P7_TA(2012)0457

Ciberseguridad y ciberdefensa

Resolución del Parlamento Europeo, de 22 de noviembre de 2012, sobre ciberseguridad y ciberdefensa (2012/2096(INI))

El Parlamento Europeo,

– Visto el informe sobre la aplicación de la Estrategia Europea de Seguridad, refrendado por el Consejo Europeo de los días 11 y 12 diciembre 2008,

– Visto el Convenio sobre la Ciberdelincuencia del Consejo de Europa, hecho en Budapest el 23 de noviembre de 2001,

– Vistas las conclusiones del Consejo sobre protección de infraestructuras críticas de información, de 27 de mayo de 2011, y las anteriores conclusiones del Consejo sobre ciberseguridad,

– Vista la Comunicación de la Comisión titulada «Una Agenda Digital para Europa» de 19 de mayo de 2010 (COM(2010)0245),

– Vista la 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[1],

– Vista la reciente Comunicación de la Comisión sobre la represión del delito en la era digital: creación de un centro europeo de ciberdelincuencia (COM(2012)0140),

– Vista su Resolución, de 10 de marzo de 2010, sobre la aplicación de la Estrategia Europea de Seguridad y la Política Común de Seguridad y Defensa[2],

– Vista su Resolución, de 11 de mayo de 2011, sobre el desarrollo de la política común de seguridad y defensa tras la entrada en vigor del Tratado de Lisboa[3],

– Vista su Resolución, de 22 de mayo de 2012, sobre la Estrategia de Seguridad Interior de la Unión Europea[4],

– Vista su Resolución, de 27 de septiembre de 2011, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo que modifica el Reglamento (CE) nº 1334/2000 por el que se establece un régimen comunitario de control de las exportaciones de productos y tecnología de doble uso[5],

– Vista su Resolución, de 12 de junio de 2012, sobre la protección de infraestructuras críticas

[1] DO L 345 de 23.12.2008, p. 75.
[2] DO C 349 E de 22.12.2010, p. 63.
[3] Textos Aprobados, P7_TA(2011)0228.
[4] Textos Aprobados, P7_TA(2012)0207.
[5] Textos Aprobados, P7_TA(2011)0406.

de información – logros y próximas etapas: hacia la ciberseguridad global»[1],

– Vista la Resolución del Consejo de Derechos Humanos de las Naciones Unidas, de 5 de julio de 2012, titulada «Promoción, protección y disfrute de los derechos humanos en Internet»[2], que reconoce la importancia de la protección de los derechos humanos y la libre circulación de la información en la red,

– Vistas las conclusiones de la Cumbre de Chicago de 20 de mayo de 2012,

– Visto el título V del Tratado UE,

– Visto el artículo 48 de su Reglamento interno,

– Visto el informe de la Comisión de Asuntos Jurídicos (A7-0335/2012),

A. Considerando que en el actual mundo globalizado, la UE y sus Estados miembros han pasado a depender de forma crucial de la seguridad del ciberespacio, de un uso seguro de las tecnologías de la información y las tecnologías digitales y de unos servicios de información y unas infraestructuras asociadas resistentes y fiables;

B. Considerando que las tecnologías de la información y la comunicación también se utilizan como herramientas de represión; considerando que el contexto en que se utilizan determina en gran medida el impacto que dichas tecnologías pueden tener como motor de avances positivos o de represión;

C. Considerando que las amenazas, los desafíos y los ataques cibernéticos están aumentando de modo espectacular y constituyen una amenaza para la seguridad, la defensa y la estabilidad de los Estados y también del sector privado; considerando, por tanto, que esas amenazas no pueden considerarse problemas del futuro; considerando que tras la mayoría de incidentes cibernéticos altamente visibles y problemáticos se esconden ahora motivaciones políticas; considerando que la gran mayoría de los incidentes cibernéticos siguen siendo poco sofisticados y que las amenazas para los activos críticos son cada vez más sofisticadas y justifican una protección en profundidad;

D. Considerando que el ciberespacio, con sus casi dos mil millones de usuarios interconectados en todo el mundo, ha sido uno de los medios más poderosos y eficaces para difundir las ideas democráticas y organizar a los ciudadanos que tratan de hacer realidad sus aspiraciones de libertad y lucha contra las dictaduras; considerando que el uso del ciberespacio por regímenes no democráticos y autoritarios supone una amenaza cada vez mayor a los derechos de libertad de expresión y asociación; considerando que, por consiguiente, resulta esencial garantizar que el ciberespacio siga abierto a la libre circulación de ideas, información y opiniones;

E. Considerando que existen numerosos obstáculos de tipo político, legislativo y organizativo en la UE y sus Estados miembros para el desarrollo de un enfoque integral y unificado de la ciberdefensa y la ciberseguridad; considerando que no existen definiciones, normas o medidas comunes en el ámbito sensible y vulnerable de la ciberseguridad;

---

[1] Textos Aprobados, P7_TA(2012)0237.
[2] ttp://www.ohchr.org/ES/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

F. Considerando que son insuficientes la puesta en común y la coordinación tanto de las instituciones de la UE con los Estados miembros como dentro las instituciones y entre los Estados miembros, así como con los socios externos;

G. Considerando que no existen a escala de la UE ni a escala internacional definiciones claras y armonizadas de ciberseguridad y ciberdefensa; considerando que la ciberseguridad y otros conceptos clave se comprenden de modo muy diferente en los distintos países;

H. Considerando que la UE aún no ha elaborado políticas propias coherentes sobre protección de información e infraestructuras críticas, lo cual exige un enfoque multidisciplinario, reforzando así la seguridad al tiempo que se respetan los derechos fundamentales;

I. Considerando que la UE ha propuesto diversas iniciativas para dar respuesta a nivel civil a la ciberdelincuencia, como la creación de un Centro Europeo de Ciberdelincuencia, pero que aún carece de un plan concreto en materia de seguridad y de defensa;

J. Considerando que generar confianza entre el sector privado, las autoridades policiales y las instituciones de defensa y otras instituciones competentes es de la mayor importancia en la lucha contra la ciberdelincuencia;

K. Considerando que la confianza mutua en las relaciones entre los actores estatales y no estatales es un requisito previo para lograr una ciberseguridad fiable;

L. Considerando que la mayoría de incidentes cibernéticos tanto en el sector público como en el privado quedan sin denunciar debido al carácter sensible de la información y a un eventual perjuicio para la imagen de las empresas afectadas;

M. Considerando que un gran número de incidentes cibernéticos se producen debido a la falta de resistencia y solidez de la infraestructura de la red privada y pública, unas bases de datos mal protegidas o mal aseguradas y otros defectos en las infraestructuras críticas de información; considerando que solo algunos Estados miembros consideran la protección de sus redes y sistemas de información y datos asociados como parte de su correspondiente deber de diligencia, lo cual explica la falta de inversión en tecnología de seguridad de vanguardia, formación y desarrollo de directrices adecuadas, que un elevado número de Estados miembros depende de la tecnología de seguridad de terceros países y que deben aumentarse los esfuerzos para reducir esa dependencia.;

N. Considerando que la mayoría de autores de ataques cibernéticos a alto nivel, que amenazan la seguridad y la defensa nacional o internacional, nunca se identifican ni persiguen; considerando que no existe una respuesta acordada internacionalmente ante un ciberataque respaldado por un Estado, ni un acuerdo de si ello se consideraría un *casus belli*;

O. Considerando que se está haciendo uso de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) como mediadora entre los Estados miembros para promover el intercambio de buenas prácticas en el ámbito de la ciberseguridad mediante recomendaciones sobre la elaboración, la puesta en marcha y el mantenimiento de estrategias de ciberseguridad, y que esta Agencia tiene una función de apoyo respecto de las estrategias nacionales de ciberseguridad, los planes nacionales de emergencia, la organización de ejercicio paneuropeos e internacionales sobre protección de infraestructuras críticas de información, y la preparación de simulaciones para ejercicios nacionales;

P. Considerando que en junio de 2012 sólo 10 Estados miembros habían adoptado oficialmente una estrategia nacional de ciberseguridad;

Q. Considerando que la ciberdefensa es una de las prioridades máximas de la AED, que al amparo del Plan de Desarrollo de Capacidades ha creado un equipo de proyecto sobre ciberseguridad con la mayoría de los Estados miembros que trabaja para recabar experiencias y proponer recomendaciones;

R. Considerando que las inversiones en investigación y desarrollo en materia de ciberseguridad y ciberdefensa son vitales para progresar y mantener un elevado nivel de ciberseguridad y ciberdefensa; considerando que el gasto en defensa dedicado a la investigación y desarrollo ha disminuido en vez de alcanzar, como se había acordado, el 2 % del gasto global en defensa;

S. Considerando que la concienciación y la educación de los ciudadanos sobre la ciberseguridad debe constituir la base de cualquier estrategia global de ciberseguridad;

T. Considerando que se ha de encontrar un claro equilibrio entre las medidas de seguridad y los derechos de los ciudadanos de conformidad con el Tratado de Funcionamiento de la Unión Europea (TFUE), como el derecho a la libertad de expresión, a la protección de datos y a la intimidad sin sacrificar ninguno de ellos en nombre del otro;

U. Considerando que cada vez es más necesario respetar y proteger mejor el derecho a la intimidad, como se establece en la Carta de la UE y en el artículo 16 del TFUE; considerando que, si bien es importante, la necesidad de asegurar y defender el ciberespacio a escala nacional para las instituciones y los órganos de defensa, no debe utilizarse nunca como excusa para limitar de ningún modo los derechos y las libertades en el espacio cibernético e informacional;

V. Considerando que el carácter mundial y sin fronteras de Internet requiere nuevas formas de cooperación internacional y gobernanza con múltiples partes interesadas;

W. Considerando que los Gobiernos dependen en creciente medida de actores privados para la seguridad de sus infraestructuras críticas;

X. Considerando que el Servicio Europeo de Acción Exterior (SEAE) todavía no ha incorporado de forma proactiva la faceta de la ciberseguridad en sus relaciones con terceros países;

Y. Considerando que el Instrumento de Estabilidad es, hasta el momento, el único programa de la UE concebido para dar respuesta a las crisis urgentes o los desafíos globales o transnacionales, incluidas las amenazas para la ciberseguridad;

Z. Considerando que una respuesta conjunta a las amenazas para la ciberseguridad —a través de un grupo de trabajo UE-EE.UU. sobre ciberseguridad y ciberdelincuencia— es una de las cuestiones prioritarias de las relaciones UE-EE.UU.;

Acciones y coordinación en la UE

1. Constata que el peligro que suponen las amenazas y los ataques cibernéticos contra órganos gubernamentales, administrativos, militares e internacionales crece rápidamente, que estos

se producen tanto en la UE como en el mundo, y que hay importantes motivos de preocupación de que actores estatales y no estatales, especialmente organizaciones terroristas y criminales, puedan atacar estructuras e infraestructuras críticas de información y comunicación de instituciones y miembros de la UE, con la posibilidad de provocar importantes daños, incluidos efectos cinéticos;

2. Subraya, por consiguiente, la necesidad de un planteamiento global y coordinado a estos desafíos a escala de la UE, a través del desarrollo de una estrategia exhaustiva de la UE en materia de ciberseguridad, que debería establecer una definición común de ciberseguridad y ciberdefensa, así como de lo que constituye un ataque relacionado con la defensa y una visión operativa común y tomar en cuenta el valor añadido de las agencias y organismos existentes; así como las buenas prácticas de aquellos Estados miembros que ya disponen de estrategias nacionales en el ámbito de la ciberseguridad; destaca la importancia crucial de la coordinación y la generación de sinergias a escala de la Unión para ayudar a combinar diferentes iniciativas, programas y actividades, tanto militares como civiles; pone de relieve que esa estrategia debe garantizar la flexibilidad y debe actualizarse periódicamente para adaptarse a los rápidos cambios inherentes al ciberespacio;

3. Insta a la Comisión y a la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad que examinen la posibilidad de que se produzca un ciberataque importante contra un Estado miembro en su próxima propuesta relativa a los acuerdos para la aplicación de la cláusula de solidaridad (artículo 222 del TFUE); opina asimismo que, aunque los ciberataques que ponen en peligro la seguridad nacional deben definirse con arreglo a una terminología común, podría aplicárseles la cláusula de defensa mutua (artículo 42, apartado 7, del TUE), sin perjuicio del principio de proporcionalidad;

4. Hace hincapié en que la política común de seguridad y defensa (PCSD) ha de garantizar que las fuerzas en las operaciones militares y las misiones civiles de la UE estén protegidas contra los ciberataques; recalca que la ciberdefensa debe convertirse en una competencia activa de la PCSD;

5. Hace hincapié en que las políticas de ciberseguridad de la UE deberían basarse y diseñarse con el fin de garantizar la máxima protección y preservación de las libertades digitales y el respeto de los derechos humanos en línea; cree que Internet y las TIC deberían integrarse en las políticas exterior y de seguridad de la UE para fomentar este esfuerzo;

6. Pide a la Comisión y al Consejo que reconozcan inequívocamente las libertades digitales como derechos fundamentales y como requisitos previos indispensables para disfrutar de derechos humanos universales; hace hincapié en que los Estados miembros deben aspirar a no poner nunca en peligro los derechos y libertades de los ciudadanos cuando desarrollan sus respuestas a las amenazas y los ataques cibernéticos, y deben establecer unas diferencias legislativas adecuadas entre incidentes cibernéticos a nivel civil y militar; exige cautela a la hora de aplicar restricciones sobre la capacidad de los ciudadanos para usar las herramientas de las TIC;

7. Pide al Consejo y la Comisión que, junto con los Estados miembros, elaboren un Libro Blanco sobre Ciberdefensa en el que se establezcan unas definiciones y unos criterios claros que separen niveles de ciberataques en ámbitos civiles y militares, con arreglo a su motivación y sus efectos, así como niveles de reacción, como la investigación, la detección y el procesamiento de los autores;

8. Subraya la evidente necesidad de actualizar la Estrategia Europea de Seguridad con miras a identificar y encontrar medios para perseguir y enjuiciar a autores de ciberataques, tanto individuales como relacionados con la red y apoyados por un Estado;

A escala de la UE

9. Destaca la importancia de la cooperación y la coordinación horizontales en materia de ciberseguridad dentro de las instituciones y agencias de la UE y entre ellas;

10. Recalca que las nuevas tecnologías cuestionan el modo en que los Gobiernos realizan las tareas centrales tradicionales; reafirma que, en última instancia, las políticas de defensa y de seguridad están en manos de los Gobiernos, incluido un control democrático adecuado; toma nota de la creciente importancia del papel de actores privados en la ejecución de tareas de seguridad y defensa, a menudo sin transparencia, rendición de cuentas ni mecanismos de control democrático;

11. Recalca que los Gobiernos deben atenerse a los principios básicos de Derecho internacional público y humanitario, como el respeto de la soberanía del Estado y los derechos humanos, cuando las nuevas tecnologías se utilicen en el ámbito de las políticas de seguridad y de defensa, y señala la valiosa experiencia de los Estados miembros de la UE, como Estonia, a la hora de definir y diseñar políticas en el ámbito de la ciberseguridad así como la ciberdefensa;

12. Es consciente de la necesidad de una evaluación del nivel global de ciberataques contra la infraestructura y los sistemas de información de la UE; destaca, en este contexto, la necesidad de una evaluación permanente del grado de preparación de las instituciones de la UE para responder a posibles ciberataques; insiste particularmente en la necesidad de fortalecer las infraestructuras críticas de información;

13. Destaca también, la necesidad de facilitar información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información.

14. Constata que ciberataques recientes contra las redes de información europeas y los sistemas de información estatales han causado cuantiosos daños desde los puntos de vista económico y de la seguridad cuyo alcance no se ha evaluado adecuadamente;

15. Pide a todas las instituciones de la UE que elaboren estrategias de ciberseguridad y planes de emergencia para sus propios sistemas a la mayor brevedad;

16. Pide a todas las instituciones de la UE que incluyan en sus análisis del riesgo y planes de gestión de crisis la cuestión de la gestión de crisis cibernéticas; pide asimismo a todas las instituciones de la UE que organicen formaciones de concienciación sobre la ciberseguridad para todo su personal; propone realizar ejercicios cibernéticos una vez al año de forma análoga a lo que ocurre con los ejercicios de emergencia;

17. Subraya la importancia de un desarrollo eficaz del equipo de respuesta a emergencias informáticas de la UE (CERT de la UE) y de CERT nacionales, así como de la elaboración de planes de emergencia nacionales para el caso de que llegue a ser necesario tomar medidas; celebra que en mayo de 2012 todos los Estados miembros de la UE hayan creado su CERT; insta a un desarrollo mayor de los CERT nacionales y de un CERT de la UE para que puedan desplegarse en 24 horas si resulta necesario; destaca la necesidad de estudiar la

viabilidad de asociaciones público-privadas en este ámbito;

18. Es consciente de que «Cyber Europe 2010», el primer ejercicio paneuropeo sobre protección de infraestructuras críticas de información, que tuvo lugar con la participación de varios Estados miembros bajo la dirección de la ENISA, fue de gran utilidad y constituye un ejemplo de buena práctica; asimismo, subraya la necesidad de crear cuanto antes a escala europea una Red de información sobre alertas en infraestructuras críticas (CIWIN);

19. Resalta la importancia que revisten los ejercicios paneuropeos de preparación para incidentes a gran escala de seguridad de las redes, y el establecimiento de un único conjunto de normas relativo a la evaluación de amenazas;

20. Pide a la Comisión que estudie la necesidad y viabilidad de un puesto de Coordinación Cibernética de la UE;

21. Considera que, dado el alto nivel de habilidad exigido tanto en la defensa adecuada de sistemas e infraestructuras cibernéticos como en su ataque, debe examinarse la posibilidad de desarrollar una estrategia «de sombrero blanco» entre la Comisión, el Consejo y los Estados miembros; observa que la posibilidad de «fuga de cerebros» en estos casos es elevada y que, sobre todo, los menores condenados por tales ataques tienen muchas posibilidades tanto de rehabilitación como de integración en las agencias y los órganos de defensa;

Agencia Europea de Defensa

22. Saluda las recientes iniciativas y proyectos relativos a la ciberdefensa, en especial los referidos a la recogida y la cartografía de datos, desafíos y necesidades pertinentes para la ciberseguridad y la ciberdefensa e insta a los Estados miembros a que cooperen más, también a nivel militar, con la AED en materia de ciberdefensa;

23. Pone de relieve la importancia para los Estados miembros de mantener una estrecha colaboración la AED para desarrollar sus capacidades nacionales de ciberdefensa; considera que la generación de sinergias y la puesta en común a nivel europeo son cruciales para la eficacia de la ciberdefensa a escala europea y nacional;

24. Alienta a la AED a que intensifique su cooperación con la OTAN, los centros de excelencia tanto nacionales como internacionales, el Centro Europeo de Ciberdelincuencia en Europol contribuyendo a unas reacciones más rápidas en caso de ciberataques y, en especial, con el Centro de Excelencia para la Ciberdefensa Cooperativa (CCDCOE), y a que preste particular atención al desarrollo y la formación de capacidades y al intercambio de información y prácticas;

25. Observa con preocupación que en 2010 solo un Estado miembro había alcanzado el 2 % del gasto en investigación y desarrollo en materia de defensa, y que en ese año cinco Estados miembros no habían gastado nada en I+D; insta a la AED a que junto a los Estados miembros ponga en común recursos e invierta de modo eficaz en una investigación y desarrollo eficaces, prestando especial atención a la ciberseguridad y la ciberdefensa;

Estados miembros

26. Pide a todos los Estados miembros que desarrollen y completen sin demora sus estrategias

nacionales de ciberseguridad y ciberdefensa y que garanticen un entorno decisorio y regulador sólido, unos procedimientos de gestión de riesgos exhaustivos y unas medidas y mecanismos preparatorios adecuados; pide a la ENISA que preste asistencia a los Estados miembros; expresa su respaldo a la ENISA en la elaboración de una guía que recoja buenas prácticas y recomendaciones sobre el desarrollo, la aplicación y el mantenimiento de estrategias de ciberseguridad;

27. Anima a todos los Estados miembros a crear unidades específicas de ciberseguridad y ciberdefensa en sus estructuras militares, con miras a cooperar con órganos similares en otros Estados miembros de la UE;

28. Alienta a los Estados miembros a que introduzcan polos jurisdiccionales especializados a escala regional para reprimir de mejor manera los ataques a los sistemas de información; insiste en la necesidad de adaptar los ordenamientos jurídicos nacionales con el fin de permitir su adaptación a los avances tecnológicos y su utilización;

29. Pide a la Comisión que continúe trabajando en pos de la coherencia y la eficiencia en Europa, de modo que se eviten iniciativas redundantes, se anime y apoye a los Estados miembros en el desarrollo de mecanismos de cooperación y se potencie el intercambio de información; considera que se debe establecer un nivel mínimo obligatorio de cooperación y puesta en común entre los Estados miembros;

30. Insta a los Estados miembros a desarrollar planes de emergencia nacionales e incluir la gestión de crisis cibernéticas en sus planes de gestión de crisis y en sus análisis de riesgo; destaca asimismo la importancia de formar adecuadamente a todo el personal de las entidades públicas en los aspectos esenciales de la ciberseguridad y, sobre todo, a ofrecer una formación adaptada a los miembros de las instituciones judiciales y de seguridad en los centros de formación; pide a la ENISA y otros organismos pertinentes que apoyen a los Estados miembros para garantizar la puesta en común de recursos y para evitar la duplicación;

31. Insta a los Estados miembros a hacer de la investigación y el desarrollo uno de los pilares centrales de la ciberseguridad y la ciberdefensa, y a fomentar la formación de ingenieros especializados en la protección de sistemas informáticos; pide a los Estados miembros que cumplan su compromiso de aumentar el gasto en defensa dedicado a la investigación y el desarrollo hasta el 2 %, prestando especial atención a la ciberseguridad y la ciberdefensa;

32. Pide a la Comisión y a los Estados miembros que propongan programas para promover y aumentar la sensibilización de los usuarios finales, tanto privados como empresariales, en cuanto a un uso seguro de Internet y de las tecnologías de la información y la comunicación; Propone que la Comisión ponga en marcha una iniciativa pública paneuropea en esta materia y pide a los Estados miembros que incluyan la educación sobre ciberseguridad en los planes de estudio desde la edad más temprana posible;

Colaboración público-privada

33. Destaca la vital importancia de una cooperación en materia de ciberseguridad significativa y complementaria entre las autoridades públicas y el sector privado, tanto a escala nacional como de la UE, con el fin de generar confianza mutua; es consciente de que el incremento de la fiabilidad y la eficiencia de las instituciones públicas pertinentes contribuirá a que se genere confianza y se comparta información;

34. Pide a los socios del sector privado que consideren soluciones de seguridad por diseño cuando ideen nuevos productos, dispositivos, servicios y aplicaciones, y creen incentivos para las personas que diseñan nuevos productos, dispositivos, servicios y aplicaciones que tengan como punto central la seguridad por diseño; pide que en la colaboración con el sector privado para prevenir ciberataques y perseguir los mismos existan estándares mínimos de transparencia y mecanismos para la rendición de cuentas;

35. Subraya que la protección de infraestructuras críticas de información está incluida en la Estrategia de Seguridad Interior de la UE con vistas a aumentar los niveles de seguridad para los ciudadanos y las empresas en el ciberespacio;

36. Pide que se establezca un diálogo permanente con estos socios sobre cómo optimizar el uso y la resiliencia de los sistemas de información y compartir la responsabilidad que exigen la estabilidad y el buen funcionamiento de esos sistemas;

37. Considera que los Estados miembros, las instituciones de la UE y el sector privado, en cooperación con la ENISA, deben adoptar medidas para aumentar la seguridad y la integridad de los sistemas de información, a fin de evitar ataques y minimizar su impacto; muestra su apoyo a la Comisión en su esfuerzo por proponer normas mínimas de ciberseguridad y sistemas de certificación para las empresas así como por ofrecer los incentivos adecuados para estimular los esfuerzos del sector privado para mejorar la seguridad;

38. Pide a la Comisión y a los Estados miembros que animen a los actores del sector privado y la sociedad civil a incluir la gestión de crisis cibernéticas en sus planes de gestión de crisis y en sus análisis de riesgo; pide, además, que se pongan en marcha formaciones para concienciar a todo su personal sobre los aspectos esenciales de la ciberseguridad y la ciberhigiene;

39. Pide a la Comisión que, en colaboración con los Estados miembros y las agencias y organismos pertinentes, desarrollen marcos e instrumentos con miras a un sistema de intercambio rápido de información que garantice el anonimato a quienes denuncien incidentes cibernéticos en el sector privado, permita a los actores públicos estar al día y preste asistencia cuando resulte necesario;

40. Destaca la necesidad de que la UE facilite el desarrollo de un mercado competitivo e innovador de la ciberseguridad en la UE de modo que las PYME puedan operar mejor en ese ámbito, lo que contribuirá a impulsar el crecimiento económico y crear más empleo;

Cooperación internacional

41. Pide al SEAE que sea proactivo en materia de ciberseguridad e incorpore la ciberseguridad a toda su actuación, en especial en relación con países terceros; pide que se acelere la cooperación y el intercambio de información sobre la forma de tratar las cuestiones de ciberseguridad con terceros países;

42. Destaca que finalizar una estrategia global de ciberseguridad de la UE es un prerrequisito para establecer el tipo de eficaz cooperación internacional en materia de ciberseguridad que requiere la naturaleza transfronteriza de las amenazas cibernéticas;

43. Pide a los Estados miembros que aún no han firmado o ratificado el Convenio sobre la

Ciberdelincuencia del Consejo de Europa (Convenio de Budapest) que lo hagan sin más demora; da su respaldo a la Comisión y al SEAE en su esfuerzo por promover el Convenio y sus valores en terceros países;

44. Es consciente de la necesidad de una respuesta acordada y coordinada internacionalmente para responder a las amenazas cibernéticas; pide, por consiguiente, a la Comisión, al SEAE y a los Estados miembros que encabecen en todos los foros, y especialmente en las Naciones Unidas, los esfuerzos por conseguir una cooperación internacional más amplia y finalmente un acuerdo sobre la definición de una visión común de normas de comportamiento en el ciberespacio, e impulsen también la cooperación para desarrollar acuerdos de control de las ciberarmas;

45. Alienta los intercambios de conocimientos en el ámbito de la ciberseguridad con países BRICS y otros países con economías emergentes, con el fin de explorar posibles respuestas comunes a las amenazas de la ciberdelincuencia y los ciberataques, que cada vez son más comunes, tanto a nivel civil como militar;

46. Insta al SEAE y a la Comisión a que sean proactivos en los foros y organizaciones internacionales relevantes, en especial las Naciones Unidas, la OSCE y la OCDE y el Banco Mundial, con el fin de aplicar el Derecho internacional vigente y consensuar normas de comportamiento responsable de los Estados en materia de ciberseguridad y ciberdefensa, coordinando las posiciones de los Estados miembros para promover los valores y políticas esenciales de la UE en el ámbito de la ciberseguridad y la ciberdefensa;

47. Pide al Consejo y a la Comisión que, en sus diálogos y relaciones y acuerdos de cooperación con terceros países, especialmente aquellos que prevén la colaboración o el intercambio en materia tecnológica, insista sobre requisitos mínimos para prevenir la ciberdelincuencia y los ciberataques y luchar contra ellos, y en normas mínimas de seguridad de los sistemas de información, y en normas mínimas de seguridad de los sistemas de información;

48. Pide a la Comisión que, cuando sea necesario, ayude a terceros países en sus esfuerzos por desarrollar sus capacidades de ciberseguridad y ciberdefensa;

Cooperación con la OTAN

49. Reitera que, sobre la base de sus valores comunes y sus intereses estratégicos, la UE y la OTAN tienen una responsabilidad y capacidad particulares para dar una respuesta más eficaz a los crecientes desafíos a la ciberseguridad, colaborando estrechamente en la búsqueda de posibles complementariedades, sin duplicación y respetando sus competencias respectivas;

50. Destaca la importancia de que en la práctica se pongan en común y se compartan recursos, dada la complementariedad de los enfoques de la UE y la OTAN en materia de ciberseguridad y ciberdefensa; destaca la necesidad de una coordinación más estrecha, en especial por lo que se refiere a la planificación, la tecnología, la formación y los equipos en lo que atañe a la ciberseguridad y la ciberdefensa;

51. Insta a todos los organismos de la UE que se ocupan de la ciberseguridad y la ciberdefensa a que, aprovechando las actuales actividades complementarias sobre desarrollo de capacidades de defensa, intensifiquen su cooperación práctica con la OTAN con miras a

intercambiar experiencias y aprender cómo dotar de resiliencia a los sistemas de la UE;

Colaboración con los Estados Unidos

52. Considera que la UE y los EE.UU. deben intensificar su cooperación mutua en la lucha contra los ciberataques y la ciberdelincuencia, ya que este aspecto se consideró una prioridad para la relación transatlántica a partir de la cumbre EU-EE.UU. de Lisboa de 2010;

53. Acoge con satisfacción la creación, en la Cumbre UE-EE.UU. de noviembre de 2010, del Grupo de trabajo UE-EE.UU. sobre ciberseguridad y ciberdelincuencia, y respalda sus esfuerzos para incluir temas relacionados con la ciberseguridad en el diálogo político transatlántico;

54. Celebra la elaboración conjunta por parte de la Comisión y el Gobierno de los Estados Unidos, bajo la égida del Grupo de trabajo UE-EE.UU., de un programa común y una hoja de ruta para realizar ciberejercicios transcontinentales conjuntos o sincronizados en 2012 y 2013; toma nota de que en 2011 tuvo lugar el primer ciberejercicio atlántico;

55. Subraya la necesidad de que los EE.UU. y la UE, como principales fuentes de ciberespacio y usuarios de Internet, colaboren en la protección de los derechos y libertades de sus ciudadanos a la hora de usar este espacio; recalca que aunque la seguridad nacional constituye un objetivo primordial, el ciberespacio no solo debe asegurarse, sino también protegerse;

o

o o

56. Encarga a su Presidente que transmita la presente Resolución al Consejo, a la Comisión, a la AR/VP, a la AED, a la ENISA y a la OTAN.