Európai Parlament
2014-2019

Plenárisülés-dokumentum

B8-0153/2019

6.3.2019

ÁLLÁSFOGLALÁSI INDÍTVÁNY

benyújtva a Tanács és a Bizottság nyilatkozatait követően

az eljárási szabályzat 123. cikkének (2) bekezdése alapján

on security threats connected with the rising Chinese technological presence in the EU and possible action at EU level to reduce them
(2019/2575(RSP))

Tiziana Beghin, Dario Tamburrano, Isabella Adinolfi, Rolandas Paksas
az EFDD képviselőcsoport nevében

B8-0153/2019

European Parliament resolution on security threats connected with the rising Chinese technological presence in the EU and possible action at EU level to reduce them (2019/2575(RSP))

Az Európai Parlament,

– having regard to the Commission communications of 14 September 2016 entitled ‘Connectivity for a Competitive Digital Single Market – Towards a European Gigabit Society’ (COM(2016)0587) and ‘5G for Europe: An Action Plan’ (COM(2016)0588),

– having regard to the Commission’s amended proposal for a regulation of the European Parliament and of the Council, of 29 January 2016, on the access of third-country goods and services to the Union’s internal market in public procurement and procedures supporting negotiations on access of Union goods and services to the public procurement markets of third countries (COM(2016)0034),

– having regard to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union[1] (NIS Directive),

– having regard to the proposal for a regulation of the European Parliament and of the Council, of 13 September 2017, on ENISA, the ‘EU Cybersecurity Agency’, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (‘Cybersecurity Act’) (COM(2017)0477),

– having regard to Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code[2],

– having regard to the Commission proposal for a regulation of the European Parliament and of the Council, of 12 September 2018, establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (COM(2018)0630),

– having regard to the WTO dispute settlement case (WT/DS549/6) of 1 June 2018 concerning certain measures imposed by China pertaining to the transfer of foreign technology into China,

– having regard to its position adopted at first reading on 14 February 2019 on the proposal for a regulation of the European Parliament and of the Council establishing a framework for the screening of foreign direct investments into the European Union[3],

– having regard to the current negotiations between the EU and China for a Comprehensive Agreement on Investment,

[1] OJ L 194, 19.7.2016, p. 1.
[2] OJ L 321, 17.12.2018, p. 36.
[3] Texts adopted, P8_TA(2019)0121.

– tekintettel eljárási szabályzata 123. cikkének (2) bekezdésére,

A. whereas recent advancements in ICT, including fifth-generation telecommunications (5G), have paved new ways for the production, distribution and fruition of goods and services, and for interaction among devices and among citizens, public administrations and other socio-economic actors, and hence have the potential to boost the European economy;

B. whereas cybersecurity in ICT, protection of sensitive information, respect for individual rights and safeguarding from external cyber-threats are preconditions for securing the technological sovereignty of EU citizens and ultimately bringing prosperity to, and supporting democracy in, the EU;

C. whereas 5G research and testing are barely keeping pace with the international pressure for the deployment and commercialisation of 5G, while a number of scientific studies have raised concerns and uncertainties with regard to both its security and its safety, especially as far as the risks of electromagnetic pollution for human health and the environment are concerned;

D. whereas ensuring cybersecurity for 5G networks is a new and complex challenge owing to 5G's virtualised and decentralised nature and its fragmented and highly specialised value chain, from production to dispatch, installation, configuration, operations, maintenance and software updates; whereas the EU needs to fill the cybersecurity gap in its critical infrastructure in the telecommunications, energy, transport, health, defence and security sectors, among others;

E. whereas ensuring safe and secure 5G networks is a task that cannot be accomplished by individual manufacturers or system operators, but requires effective coordinated action by all relevant national and international authorities;

F. whereas the EU has the potential to lead the development of cybersecurity technologies by supporting European enterprises in this sector and promoting all changes in the value chain that could decrease the EU's dependence on foreign technology;

G. whereas the EU has been developing a set of measures to ensure cybersecurity, including the NIS Directive and the Cybersecurity Act, which should be swiftly implemented and continuously monitored in order to ensure that they remain effective throughout the necessary updates and reviews;

H. whereas an increased presence of Chinese and other third-country technology providers has become apparent in the EU 5G market, notably of state-owned enterprises or businesses lacking transparency;

I. whereas reciprocity is one of the most effective ways to make progress towards a global level playing field;

J. whereas foreign companies have to deal with the current gap in EU data protection standards between the General Data Protection Regulation and different requirements

under national laws;

K. whereas the EU and China have been negotiating a Comprehensive Agreement on Investment since 2013; whereas the proposed deal would help resolve market access issues, establish a framework for investment protection, and set basic labour and environmental standards;

L. whereas evidence, albeit inconclusive, has emerged with regard to security lapses in the equipment provided by third-country suppliers, including China, which could endanger individual rights to privacy and the protection of sensitive information in the EU;

1. Stresses that the deployment and commercialisation of 5G should be conducted in accordance with the precautionary principle, with all socio-economic actors anticipating potential safety and security impacts and taking proportionate precautions, including the prompt disclosure of factors that might endanger public health or the environment;

2. Stresses that the social and economic impacts of 5G and of the technologies that it enables, from the Internet of Things to artificial intelligence, should be thoroughly assessed, and that measures should be taken in order for the transition to the European Gigabit Society to take place in a way that is fair and equal for all and based on ethical responsibility;

3. Calls on the Commission and the Member States to create an innovation-friendly environment for EU vendors to develop new products, services and technologies, and to support EU entrepreneurship in the deployment and commercialisation of safe and secure 5G, while ensuring that its potential is accessible to all businesses in the EU digital economy, including small and medium-sized enterprises;

4. Recalls that cybersecurity is one of the main challenges the EU is currently facing and that failure in this area could violate the privacy and fundamental rights of EU consumers and producers, seriously undermine the trust of citizens in ICT products and services, and ultimately cause serious economic damage; calls for a network that is secure by default and by design;

5. Calls on the Commission and the Member States to cooperate closely in implementing the EU's cybersecurity strategy, and to combine EU and national measures in order to minimise the risk of security lapses and data breaches across the entire value chain; considers that such measures could include EU cybersecurity certification, configuration requirements and operational procedures and practices, as well as the promotion of cyber hygiene and digital education;

6. Believes that the EU's cybersecurity agency (the European Union Agency for Network and Information Security - ENISA) has a crucial role to play in analysing possible threats arising from foreign vendors, including China, and coordinating a common approach between Member States to tackle cybersecurity threats and attacks;

7. Calls on the Commission and the Member States to swiftly implement the Circular Economy package and to boost raw materials management throughout their lifecycle. as well as the recycling of waste, so as to improve EU access to critical raw materials, which are fundamental for high-tech products and emerging innovations;

8. Considers it urgent to deal with the possible technological security threats posed by the current EU market penetration of foreign vendors, including China, by taking a common approach on security and data protection between Member States;

9. Calls on the Commission and the Member States to analyse and monitor the security of those ICT systems where third-country technologies are strongly present, also by performing stress tests;

10. Stresses that third-country suppliers should not be discriminated against on the grounds of their country of origin, but that the transparency of these companies, their cybersecurity standards and the existence of reciprocal conditions for European companies in the country of origin should be taken into account, in order to ensure a level playing field;

11. Stresses that under no circumstances should Chinese or other third-country suppliers and operators endanger the individual rights guaranteed under EU law, even where different requirements exist under national law in their country of origin;

12. Asks the Council to positively consider the reopening of discussions on the new revised Commission proposal on the procedure restricting the access of foreign products to the EU procurement market where there is a lack of reciprocal accession;

13. Recalls the importance of further improving negotiations on regulatory cooperation on digital technology with third countries and of ensuring greater engagement on their part in international standards-setting bodies;

14. Instructs its President to forward this resolution to the Council and the Commission.