Parlamento Europeo
2014-2019

Documento de sesión

B8-0155/2019

6.3.2019

PROPUESTA DE RESOLUCIÓN

tras las declaraciones del Consejo y de la Comisión

presentada de conformidad con el artículo 123, apartado 2, del Reglamento interno

sobre las amenazas en materia de seguridad relacionadas con la creciente presencia tecnológica de China en la Unión y la posible acción a escala de la Unión para reducirlas
(2019/2575(RSP))

Luděk Niedermayer, Angelika Niebler, Ivo Belet, Paul Rübig
en nombre del Grupo PPE

B8-0155/2019

Resolución del Parlamento Europeo sobre las amenazas en materia de seguridad relacionadas con la creciente presencia tecnológica de China en la Unión y la posible acción a escala de la Unión para reducirlas
(2019/2575(RSP))

El Parlamento Europeo,

– Vista la Directiva (UE) 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas[1],

– Vista la Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión[2],

– 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[3],

– Vista la propuesta de Reglamento del Parlamento Europeo y del Consejo, de 13 de septiembre de 2017, relativo a ENISA, la «Agencia de Ciberseguridad de la UE», y por el que se deroga el Reglamento (UE) n.º 526/2013, y relativo a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación («Reglamento de Ciberseguridad»), presentada por la Comisión (COM(2017)0477),

– Vista la propuesta de Reglamento del Parlamento Europeo y del Consejo, de 12 de septiembre de 2018, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación, presentada por la Comisión (COM(2018)0630),

– Vista la adopción de la nueva Ley de Inteligencia Nacional por la Asamblea Popular Nacional China el 28 de junio de 2017,

– Vistas las declaraciones del Consejo y de la Comisión, de 13 de febrero de 2019, sobre las amenazas en materia de seguridad relacionadas con la creciente presencia tecnológica de China en la Unión y la posible acción a escala de la Unión para reducirlas,

– Vista la aprobación, por parte del Gobierno australiano, de las reformas del sector de las telecomunicaciones del Gobierno, en vigor desde el 18 de septiembre de 2018,

– Vista su Posición aprobada en primera lectura el 14 de febrero de 2019 sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establece

[1] DO L 321 de 17.12.2018, p. 36
[2] DO L 194 de 19.7.2016, p. 1
[3] DO L 218 de 14.8.2013, p. 8.

un marco para el control de las inversiones extranjeras directas en la Unión Europea[4],

– Vistas sus resoluciones sobre las relaciones entre la Unión y China, en especial la de 12 de septiembre de 2018 sobre el estado de las relaciones UE-China[5],

– Vista la Comunicación de la Comisión, de 14 de septiembre de 2016, titulada «La 5G para Europa: un plan de acción» (COM(2016)0588),

– Vista su Resolución, de 1 de junio de 2017, sobre la conectividad a internet para el crecimiento, la competitividad y la cohesión: la sociedad europea del gigabit y 5G[6],

– Visto el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)[7],

– Visto el Reglamento (UE) n.º 1316/2013 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2013, por el que se crea el Mecanismo «Conectar Europa», por el que se modifica el Reglamento (UE) n.º 913/2010 y por el que se derogan los Reglamentos (CE) n.º 680/2007 y (CE) n.º 67/2010[8],

– Vista la propuesta de la Comisión de Reglamento del Parlamento Europeo y del Consejo por el que se establece el programa Europa Digital para el período 2021-2027 (COM(2018)0434),

– Visto el artículo 123, apartado 2, de su Reglamento interno,

A. Considerando que la Unión Europea debe impulsar su agenda de ciberseguridad para desarrollar su potencial de desempeñar una posición de liderazgo en ciberseguridad y aprovecharla en beneficio de su industria;

B. Considerando que podrían aprovecharse las vulnerabilidades de las redes 5G para poner en peligro los sistemas informáticos, lo que podría provocar daños muy graves a las economías a escala europea y nacional; que es necesario un enfoque basado en el análisis de riesgos en toda la cadena de valor a fin de minimizar estos riesgos;

C. Considerando que la red 5G será la columna vertebral de nuestra infraestructura digital, pues ampliará la posibilidad de conectar varios dispositivos a las redes (internet de las cosas, etc.), y aportará nuevos beneficios y oportunidades a la sociedad y a las empresas en muchos ámbitos, en especial en sectores vitales de la economía como el transporte, la energía, la salud, las finanzas, las telecomunicaciones, la defensa, el espacio y la seguridad;

D. Considerando que el establecimiento de un mecanismo adecuado para responder a los

[4] Textos Aprobados, P8_TA(2019)0121.
[5] Textos Aprobados, P8_TA(2018)0343.
[6] DO C 307 de 30.8.2018, p. 144.
[7] DO L 119 de 4.5.2016, p. 1.
[8] DO L 348 de 20.12.2013, p. 129.

desafíos de seguridad ofrecerá a la Unión la oportunidad de tomar medidas activamente para establecer normas aplicables a la 5G;

E. Considerando las preocupaciones planteadas acerca de los vendedores de equipos de terceros países que pueden presentar un riesgo para la seguridad de la Unión debido a las leyes de su país de origen, en especial tras la entrada en vigor de la Ley china de seguridad del Estado, que prevé obligaciones para todos los ciudadanos, las empresas y otras entidades de cooperar con el Estado para salvaguardar la seguridad estatal; que no hay garantías de que estas obligaciones carezcan de aplicación extraterritorial, y que los distintos países han reaccionado ante las normativas chinas de distintas maneras, desde la realización de evaluaciones de seguridad hasta la prohibición absoluta;

F. que, en diciembre de 2018, la autoridad nacional checa de ciberseguridad emitió una advertencia contra las amenazas para la seguridad planteadas por las tecnologías proporcionadas por las empresas chinas Huawei y ZTE; que, posteriormente, en enero de 2019, las autoridades fiscales checas excluyeron a Huawei de una licitación para construir un portal para fines tributarios;

G. Considerando que es necesaria una investigación exhaustiva para aclarar si los dispositivos implicados o bien otros dispositivos o proveedores plantean riesgos para la seguridad debido a características tales como las puertas traseras a los sistemas;

H. Considerando que las soluciones deben coordinarse y tratarse al nivel de la Unión a fin de evitar distintos niveles de seguridad y posibles lagunas en materia de ciberseguridad; que la coordinación también es necesaria al nivel mundial a fin de ofrecer una respuesta firme;

I. Considerando que los beneficios del mercado único están acompañados de la obligación de cumplir las normas de la Unión y su marco jurídico, y que los proveedores no deben recibir un trato diferente según su país de origen;

J. Considerando que el Reglamento sobre el control de las inversiones extranjeras directas, que debería entrar en vigor antes de finales de 2020, refuerza la posibilidad de los Estados miembros de controlar la inversión extranjera sobre la base de la seguridad y el orden público y establece un mecanismo de cooperación que permite a la Comisión y a los Estados miembros cooperar en la evaluación de los riesgos para la seguridad, en particular para la ciberseguridad, que plantean las inversiones extranjeras, y cubre también proyectos y programas de interés para la Unión, como las redes transeuropeas de telecomunicaciones y Horizonte 2020;

1. Estima que la Unión debe asumir el liderazgo en materia de ciberseguridad con un planteamiento común basado en el uso eficaz y eficiente de los conocimientos especializados de la Unión, los Estados miembros y el sector, dado que un mosaico de decisiones nacionales divergentes perjudicaría al mercado único digital;

2. Expresa su profunda preocupación por las recientes acusaciones de que los equipos 5G desarrollados por empresas chinas incluyen «puertas traseras» que permitirían a los fabricantes y a las autoridades acceder sin autorización a los datos y las telecomunicaciones de ciudadanos y empresas de la Unión;

3. Manifiesta igualmente su inquietud ante la presencia potencial de grandes vulnerabilidades en los equipos 5G desarrollados por dichos fabricantes si se instalaran en el despliegue de las redes 5G en los próximos años;

4. Subraya que las implicaciones para la seguridad de redes y equipos son similares en todo el mundo, y pide a la Unión que extraiga enseñanzas de la experiencia de que dispone a fin de garantizar los niveles más elevados de ciberseguridad; pide a la Comisión que elabore una estrategia para situar a Europa en la vanguardia de la tecnología de ciberseguridad con el objetivo de reducir la dependencia de Europa de la tecnología extranjera en el ámbito de la ciberseguridad;

5. Pide a los Estados miembros que informen a la Comisión de toda medida nacional que tengan intención de adoptar, a fin de coordinar la respuesta de la Unión y así garantizar los más altos niveles de ciberseguridad en toda la Unión, y reitera la importancia de abstenerse de introducir medidas unilaterales desproporcionadas que fragmenten el mercado único;

6. Reitera que toda entidad que suministre equipos o servicios en la Unión, independientemente de su país de origen, debe respetar las obligaciones en materia de derechos fundamentales y las legislaciones de la Unión y de los Estados miembros, incluido el marco jurídico en materia de privacidad, protección de datos y ciberseguridad;

7. Pide a la Comisión que evalúe la solidez del marco jurídico de la Unión a fin de atender la preocupación por la presencia de equipos vulnerables en sectores estratégicos e infraestructuras troncales; insta a la Comisión a que presente iniciativas, incluidas propuestas legislativas cuando proceda, a fin de abordar con prontitud las deficiencias detectadas, ya que la Unión se encuentra en un proceso permanente de detección y corrección de los desafíos en materia de ciberseguridad, y de mejora de la resiliencia de la ciberseguridad en la Unión;

8. Insta a aquellos Estados miembros que aún no hayan incorporado a su legislación la Directiva (UE) 2016/1148, relativa a la seguridad de las redes y sistemas de información (SRI), a que lo hagan sin demora, y pide a la Comisión que supervise estrechamente esta transposición a fin de garantizar que sus disposiciones se cumplen correctamente y que los ciudadanos europeos están mejor protegidos frente a las amenazas para la seguridad externas e internas;

9. Insta a la Comisión y a los Estados miembros a que se aseguren de que los mecanismos de notificación introducidos por la Directiva SRI se aplican correctamente. señala que la Comisión y los Estados miembros deben realizar un seguimiento exhaustivo de todos los incidentes de seguridad o reacciones inadecuadas de los proveedores a fin de corregir las deficiencias detectadas;

10. Pide a la Comisión que evalúe la necesidad de ampliar el ámbito de aplicación de la Directiva a otros sectores y servicios críticos que no están cubiertos por una legislación específica, como la infraestructura de red;

11. Celebra y apoya el acuerdo alcanzado en relación con el Reglamento de Ciberseguridad y el fortalecimiento del mandato de la Agencia de Seguridad de las Redes y de la

Información de la Unión Europea (ENISA), con vistas a brindar un mejor apoyo a los Estados miembros en la lucha contra las amenazas para la ciberseguridad y los ataques;

12. Recuerda que la ciberseguridad exige unos requisitos de seguridad muy estrictos; aboga por una red segura desde el diseño y por defecto; insta a los Estados miembros a que, junto con la Comisión, estudien todos los medios disponibles para garantizar un alto nivel de seguridad;

13. Insta a la Comisión a que encargue a la ENISA que dé prioridad a trabajar sobre un sistema de certificación para los equipos 5G a fin de garantizar que el despliegue de la 5G en la Unión respete las normas de seguridad más estrictas y sea resistente a las puertas traseras y otras vulnerabilidades importantes que puedan poner en peligro la seguridad de las redes de telecomunicaciones de la Unión y de los servicios dependientes; recomienda dedicar especial atención a los procesos, productos y programas informáticos de uso común que, por su magnitud, tienen un impacto importante en la vida cotidiana de los ciudadanos y la economía;

14. Acoge con gran satisfacción las propuestas sobre los centros de competencias en materia de ciberseguridad y una red de centros nacionales de coordinación, concebida para ayudar a la Unión a conservar y desarrollar las capacidades tecnológicas e industriales en materia de ciberseguridad necesarias para la seguridad de su mercado único digital;

15. Reafirma su posición sobre el programa Europa Digital, que impone requisitos de seguridad y la supervisión de la Comisión a entidades establecidas en la Unión pero controladas desde terceros países, en especial en acciones relacionadas con la ciberseguridad;

16. Pide a los Estados miembros que garanticen que las instituciones públicas y las empresas privadas que trabajan para garantizar el correcto funcionamiento de redes de infraestructuras críticas, tales como las telecomunicaciones, la energía y los sistemas sanitarios y sociales, efectúen evaluaciones pertinentes de riesgos teniendo en cuenta las amenazas para la seguridad vinculadas con las características técnicas de cada sistema o la dependencia de proveedores externos de tecnologías de equipos y programas informáticos;

17. Recuerda que el vigente marco jurídico en materia de telecomunicaciones encomienda a los Estados miembros velar por que los operadores de telecomunicaciones garanticen la integridad y disponibilidad de las redes públicas de comunicaciones electrónicas; destaca que, con arreglo al Código Europeo de las Comunicaciones Electrónicas, los Estados miembros disponen de todas las competencias necesarias para investigar y aplicar una amplia gama de medidas en caso de presencia de productos no conformes en el mercado de la Unión;

18. Pide a la Comisión y a los Estados miembros que hagan de la seguridad un aspecto obligatorio de todos los procedimientos de contratación pública relativos a las infraestructuras pertinentes, tanto a nivel de la Unión como nacional;

19. Pide a la Comisión y a los Estados miembros que aumenten la transparencia y la seguridad mediante el desarrollo de procedimientos de contratación en varias fases para

las infraestructuras de TIC, lo que permitiría distinguir las ofertas relativas a la arquitectura, la producción, la explotación y el mantenimiento de estos sistemas y a cada proveedor de tecnología;

20. Recuerda a los Estados miembros las obligaciones que les incumben en virtud del Derecho penal de la Unión de imponer sanciones, en particular multas de carácter penal o de otro tipo, a las personas jurídicas que hayan cometido delitos tales como ataques contra los sistemas de información, interferencia ilegal en los sistemas de información, interferencia ilegal en los datos e interceptación ilegal; resalta que los Estados miembros también deben hacer uso de la posibilidad de imponer otras sanciones a esas entidades jurídicas, como la inhabilitación temporal o permanente para el ejercicio de actividades comerciales;

21. Confía en que las autoridades nacionales de protección de datos y el Supervisor Europeo de Protección de Datos investiguen a fondo los indicios de violación de la seguridad de los datos por parte de proveedores externos e impongan penalizaciones y sanciones adecuadas en consonancia con la legislación europea en materia de protección de datos;

22. Acoge con satisfacción la próxima entrada en vigor de un Reglamento por el que se establece un marco para el control de las inversiones extranjeras directas por motivos de seguridad y orden público, y subraya que este Reglamento establece, por primera vez, una lista de ámbitos y factores, incluidas las comunicaciones y la ciberseguridad, pertinentes a efectos de seguridad y orden público a escala de la Unión;

23. Reitera que la Unión debe apoyar la ciberseguridad en toda la cadena de valor, desde la investigación hasta el despliegue y la adopción de tecnologías clave, difundir información pertinente y promover la ciberhigiene y un plan de estudios sobre ciberseguridad, y considera que, entre otras medidas, el programa Europa Digital será una herramienta eficiente para ello;

24. Insta a la Comisión y a los Estados miembros a que adopten las medidas necesarias, incluidos sistemas de inversión sólidos, para crear en la Unión un entorno favorable a la innovación al que puedan acceder todas las empresas de la economía digital de la Unión, incluidas las pequeñas y medianas empresas (pymes); insta asimismo a que dicho entorno permita a los proveedores europeos desarrollar nuevos productos, servicios y tecnologías que les permitan ser competitivos;

25. Encarga a su presidente que transmita la presente Resolución al Consejo y a la Comisión.