65. Destaca la necesidad de fomentar el voluntariado, en particular, durante el Año Europeo de los Ciudadanos en 2013, y pide a la Comisión que incluya el apoyo al voluntariado en las políticas internacionales de ayuda al desarrollo, sobre todo para cumplir todos los objetivos establecidos en los Objetivos de Desarrollo del Milenio;

66. Apoya un examen formal de la «Propuesta Solidaridad» para un programa interinstitucional de recursos humanos en las instituciones de la UE, a fin de facilitar la participación del personal fijo y en prácticas de las instituciones en actividades humanitarias y sociales de voluntariado, tanto como parte de la formación del personal como de las actividades de voluntariado realizadas en su tiempo libre;

67. Destaca que el programa propuesto permite ahorrar costes, representa un importante valor añadido y contribuiría a aplicar las políticas y los programas de la UE;

68. Recomienda a la Comisión que mantenga los puntos de contacto útiles establecidos con la Alianza del AEV 2011 y con la posterior plataforma de voluntariado, que incluye muchas organizaciones de voluntariado y redes de la sociedad civil, tanto con los organismos de coordinación nacionales, los socios estratégicos y los portavoces de los gobiernos nacionales en este ámbito, habida cuenta de la amplia variedad de servicios responsables del voluntariado en la UE, y alienta a estos puntos de contacto a que se comprometan con el proyecto de portal centralizado de la UE, como plataforma paneuropea, con el fin de facilitar una mayor coordinación y el aumento de la actividad transfronteriza;

69. Subraya la importancia que tienen las redes de contacto y el intercambio de buenas prácticas en la difusión de información relativa a los actuales procedimientos de la UE que pueden contribuir al voluntariado transfronterizo;

70. Pide a la Comisión que tome medidas, cuando lo estime conveniente, en relación con el programa político para el voluntariado en Europa, elaborado por las organizaciones de voluntarios que se reunieron en el marco de la Alianza del AEV 2011;

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

Protección de infraestructuras críticas de información: hacia la ciberseguridad global

P7_TA(2012)0237

Resolución del Parlamento Europeo, de 12 de junio de 2012, sobre la protección de infraestructuras críticas de información – logros y próximas etapas: hacia la ciberseguridad global (2011/2284(INI))

(2013/C 332 E/03)

El Parlamento Europeo,

— Vista su Resolución, de 5 de mayo de 2010, titulada «Una nueva agenda digital para Europa: 2015.eu» ([1]),

— Vista su Resolución, de 15 de junio de 2010, titulada «La gobernanza de Internet: los próximos pasos» ([2]),

— Vista su Resolución, de 6 de julio de 2011, titulada «Banda ancha europea: inversión en crecimiento impulsado por la tecnología digital» ([3]),

— Visto el artículo 48 de su Reglamento,

— Vistos el informe de la Comisión de Industria, Investigación y Energía, y la opinión de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (A7-0167/2012),

([1]) DO C 81 E de 15.3.2011, p. 45.
([2]) DO C 236 E de 12.8.2011, p. 33.
([3]) Textos Aprobados P7_TA(2011)0322.

A. Considerando que las tecnologías de la información y la comunicación (TIC) son capaces de desplegar todo su potencial como factores de progreso de la economía y la sociedad, únicamente cuando los usuarios confían en su seguridad y resistencia, y cuando la legislación sobre cuestiones tales como la privacidad de los datos y los derechos de propiedad intelectual se aplica de forma efectiva en el entorno de Internet;

B. Considerando que Internet y las tecnologías de la información y la comunicación (TIC) tienen cada vez un mayor impacto en diversos aspectos de la vida de los ciudadanos y constituyen un factor crucial de la interacción social, el enriquecimiento cultural y el crecimiento económico;

C. Considerando que la seguridad de las TIC y de Internet es un concepto muy amplio que incide a nivel mundial en aspectos económicos, sociales, tecnológicos y militares, que exigen una clara definición y diferenciación de las responsabilidades, así como un sólido mecanismo de cooperación internacional;

D. Considerando que el objetivo de la iniciativa emblemática Agenda Digital de la UE es impulsar la competitividad de Europa mediante el fortalecimiento de las TIC, así como crear las condiciones para un crecimiento elevado y sólido y la creación de puestos de trabajo basados en la tecnología;

E. Considerando que el sector privado sigue siendo el principal inversor, propietario y gestor de productos, servicios, aplicaciones e infraestructuras para la seguridad de la información y ha invertido miles de millones de euros en la última década; que esta participación debe reforzarse mediante estrategias políticas adecuadas para promover la resistencia de las infraestructuras que son propiedad, o están operadas, por el sector público, el privado o una combinación de ambos;

F. Considerando que el desarrollo de un alto nivel de seguridad y resistencia para redes, servicios y tecnologías de TIC aumentaría la competitividad de la economía de la UE, al mejorar tanto la evaluación como la gestión de los ciberriesgos, y al ofrecer a la economía de la UE en general infraestructuras de información más sólidas para promover la innovación y el crecimiento, generando nuevas oportunidades para que las empresas sean más productivas;

G. Considerando que los datos sobre delitos cibernéticos de las autoridades policiales y judiciales, que incluyen los ciberataques, pero también otros tipos de delitos cometidos en línea, indican que se ha producido un fuerte aumento en varios países europeos; que, no obstante, los datos estadísticamente representativos sobre ciberataques, tanto de las autoridades policiales y judiciales como del CERT (equipo de respuesta a emergencias informáticas), siguen siendo escasos y deberían recogerse mejor en el futuro, para permitir que las autoridades policiales y judiciales den una respuesta más firme en toda la UE así como respuestas legislativas mejor fundadas a las amenazas cibernéticas en constante evolución;

H. Considerando que un nivel adecuado de seguridad de la información resulta crucial para que los servicios basados en Internet se expandan con solidez;

I. Considerando que los ciberincidentes, las perturbaciones y los ataques que se han producido recientemente contra las infraestructuras de información de las instituciones, la industria y los Estados miembros de la UE ponen de manifiesto la necesidad de establecer un sistema sólido, innovador y eficaz de protección de infraestructuras críticas de información (PICI), basado en una plena cooperación internacional y en estándares mínimos de resistencia acordados por los Estados miembros;

J. Considerando que el rápido desarrollo de nuevas avenidas de las TIC, como la computación en nube, exige que se preste mayor atención a la seguridad a fin de que sea posible obtener el máximo beneficio de los avances tecnológicos;

K. Considerando que el Parlamento Europeo ha insistido en repetidas ocasiones en la aplicación de altos niveles de privacidad y protección de los datos, en la neutralidad de las redes y en la protección de los derechos de propiedad intelectual;

Medidas para reforzar la protección de infraestructuras críticas a nivel nacional y de la Unión

1. Celebra la aplicación por parte de los Estados miembros del Programa europeo para la Protección de Infraestructuras Críticas de Información (PICI), incluyendo la creación de la Red de información sobre Alertas en Infraestructuras Críticas (CIWIN);

2. Considera que los esfuerzos llevados a cabo en el marco del PICI no solo aumentarán la seguridad general de los ciudadanos, sino que también mejorarán su percepción de la seguridad y su confianza en las medidas adoptadas por el Gobierno para protegerlos;

3. Reconoce que la Comisión está estudiando la posibilidad de revisar la Directiva 2008/114/CE del Consejo ([1]), y pide que se presenten pruebas de la eficacia y las repercusiones de esta Directiva antes de seguir adelante; pide que se examine la posibilidad de ampliar su ámbito de aplicación, en concreto incluyendo al sector de las TIC y los servicios financieros; pide, además, que se preste atención a sectores como la salud, la alimentación y los sistemas de suministro de agua, la investigación nuclear y la industria, cuando no estén cubiertos por disposiciones específicas; opina que estos sectores también deberían beneficiarse del planteamiento intersectorial adoptado en la CIWIN, consistente en una cooperación, un sistema de alerta y el intercambio de mejores prácticas;

4. Subraya la importancia de establecer y asegurar la integración duradera de la investigación europea a fin de mantener y reforzar la excelencia europea en el ámbito de la protección de las infraestructuras críticas de información;

5. Pide, en vista de la naturaleza interconectada y altamente interdependiente, sensible, estratégica y vulnerable de las infraestructuras críticas de información nacionales y europeas, una actualización regular de los estándares mínimos de resistencia de preparación y respuesta frente a cualquier interrupción, incidente, intento de destrucción o ataque, como los resultantes de una infraestructura que no sea lo suficientemente robusta o de una seguridad insuficiente de las terminales;

6. Destaca la importancia de las normas y protocolos de seguridad de la información y acoge con satisfacción el mandato concedido en 2011 al CEN, al Cenelec y al ETSI para que elaboren normas de seguridad;

7. Espera que los propietarios y operadores de infraestructuras críticas de información permitan y, de ser necesario, presten asistencia a los usuarios para utilizar los medios adecuados para protegerse de ataques maliciosos o perturbaciones, mediante una supervisión tanto humana como automatizada;

8. Apoya la cooperación entre las partes interesadas, tanto públicas como privadas, a nivel de la Unión, y alienta sus esfuerzos para desarrollar y aplicar normas de seguridad y resistencia para las infraestructuras críticas de información civiles (públicas, privadas o público-privadas), nacionales y europeas;

9. 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;

10. Pide a la Comisión que evalúe, en cooperación con los Estados miembros, la aplicación del plan de acción de PICI; pide a los Estados miembros que creen CERT nacionales o gubernamentales eficaces, desarrollen estrategias nacionales de ciberseguridad, organicen periódicamente ejercicios nacionales y paneuropeos para hacer frente a ciberincidentes, elaboren planes nacionales de contingencia para ciberincidentes y contribuyan al desarrollo de un plan europeo de contingencia para ciberincidentes antes de que finalice 2012;

11. Recomienda la creación de planes de seguridad por parte de los operadores o medidas equivalentes para todas las infraestructuras críticas de información europeas, así como el nombramiento de responsables de enlace para la seguridad;

12. Acoge con beneplácito la actual revisión de la Decisión marco 2005/222/JAI del Consejo ([2]) relativa a los ataques de los que son objeto los sistemas de información; señala que es necesario coordinar los esfuerzos de la UE para luchar contra los ciberataques a gran escala, mediante la inclusión de las competencias de la ENISA, los CERT de los Estados miembros y el futuro CERT europeo;

13. Considera que la ENISA puede desempeñar un papel clave a escala europea en lo relativo a la protección de las infraestructuras críticas, ofreciendo peritajes de orden técnico a los Estados miembros y a las instituciones y organismos de la Unión Europea, así como mediante informes y análisis sobre la seguridad de los sistemas de información a escala europea y mundial;

Otras actividades de la UE para reforzar la seguridad en Internet

14. Insta a la Agencia Europea de Seguridad de las Redes y de la Información, ENISA, a que coordine y celebre anualmente el mes de concienciación sobre seguridad en Internet a nivel de la UE con objeto de llamar la atención de los Estados miembros y los ciudadanos de la UE sobre las cuestiones relacionadas con la ciberseguridad;

([1]) DO L 345 de 23.12.2008, p. 75.
([2]) DO L 69 de 16.3.2005, p. 67.

15. Apoya a la ENISA, de acuerdo con los objetivos de la Agenda Digital, en el ejercicio de sus funciones en lo relacionado con la seguridad de las redes de información y, en particular, para que ofrezca orientación y asesoramiento a los Estados miembros para que sus CERT cumplan las capacidades básicas, y apoye el intercambio de buenas prácticas mediante el desarrollo de un entorno de confianza; pide a esta Agencia que consulte a las partes interesadas con vistas a definir medidas similares de ciberseguridad para los propietarios y operadores de redes e infraestructuras privadas, y que preste asistencia a la Comisión y a los Estados miembros para que contribuyan al desarrollo y la adopción de sistemas de certificación, normas de conducta y prácticas de cooperación en materia de seguridad de la información entre los CERT nacionales y europeos y los propietarios y operadores de infraestructura y, en aquellos casos en los que sea necesario, mediante la definición de requisitos mínimos comunes que sean neutros desde el punto de vista tecnológico;

16. Acoge con satisfacción la reciente propuesta de revisión del mandato de la ENISA, en particular la extensión de éste y la ampliación de las tareas de la agencia; considera que, aparte de prestar asistencia a los Estados miembros por medio de conocimientos técnicos y análisis, la ENISA debería poder gestionar una serie de tareas ejecutivas a nivel de la UE relacionadas con la prevención y detección de incidentes de seguridad en las redes y la información, en cooperación con sus homólogos estadounidenses, y mejorar la cooperación entre los Estados miembros; señala que, de conformidad con el Reglamento ENISA, también se podrían atribuir a la agencia responsabilidades adicionales relacionadas con la respuesta a los ataques en Internet, ya que se trata de algo que, sin lugar a dudas, añade valor a los mecanismos nacionales de respuesta;

17. Acoge con beneplácito los resultados de los ejercicios paneuropeos de seguridad realizados en 2010 y 2011 en toda la Unión y supervisados por la ENISA, cuyo objetivo era ayudar a los Estados miembros a diseñar, mantener y ensayar un plan de contingencia paneuropeo; pide a la ENISA que mantenga estos ejercicios en su plan de trabajo y que involucre progresivamente a los operadores privados oportunos, según proceda, a fin de aumentar las capacidades generales europeas de seguridad en Internet; espera su expansión a nivel internacional con socios que persigan los mismos objetivos;

18. Pide a los Estados miembros que elaboren planes de contingencia nacionales en materia de ciberincidentes y que incluyan elementos clave como puntos de contacto pertinentes y disposiciones en materia de asistencia, contención y reparación en caso de ciberataques o perturbaciones de alcance regional, nacional o transfronterizo; señala que los Estados miembros también deberían establecer mecanismos y estructuras de coordinación apropiados en el plano nacional, que contribuirían a garantizar una mejor coordinación entre las autoridades nacionales competentes y a dotar de una mayor coherencia a sus acciones;

19. Sugiere que la Comisión proponga medidas vinculantes a través del plan de contingencia contra ciberincidentes de la UE para coordinar mejor a escala de la UE las funciones técnicas y de dirección entre los CERT nacionales o gubernamentales;

20. Pide a la Comisión y a los Estados miembros que adopten las medidas necesarias a fin de proteger las infraestructuras críticas frente a los ciberataques, y que prevean maneras de cerrar herméticamente el acceso a una infraestructura crítica si un ciberataque plantea una grave amenaza para su buen funcionamiento;

21. Espera que se realice plenamente el CERT de la UE, que será un factor clave para la prevención, detección, respuesta y recuperación de ciberataques mal intencionados dirigidos contra las instituciones de la UE;

22. Recomienda que la Comisión proponga medidas vinculantes destinadas a imponer estándares mínimos sobre seguridad y resistencia y a mejorar la coordinación entre los equipos de respuesta ante emergencias informáticas (CERT) nacionales;

23. Pide a los Estados miembros y a las instituciones de la UE que velen por la existencia de CERT eficaces, que cuenten con las capacidades mínimas de seguridad y resistencia basadas en las buenas prácticas acordadas; 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 confidencialidad necesarias; pide la creación de un servicio permanente de PICI en cada Estado miembro, así como el establecimiento de un protocolo europeo de emergencia para su aplicación entre los puntos de contacto nacionales;

24. Subraya que el fomento de la confianza y la promoción de la cooperación entre los Estados miembros son cruciales para proteger los datos y las redes e infraestructuras nacionales; pide a la Comisión que proponga un procedimiento común para la identificación y designación de un enfoque común para hacer frente a las amenazas transfronterizas de TIC, y espera que los Estados miembros faciliten a la Comisión información genérica sobre los riesgos y las amenazas para sus infraestructuras críticas de información, así como sus aspectos vulnerables;

25. Celebra la iniciativa de la Comisión de desarrollar un sistema europeo de intercambio de información y alerta (EISAS) para 2013;

26. Acoge con satisfacción las diversas consultas a las partes interesadas en materia de seguridad en Internet y PICI puestas en marcha por la Comisión, como la Asociación público-privada europea de resistencia; reconoce la participación y el compromiso, ya importantes, de los proveedores de TIC en dichos esfuerzos, e insta a la Comisión a que realice nuevos esfuerzos para fomentar que el mundo académico y las asociaciones de usuarios de las TIC desempeñen un papel más activo, así como para promover un diálogo constructivo con múltiples partes interesadas sobre cuestiones de ciberseguridad; apoya el desarrollo de la Asamblea Digital como marco para la gobernanza de la PICI;

27. Celebra el trabajo realizado hasta la fecha por el Foro Europeo de Estados miembros en lo referente al establecimiento de criterios específicos para el sector destinados a identificar las infraestructuras críticas europeas, concentrándose en las comunicaciones fijas y móviles, así como para debatir las directrices y principios de la UE en materia de resistencia y estabilidad de Internet; desea que continúe la constante búsqueda de consenso entre los Estados miembros, y en este contexto invita al Foro a que complemente su enfoque actual centrado en los recursos físicos con esfuerzos para incluir igualmente las infraestructuras lógicas que adquirirán cada vez más importancia para la eficacia de la PICI a medida que se desarrollen las tecnologías de virtualización y computación en nube;

28. Propone que la Comisión ponga en marcha una iniciativa pública paneuropea en materia de educación, destinada a educar y sensibilizar a los usuarios finales, tanto privados como empresariales, sobre las posibles amenazas en Internet y los dispositivos fijos y móviles de TIC a todo lo largo de la cadena de servicio, así como a promover conductas personales más seguras en línea; recuerda a este respecto los riesgos que presentan los equipos y software informáticos desfasados;

29. Pide a los Estados miembros que refuercen, con la ayuda de la Comisión, los programas de formación y educación sobre seguridad de la información dirigidos a las autoridades policiales y judiciales nacionales y a las agencias de la UE competentes;

30. Apoya la creación de un plan de estudios de la UE para expertos académicos en el ámbito de la seguridad de la información, pues tendría efectos positivos en los conocimientos técnicos y la preparación de la UE ante un ciberespacio en constante evolución y las amenazas de que puede ser objeto;

31. Aboga por el fomento de la educación en ciberseguridad (prácticas de postgrado, cursos universitarios, talleres, formación de estudiantes, etc.) y ejercicios de formación especializada en materia de PICI;

32. Pide a la Comisión que proponga, para finales de 2012, una estrategia integral de seguridad en Internet para la Unión, basada en una terminología clara; opina que la estrategia de seguridad en Internet debería estar orientada a la creación de un ciberespacio, respaldado por una infraestructura resistente y segura y normas abiertas, que favorezca la innovación y la prosperidad a través del libre flujo de información y garantice al mismo tiempo una sólida protección de la privacidad así como otras libertades civiles; mantiene que la estrategia debería detallar los principios, los objetivos, los métodos, los instrumentos y las políticas, tanto interiores como exteriores, necesarios para racionalizar los esfuerzos realizados en el plano nacional y de la UE, y para establecer estándares mínimos de resistencia entre los Estados miembros, con el objetivo de garantizar un servicio seguro, constante, sólido y resistente, ya sea en relación con las infraestructuras críticas o con el uso de Internet en general;

33. Destaca que la próxima «Estrategia de Seguridad en Internet» de la Comisión debería tomar como centro de referencia la labor en materia de CIIP y adoptar un enfoque global y sistemático de la ciberseguridad que incluya tanto medidas proactivas, por ejemplo, la introducción de pautas mínimas para las medidas de seguridad o la formación de los usuarios particulares, las empresas y las instituciones públicas, como reactivas, por ejemplo, sanciones penales, civiles y administrativas;

34. Insta a la Comisión a que proponga un mecanismo sólido para coordinar la aplicación y la actualización periódica de la estrategia de seguridad en Internet; opina que este mecanismo debería contar con el respaldo de recursos administrativos, técnicos y financieros suficientes, y tener competencias para facilitar la elaboración de las posiciones de la UE sobre cuestiones referentes a la seguridad en Internet en las relaciones con las partes interesadas tanto internas como internacionales;

35. Pide a la Comisión que proponga un marco de la UE para la notificación de las violaciones de seguridad en sectores fundamentales como la energía, el transporte y el suministro de agua y alimentos, así como en las TIC y los servicios financieros, con vistas a informar a los Estados miembros y a los usuarios de incidentes, ataques y perturbaciones de carácter cibernético;

36. Insta a la Comisión a que mejore la disponibilidad de datos estadísticamente representativos sobre los costes de los ciberataques en la UE, los Estados miembros y la industria, en particular en el sector de los servicios financieros y de las TIC, mediante la mejora de las capacidades de recopilación de datos del futuro Centro Europeo contra la Ciberdelincuencia, cuya creación se prevé en 2013, de los CERT y de otras iniciativas de la Comisión, como el sistema europeo de intercambio de información y alerta, a fin de garantizar una transmisión y un intercambio de datos sistemáticos sobre ciberataques y otras formas de ciberdelincuencia que afecten a la industria europea y a los Estados miembros, así como para reforzar la observancia de la ley;

37. Aboga por una estrecha relación e interacción entre los sectores privados nacionales y la ENISA para la interfaz del CERT nacional/gubernamental con el desarrollo del Sistema Europeo de Intercambio de Información y Alerta (EISAS);

38. Señala que el principal motor del desarrollo y uso de tecnologías diseñadas para aumentar la seguridad en Internet es el sector de las TIC; recuerda que las políticas de la UE deben evitar ser un obstáculo para el crecimiento de la economía europea de Internet e incluir los incentivos necesarios para explotar plenamente el potencial de empresas y asociaciones público-privadas; recomienda que se estudien otros incentivos para que el sector desarrolle planes de seguridad más sólidos para operadores de conformidad con la Directiva 2008/114/CE;

39. Pide a la Comisión que presente una propuesta legislativa para la ulterior tipificación de los ciberataques ((es decir, spear-phishing, fraude en línea, etc.);

Cooperación internacional

40. Recuerda que la cooperación internacional es el instrumento central para la introducción de unas medidas efectivas de ciberseguridad; reconoce que, en estos momentos, la UE no participa de forma activa y constante en los diálogos y procesos de cooperación internacional en materia de ciberseguridad; pide a la Comisión y al Servicio Europeo de Acción Exterior (SEAE) que inicien un diálogo constructivo con todos los países con ideas afines, y ello con vistas a desarrollar un entendimiento común y políticas orientadas a aumentar la resistencia de Internet y de las infraestructuras fundamentales; mantiene que, al mismo tiempo, la UE debería incluir las cuestiones de seguridad en Internet, de forma permanente, en el ámbito de aplicación de sus relaciones exteriores, entre otras cosas a la hora de diseñar diversos instrumentos de financiación o celebrar acuerdos internacionales que contemplen el intercambio y almacenamiento de datos sensibles;

41. Toma nota de los positivos logros del Convenio del Consejo de Europa sobre la ciberdelincuencia celebrado en Budapest en 2001; señala, no obstante, que, aunque alienta a más países a que firmen y ratifiquen este Convenio, el SEAE debería celebrar también acuerdos bilaterales y multilaterales sobre seguridad y resistencia en Internet con socios internacionales que persigan los mismos objetivos;

42. Señala que las innumerables actividades en curso llevadas a cabo por diferentes instituciones, organismos y agencias internacionales y de la UE, así como por los Estados miembros, requieren coordinación a fin de evitar la duplicación, para lo cual cabe considerar la designación de un funcionario responsable de la coordinación, posiblemente a través del nombramiento de un coordinador de ciberseguridad de la UE;

43. Subraya la importancia de un diálogo estructurado entre los principales actores y legisladores de la UE y los EE UU que intervienen en la CIIP intercontinental, para llegar a un entendimiento, una interpretación y una posición comunes respecto del marco jurídico y de gestión;

44. 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 seguridad en Internet en el diálogo político transatlántico; 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;

45. Sugiere el establecimiento de un diálogo estructurado entre los legisladores de la UE y los Estados Unidos, a fin de debatir cuestiones relacionadas con Internet como parte de una búsqueda de un entendimiento, una interpretación y unas posiciones comunes;

46. Insta al SEAE y a la Comisión, en base del trabajo realizado por el Foro Europeo de Estados miembros, a que aseguren una posición activa dentro de los correspondientes foros internacionales, entre otras cosas mediante la coordinación de las posiciones de los Estados miembros, con vistas a promover los principales valores, objetivos y políticas de la UE en materia de seguridad y resistencia en Internet; señala que estos foros incluyen la OTAN, las Naciones Unidas (en particular a través de la Unión Internacional de Telecomunicaciones y el Foro para la Gobernanza de Internet), la Corporación de Asignación de Nombres y Números de Internet, la Autoridad de Número Asignado por Internet, la OSCE, la OCDE y el Banco Mundial;

47. Insta a la Comisión y a la ENISA a que participen en los principales diálogos entre las partes interesadas para definir las normas técnicas y legales del ciberespacio a nivel internacional;

*

* *

48. Encarga a su Presidente que transmita la presente Resolución al Consejo y a la Comisión.

Cooperación en materia de política energética con socios más allá de nuestras fronteras

P7_TA(2012)0238

Resolución del Parlamento Europeo, de 12 de junio de 2012, sobre Cooperar en materia de política energética con socios más allá de nuestras fronteras: una estrategia para un suministro energético seguro, sostenible y competitivo (2012/2029(INI))

(2013/C 332 E/04)

El Parlamento Europeo,

— Vista la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones sobre la seguridad del abastecimiento energético y la cooperación internacional: «La política energética de la UE: establecer asociaciones más allá de nuestras fronteras» (COM(2011)0539),

— Vista la propuesta de Decisión del Parlamento Europeo y del Consejo por la que se establece un mecanismo de intercambio de información con respecto a los acuerdos intergubernamentales entre los Estados miembros y terceros países en el sector de la energía (COM (2011)0540),

— Vistas las conclusiones del Consejo de 24 de noviembre de 2011 sobre la seguridad del abastecimiento energético y la cooperación internacional: «La política energética de la UE: establecer asociaciones más allá de nuestras fronteras»,

— Vista su resolución de 25 de noviembre de 2010 sobre una nueva estrategia energética para Europa 2011-2020 ([1]),

— Visto el artículo 48 de su Reglamento,

— Vistos el informe de la Comisión de Industria, Investigación y Energía y las opiniones de la Comisión de Asuntos Exteriores y de la Comisión de Comercio Internacional (A7-0168/2012),

([1]) DO C 99 E de 3.4.2012, p. 64.