libertad, seguridad y justicia para los ciudadanos europeos - Plan de acción por el que se aplica el programa de

[1] DO L 218 de 14.08.13, p. 8.
[2] DO L 345 de 23.12.2008, p. 75.
[3] DO L 335 de 17.12.11, p. 1.
[4] DO C 115 de 4.5.2010, p. 1.

Estocolmo» (COM(2010)0171) y «La Estrategia de Seguridad Interior de la UE en acción: cinco medidas para una Europa más segura» (COM(2010)0673), así como su Resolución, de 22 de mayo de 2013, sobre la Estrategia de Seguridad Interna de la Unión Europea[1],

– Vista la propuesta conjunta de la Comisión y de la Alta Representante para una Decisión del Consejo sobre las medidas para la aplicación por la Unión de la Cláusula de Solidaridad (JOIN/2012/039),

– Vista la Decisión marco del Consejo 2001/413/JAI, de 28 de mayo de 2001, sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo[2],

– Vista su Resolución, de 12 de junio de 2012, sobre la protección de infraestructuras críticas de información – logros y próximas etapas: hacia la ciberseguridad global[3], así como las conclusiones del Consejo, de 27 de mayo de 2011, sobre la comunicación de la Comisión titulada «Protección de infraestructuras críticas de información – logros y próximas etapas: hacia la ciberseguridad global» (COM(2011)0163),

– Vista su Resolución, de 11 de diciembre de 2012, sobre la culminación del Mercado Único Digital[4],

– Vista su Resolución, de 22 de noviembre de 2012, sobre ciberseguridad y defensa[5],

– Vista su Resolución legislativa, de 16 de abril de 2013, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativa a la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) (COM(2010)521), en la que aprueba su posición en primera lectura[6],

– Vista su Resolución, de 11 de diciembre de 2012, sobre una «Estrategia de libertad digital en la política exterior de la UE»[7],

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

– Vistas las obligaciones internacionales de la Unión, especialmente las derivadas del Acuerdo General sobre el Comercio de Servicios (GATS),

– Visto el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE) y la Carta de los Derechos Fundamentales de la Unión Europea y en particular sus artículos 6, 8 y 11[8],

– Vistas las negociaciones en curso sobre la Asociación Transatlántica de Comercio e Inversión (ATCI),

---

[1] Textos Aprobados, P7_TA(2012)0207.
[2] DO L 149 de 2.6.01, p. 1.
[3] Textos Aprobados, P7_TA(2012)0237.
[4] Textos Aprobados, P7_TA(2012)0468.
[5] Textos Aprobados, P7_TA(2012)0457.
[6] Textos Aprobados, P7_TA(2013)0103.
[7] Textos Aprobados, P7_TA(2012)0470.
[8] DO C 83 de 30.3.10, p. 389.

– Visto el artículo 110, apartado 2, de su Reglamento,

A. Considerando que los crecientes retos cibernéticos, bajo la forma de amenazas y ataques más y más sofisticados, constituyen un peligro de primer orden para la seguridad, la estabilidad y la prosperidad económica de los Estados miembros así como del sector privado y del conjunto de la sociedad; que, por consiguiente, la protección de nuestra sociedad y de nuestra economía será un reto en constante evolución;

B. Considerando que el ciberespacio y la ciberprotección deben constituir uno de los pilares estratégicos de las políticas de seguridad y defensa de la UE y de todos sus Estados miembros; considerando que resulta esencial garantizar que el ciberespacio siga abierto a la libre circulación de ideas, información y opiniones;

C. Considerando que el comercio electrónico y los servicios en línea son una fuerza vital de Internet y son cruciales para alcanzar los objetivos de la Estrategia Europa 2020, beneficiando tanto a los ciudadanos como al sector privado; que la Unión debe aprovechar plenamente el potencial y las oportunidades que supone Internet para la profundización del mercado único, incluido el mercado único digital;

D. Considerando que entre las prioridades estratégicas perfiladas en la Comunicación conjunta sobre la estrategia de ciberseguridad para la Unión Europa se incluyen la consecución de la ciberresiliencia, la reducción de la ciberdelincuencia, el desarrollo de una política de ciberdefensa y de cibercapacidades relacionadas con la Política Exterior y de Seguridad Común (PESC), y el establecimiento de una política internacional coherente en materia de ciberespacio;

E. Considerando que las redes y los sistemas de información en toda la Unión poseen un elevado nivel de interconexión; que dado el alcance mundial de Internet, muchos de los incidentes de seguridad en estos sistemas trascienden las fronteras estatales y pueden comprometer el funcionamiento del mercado interior y la confianza de los consumidores en el mercado único digital;

F. Considerando que la ciberseguridad, tanto en la Unión como en el resto del mundo, no es más fuerte que el más débil de sus eslabones, y que las perturbaciones en cualquier sector o en cualquier Estado miembro repercuten sobre otros sectores o Estados miembros, con consecuencias sobre el conjunto de la economía de la Unión;

G. Considerando que en abril de 2013 solo trece Estados miembros habían aprobado oficialmente estrategias nacionales en materia de ciberseguridad; que persisten diferencias fundamentales entre los diversos Estados miembros en cuanto a su nivel de preparación, seguridad, cultura estratégica y capacidad de desarrollar y aplicar estrategias nacionales de ciberseguridad; que es preciso evaluar estas diferencias;

H. Considerando que las diferentes culturas en materia de seguridad y la falta de un marco jurídico conducen a la fragmentación del mercado único digital, y suponen un problema de primer orden; que la falta de un planteamiento armonizado en materia de ciberseguridad conlleva graves riesgos para la prosperidad económica y para la seguridad de las transacciones, lo que exige esfuerzos concertados y una mayor cooperación entre los Gobiernos, el sector privado, las agencias de inteligencia y a las fuerzas de seguridad;

I. Considerando que la ciberdelincuencia es un problema internacional cada vez más caro para la economía mundial, con un coste cercano a los 295 000 millones anuales según la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD);

J. Considerando que la ciberdelincuencia internacional organizada se aprovecha de los avances tecnológicos para seguir transfiriendo su campo de operaciones al ciberespacio, donde la ciberdelincuencia está alterando radicalmente la tradicional estructura de los grupos delictivos organizados; considerando que esto ha permitido que la delincuencia organizada esté menos localizada y pueda aprovechar mejor a escala mundial la territorialidad y la diversidad de jurisdicciones nacionales;

K. Considerando que la investigación de los delitos cibernéticos por parte de las autoridades competentes sigue viéndose obstaculizada por diversos elementos, entre ellos el uso, en las transacciones cibernéticas, de «divisas virtuales» con fines de blanqueo de dinero, las problemas de la territorialidad y los límites jurisdiccionales, las carencias en las capacidades de puesta en común de recursos de inteligencia, la falta de personal con formación adecuada, y una cooperación poco sólida con otros actores;

L. Considerando que la tecnología es la base para el desarrollo del ciberespacio, y que para mejorar la resiliencia y la protección del ciberespacio de la UE es fundamental una continua adaptación a los cambios tecnológicos; que deben tomarse medidas para garantizar que la legislación se actualice en función de la evolución tecnológica, permitiendo así identificar y perseguir eficazmente a los ciberdelincuentes y proteger a las víctimas de sus delitos;

1. Celebra la comunicación conjunta sobre la estrategia de ciberseguridad para la Unión Europea y la propuesta de Directiva sobre medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión;

2. Destaca la creciente y capital importancia que Internet y el ciberespacio revisten para las transacciones políticas, económicas y sociales, ya no solo en el seno de la Unión Europea sino también en las relaciones con otros actores mundiales;

3. Destaca la necesidad de desarrollar una política de comunicación estratégica sobre ciberseguridad en la UE, situaciones de crisis cibernética, análisis estratégicos, alertas y colaboración entre el sector público y el privado, y recomendaciones al público;

4. Recuerda que un elevado nivel de seguridad de la información y las redes es necesario no solo para mantener servicios esenciales para el buen funcionamiento de la sociedad y la economía, sino también para garantizar la integridad física de los ciudadanos, mejorando la eficiencia, la eficacia y el funcionamiento seguro de las infraestructuras críticas; destaca que, si bien debe abordarse la seguridad de la información y las redes, también la mejora de la seguridad física es un aspecto importante; hace hincapié en que las infraestructuras deben ser resistentes a las perturbaciones tanto deliberadas como accidentales; recalca que, en este sentido, la estrategia de ciberseguridad debería hacer más hincapié en las causas comunes de los fallos de sistema accidentales;

5. Reitera su petición a los Estados miembros de que adopten estrategias de ciberseguridad que cubran los aspectos técnicos, de coordinación y de recursos humanos y financieros e

incluyan normas claras sobre los beneficios y responsabilidades que correspondan al sector privado, con objeto de garantizar la participación del mismo sin demora, y que establezcan procedimientos exhaustivos de gestión de riesgos y salvaguarden el marco regulador;

6. Constata que solo la combinación de liderazgo y de compromiso político por parte de las instituciones de la Unión y de los Estados miembros permitirá un elevado nivel de seguridad de la información y las redes en toda la Unión, contribuyendo así al funcionamiento seguro y fluido del mercado único;

7. Destaca que la política de ciberseguridad de la Unión debe ofrecer un entorno digital seguro y fiable basado en, y diseñado para garantizar la protección y la preservación de las libertades y el respeto de los derechos fundamentales en Internet –tal y como establecen la Carta de la UE y el artículo 16 del TFUE–, en particular los derechos a la intimidad y a la protección de datos; considera que debe prestarse atención específica a la protección de los niños en Internet;

8. Pide a los Estados miembros y a la Comisión que adopten todas las acciones necesarias para presentar programas de formación destinados a la promoción y mejora de la sensibilización, las aptitudes y la educación entre los ciudadanos europeos, en particular en lo relativo a la seguridad personal, como parte de un currículo de alfabetización digital desde temprana edad; celebra la iniciativa de organizar un Mes Europeo de la Ciberseguridad con el apoyo de ENISA y en colaboración con las autoridades públicas y el sector privado, con objeto de sensibilizar respecto a los desafíos que supone la protección de las redes y de los sistemas de información;

9. Considera que la educación en materia de ciberseguridad aumenta la concienciación de la sociedad europea respecto a las ciberamenazas, alentando así a un uso responsable del ciberespacio, y contribuye a potenciar la reserva de cibercompetencias; reconoce el papel protagonista de Europol y de su nuevo Centro Europeo contra la Ciberdelincuencia (EC3), así como de ENISA y de Eurojust, en la oferta de actividades de formación a nivel de la UE en el uso de herramientas de cooperación judicial internacional y en el cumplimiento de la ley en relación con diversos aspectos de la ciberdelincuencia;

10. Reitera la necesidad de ofrecer asesoramiento técnico e información jurídica y de crear programas sobre la prevención y la lucha contra la ciberdelincuencia; respalda la formación de los ingenieros informáticos especializados en la protección de infraestructuras críticas y sistemas de información, así como la de los operadores de los sistemas de control de transporte y los centros de gestión de tráfico; destaca la imperiosa necesidad de implantar programas de formación en ciberseguridad para el personal del sector público a todos los niveles;

11. Reitera su petición de prudencia en la aplicación de restricciones a la capacidad de los ciudadanos de hacer uso de las tecnologías de la comunicación y la información, y destaca que los Estados miembros deberían siempre evitar, cuando busquen respuestas a las amenazas y ataques cibernéticos, poner en peligro los derechos y libertades de los ciudadanos, y disponer de medios legislativos adecuados para distinguir entre ciberincidentes a nivel civil y a nivel militar;

12. Considera que el papel de la reglamentación en el campo de la ciberseguridad debe orientarse a los riesgos, centrarse en aquellas infraestructuras críticas cuyo funcionamiento sea de primerísimo interés público, y aprovechar los esfuerzos basados en el mercado que ya ha hecho el sector para garantizar la resiliencia de las redes; destaca el papel decisivo de la cooperación a nivel operativo en la promoción de un intercambio de información más eficiente entre las autoridades públicas y el sector privado –tanto a nivel nacional y de la Unión como con los interlocutores estratégicos de la Unión– en lo relativo a las amenazas informáticas, con objeto de garantizar la seguridad de las redes y la información, mediante la instauración de confianza, valores y compromiso mutuos y el intercambio de conocimientos especializados; considera que las asociaciones público-privadas deberían basarse en la neutralidad tecnológica y de las redes y centrarse en los esfuerzos para abordar los problemas con gran repercusión pública; pide a la Comisión que aliente a todos los operadores del mercado involucrados a que sean más prudentes y más colaboradores, a fin de proteger a los demás operadores de posibles daños a sus servicios;

13. Reconoce que la detección y notificación de los incidentes de ciberseguridad es fundamental para promover la ciberresiliencia en la Unión; considera necesaria la introducción de unos requisitos de divulgación de información proporcionados para posibilitar la notificación a las autoridades nacionales competentes de aquellos incidentes que impliquen fallos importantes en la seguridad, permitiendo así un mejor seguimiento de los incidentes de ciberdelincuencia y facilitando los esfuerzos para aumentar la concienciación a todos los niveles;

14. Alienta a la Comisión y a otros actores a que introduzcan políticas de ciberseguridad y ciberresiliencia que incluyan incentivos económicos para promover un elevado nivel de ciberseguridad y ciberresiliencia;

Ciberresiliencia

15. Constata que los diferentes sectores y Estados miembros tienen diferentes niveles de capacidades y aptitudes y que esto perjudica el desarrollo de una cooperación con confianza y socava el funcionamiento del mercado único;

16. Considera que los requisitos impuestos a las pequeñas y medianas empresas deben adoptar un enfoque proporcionado y basado en el riesgo;

17. Insiste en el desarrollo de la ciberresiliencia para las infraestructuras críticas, y recuerda que las próximas disposiciones para la aplicación de la cláusula de solidaridad (artículo 222 del TFUE) deberían tener en cuenta el riesgo de ciberataques contra un Estado miembro; pide a la Comisión y a la Alta Representante que tengan este riesgo en cuenta en sus informes conjuntos sobre la evaluación integrada de amenazas y riesgos, cuya publicación está prevista para 2015;

18. Destaca que, para garantizar la integridad, disponibilidad y confidencialidad de los servicios críticos en particular la identificación y categorización de las infraestructuras críticas, deben estar actualizadas, y deben fijarse los requisitos de seguridad mínimos para sus sistemas de información y redes;

19. Reconoce que la propuesta de Directiva relativa a las medidas para garantizar un elevado nivel común de seguridad de las redes y de la información en la Unión prevé estos requisitos de seguridad mínimos para los proveedores de servicios de la sociedad de la información y los operadores de infraestructuras críticas;

20. Pide a los Estados miembros y a la Unión que instauren marcos adecuados para unos sistemas de intercambio de información rápidos y bidireccionales que garanticen la anonimidad al sector privado, mantengan al sector público constantemente informado y, en caso necesario, ofrezcan asistencia al sector privado;

21. Celebra la idea de la Comisión de crear una cultura de gestión de riesgos en relación con la ciberseguridad, e insta a los Estados miembros y a las instituciones de la Unión a incluir cuanto antes la gestión de las crisis cibernéticas en sus planes de gestión de crisis y sus análisis de riesgos; pide además a los Gobiernos de los Estados miembros y a la Comisión que animen a los actores del sector privado a que incluyan la gestión de las crisis cibernéticas en sus planes de gestión y sus análisis de riesgos y a que formen a su personal en ciberseguridad;

22. Pide a todos los Estados miembros y a las instituciones de la Unión que creen una red de Centros de Respuesta a Emergencias de Seguridad Informática (CERT) eficaces y operativos día y noche todos los días de la semana; señala que los CERT nacionales deberían formar parte de una red eficaz en la que se intercambie información pertinente de acuerdo con las normas de confianza y confidencialidad necesarias; constata que las iniciativas-marco para agrupar los CERT y otros organismos de seguridad relevantes pueden resultar herramientas útiles para la creación de confianza en un contexto transfronterizo e intersectorial; reconoce la importancia que reviste una cooperación eficiente y eficaz entre los CERT y los órganos judiciales y fuerzas de seguridad en la lucha contra la ciberdelincuencia;

23. Apoya a ENISA en el ejercicio de sus funciones relativas a la seguridad de la información y las redes, en particular ofreciendo orientación y asistencia a los Estados miembros, así como respaldando el intercambio de mejores prácticas y el desarrollo de un marco de confianza;

24. Destaca la necesidad de que la industria aplique unos adecuados requisitos de rendimiento en materia de ciberseguridad en toda la cadena de valor para los productos de TIC utilizados en redes de transporte y sistemas de información, de que efectúe una adecuada gestión de riesgos, de que adopte normas y soluciones de seguridad, y de que desarrolle las mejores prácticas y una puesta en común de información con vistas a garantizar la ciberseguridad de los sistemas de transporte;

Recursos tecnológicos e industriales

25. Considera que el hecho de garantizar un alto nivel de seguridad de la información y de las redes juega un papel central en el fomento de la competitividad tanto de los proveedores como de los usuarios de soluciones de seguridad en la Unión Europea; considera que, si bien el sector de la seguridad informática en la Unión posee un importante potencial por explotar, tanto empresas como sector público están a menudo mal informados sobre los costes y beneficios de invertir en ciberseguridad, lo que les hace vulnerables frente a las

ciberamenazas dañinas; destaca que la puesta en marcha de los CERT constituye un factor relevante en este sentido;

26. Considera que una oferta y una demanda importantes de soluciones de ciberseguridad exigen unas inversiones adecuadas en recursos académicos, investigación y desarrollo (I+D) y creación de conocimientos y capacidades por parte de las autoridades nacionales competentes en asuntos de TIC, a fin de fomentar la innovación y concienciar suficientemente a los ciudadanos en cuanto a los riesgos de seguridad de la información y las redes, lo que conducirá hacia un sector de seguridad europeo concertado;

27. Pide a las instituciones de la Unión y a los Estados miembros que adopten las medidas necesarias para crear un «mercado único de la ciberseguridad» en el que usuarios y proveedores puedan aprovechar al máximo todas las innovaciones y sinergias y todo el caudal de conocimientos especializados disponibles, y que permita la entrada de pymes;

28. Alienta a los Estados miembros a que estudien la posibilidad de hacer inversiones en el sector de la ciberseguridad europeo, de manera similar a como se ha hecho en otros sectores, como por ejemplo el de la aviación;

Ciberdelincuencia

29. Considera que las actividades delictivas en el ciberespacio pueden ser para el bienestar de las sociedades tan dañinas como lo son los delitos en el mundo físico, y que estas formas de delincuencia a menudo se refuerzan mutualmente, como se observa por ejemplo en la explotación sexual infantil y en la delincuencia organizada y el blanqueo de dinero;

30. Observa que en algunos casos existen vínculos entre las actividades empresariales legales y las ilegales; destaca la importancia del vínculo, facilitado por Internet, entre la financiación del terrorismo y la delincuencia grave organizada; señala que la opinión pública debe concienciarse de la gravedad que supone involucrarse en la ciberdelincuencia y de la posibilidad de que lo que a primera vista pueden parecer delitos «socialmente aceptables», como por ejemplo la descarga ilegal de películas, a menudo reporta a las organizaciones criminales internacionales grandes beneficios;

31. Coincide con la Comisión en que dentro de Internet son aplicables las mismas normas y principios que fuera, y que por consiguiente la lucha contra la ciberdelincuencia debe reforzarse con capacidades operativas y legislación actualizadas;

32. Estima que, dado el carácter sin fronteras de la delincuencia, revisten especial importancia los esfuerzos que se hagan, y los conocimientos que se ofrezcan, a nivel de la Unión, esto es, por encima del nivel de los Estados miembros individuales, por lo que debe dotarse a Eurojust, al EC3 de Europol, a los CERT y a las universidades y centros de investigación de unos recursos y capacidades que les permitan funcionar adecuadamente como centros neurálgicos del conocimiento, la cooperación y la puesta en común de información;

33. Acoge con suma satisfacción la creación del EC3, y alienta el futuro desarrollo de esta agencia y su papel vital a la hora de coordinar un intercambio transfronterizo de información y conocimientos especializados puntual y eficaz destinado a apoyar la prevención, la detección y la investigación de la ciberdelincuencia;

34. Pide a los Estados miembros que garanticen a los ciudadanos un fácil acceso a la información sobre las amenazas cibernéticas y la manera de combatirlas; considera que esta orientación debe ir acompañada de información sobre la manera en que los usuarios pueden proteger su intimidad en Internet, detectar y notificar los casos de *grooming* (acercamiento a menores con fines de abuso sexual), instalar software y cortafuegos, gestionar contraseñas, y detectar falsas identidades (*phishing*), situaciones de *pharming* y otros ataques;

35. Encarece a los Estados miembros que todavía no hayan ratificado el Convenio de Budapest del Consejo de Europa sobre Ciberdelincuencia a que lo hagan sin demora; celebra las reflexiones del Consejo de Europa sobre la necesidad de actualizar el citado Convenio a la luz de los avances tecnológicos para garantizar su eficacia en la lucha contra la ciberdelincuencia, y pide a la Comisión y a los Estados miembros que participen en este debate; respalda los esfuerzos por promover la ratificación del Convenio por otros países, y pide a la Comisión que la promueva activamente fuera de la Unión;

Ciberdefensa

36. Destaca que los desafíos, amenazas y ataques cibernéticos comprometen los intereses de defensa y seguridad nacional, y que los enfoques militar y civil frente a la labor de protección de las infraestructuras críticas deberían maximizar el beneficio que suponen para ambos los esfuerzos por lograr sinergias;

37. Pide, por consiguiente, a los Estados miembros que intensifiquen su cooperación con la Agencia Europea de Defensa con vistas a elaborar propuestas e iniciativas para el desarrollo de capacidades de ciberdefensa a partir de las recientes iniciativas y proyectos; subraya la necesidad de incrementar la I+D, entre otras vías mediante la puesta en común de recursos;

38. Se reafirma en que una estrategia exhaustiva de ciberseguridad de la UE debe tener en cuenta el valor añadido de las agencias y organismos existentes, así como las buenas prácticas cosechadas de los Estados miembros que ya han puesto en marcha sus propias estrategias de ciberseguridad;

39. Pide a la Vicepresidenta / Alta Representante que incluya la gestión de las crisis cibernéticas en la planificación de la gestión de crisis, e insiste en la necesidad de que los Estados miembros, en cooperación con la Agencia de Defensa Europea, elaboren planes para proteger las misiones y operaciones PESC frente a los ciberataques; pide a los Estados miembros que pongan en común una fuerza europea de ciberdefensa;

40. Destaca la buena cooperación a nivel práctico con la OTAN en el ámbito de la ciberseguridad, así como la necesidad de reforzarla, en particular mediante una mayor coordinación en las áreas de planificación, tecnología, formación e instalaciones;

41. Pide que la Unión haga esfuerzos por intercambiar información con actores internacionales –incluida la OTAN–, para identificar áreas de cooperación, evitar duplicidades y complementar actividades, siempre que sea posible;

Política internacional

42. Considera que la cooperación y el diálogo internacionales juegan un papel fundamental en la creación de confianza y transparencia y en el fomento de un gran nivel de creación de redes e intercambio de información a nivel mundial; pide, por consiguiente, a la Comisión y al Servicio Europeo de Acción Exterior que creen un equipo de ciberdiplomacia cuyas responsabilidades incluirían el fomento del diálogo con los países y organizaciones con posicionamientos similares; pide una participación más activa de la UE en el amplio abanico de conferencias internacionales de alto nivel sobre ciberseguridad;

43. Considera que es preciso un equilibrio entre los objetivos enfrentados de la transferencia transfronteriza de datos y la protección de los mismos y la ciberseguridad, en consonancia con las obligaciones internacionales de la Unión, especialmente las derivadas del GATS;

44. Pide a la Vicepresidenta / Alta Representante que integre la dimensión de la ciberseguridad en las acciones exteriores de la UE, especialmente en relación con países terceros, para reforzar la cooperación, así como el intercambio de experiencias e información, sobre cómo gestionar la ciberseguridad;

45. Pide que la Unión se esfuerce en intercambiar información con actores internacionales con vistas a identificar áreas de cooperación, evitar duplicidades y complementar actividades, siempre que sea posible; pide a la Vicepresidenta / Alta Representante y a la Comisión que se muestren proactivas en las organizaciones internacionales y coordinen las posturas de los Estados miembros sobre cómo promover eficazmente políticas y soluciones en el ámbito cibernético;

46. Entiende que debe trabajarse para garantizar que los instrumentos jurídicos internacionales existentes, en particular el Convenio del Consejo de Europa sobre la ciberdelincuencia, se apliquen en el ciberespacio; considera, por consiguiente, que actualmente no hay necesidad de crear nuevos instrumentos jurídicos a nivel internacional; celebra, no obstante, la cooperación internacional para la elaboración de normas de comportamiento en el ciberespacio que contribuyan a la presencia del Estado de Derecho en el mismo; considera que debe estudiarse la conveniencia de actualizar los instrumentos jurídicos existentes de modo que reflejen los avances tecnológicos; opina que los aspectos jurisdiccionales requieren un exhaustivo debate sobre la cuestión de la cooperación y procesamiento judiciales en los delitos transnacionales;

47. Considera que en particular el Grupo de Trabajo UE-EE.UU. sobre Ciberseguridad y Ciberdelincuencia debería permitir la UE y a los EE.UU. intercambiar, cuando proceda, las mejores prácticas sobre políticas de ciberseguridad; observa, en este sentido, que los ámbitos relacionados con la ciberseguridad, como por ejemplo los servicios dependientes de un funcionamiento seguro de las redes y los sistemas de información, se incluirán en las próximas negociaciones de la Asociación Transatlántica de Comercio e Inversión (ATCI);

48. Observa que las aptitudes en ciberseguridad, así como la capacidad de prevenir, detectar y contrarrestar eficazmente las amenazas y los ataques malintencionados no tienen el mismo nivel de desarrollo en todo el mundo; destaca que los esfuerzos por incrementar la ciberresiliencia y combatir las ciberamenazas no deben limitarse a los interlocutores con similar posicionamiento sino también orientarse a aquellas regiones que dispongan de capacidades, infraestructuras técnicas y marcos jurídicos menos desarrollados; considera

que la coordinación de los CERT es fundamental en este sentido; pide a la Comisión que facilite los esfuerzos de los países terceros, prestándoles asistencia en caso necesario, por crearse sus propias capacidades de ciberseguridad utilizando los medios adecuados;

Ejecución

49. Pide que se hagan evaluaciones periódicas de la eficacia de las estrategias nacionales de ciberseguridad al más alto nivel político, con vistas a asegurar la adaptación a las nuevas amenazas globales y a garantizar el mismo nivel de ciberseguridad en los distintos Estados miembros;

50. Pide a la Comisión que elabore una clara hoja de ruta en la que se fijen los calendarios para el cumplimiento de los objetivos a nivel de la Unión respecto a la estrategia de ciberseguridad, así como las evaluaciones de la misma; pide a los Estados miembros que acuerden un plan de ejecución similar para las acciones nacionales en relación con esta estrategia;

51. Pide que se efectúen informes regulares –de la Comisión, los Estados miembros, Europol y el recién creado EC3, Eurojust y ENISA– en que se evalúen los progresos hechos en relación con los objetivos marcados en la estrategia de ciberseguridad, incluidos los indicadores de rendimiento claves que miden los progresos en la ejecución;

52. Encarga a su Presidente que transmita la presente Resolución al Consejo y a la Comisión así como a los Gobiernos y Parlamentos de los Estados miembros, a Europol, a Eurojust y al Consejo de Europa.