

Tuesday 12 March 2019

I

(Resolutions, recommendations and opinions)

RESOLUTIONS

EUROPEAN PARLIAMENT

P8_TA(2019)0156

Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them**European Parliament resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them (2019/2575(RSP))**

(2021/C 23/01)

The European Parliament,

- 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 ⁽¹⁾,
- 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 ⁽²⁾,
- having regard to Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA ⁽³⁾,
- having regard to the Commission 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) No 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act') (COM(2017)0477),
- having regard to the Commission proposal of 12 September 2018 for a regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (COM(2018)0630),
- having regard to the adoption of the new National Intelligence Law by the Chinese National People's Congress on 28 June 2017,
- having regard to the statements by the Council and the Commission of 13 February 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them,

⁽¹⁾ OJ L 321, 17.12.2018, p. 36.

⁽²⁾ OJ L 194, 19.7.2016, p. 1.

⁽³⁾ OJ L 218, 14.8.2013, p. 8.

Tuesday 12 March 2019

- having regard to the adoption by the Australian Government of the Government's Telecommunications Sector Security Reforms, which entered into force on 18 September 2018,
 - 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 ⁽¹⁾,
 - having regard to its previous resolutions on the state of EU-China relations, in particular that of 12 September 2018 ⁽²⁾,
 - having regard to the Commission communication of 14 September 2016 entitled '5G for Europe: an action plan' (COM(2016)0588),
 - having regard to its resolution of 1 June 2017 on internet connectivity for growth, competitiveness and cohesion: European gigabit society and 5G ⁽³⁾,
 - having regard to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ⁽⁴⁾,
 - having regard to Regulation (EU) No 1316/2013 of the European Parliament and of the Council of 11 December 2013 establishing the Connecting Europe Facility, amending Regulation (EU) No 913/2010 and repealing Regulations (EC) No 680/2007 and (EC) No 67/2010 ⁽⁵⁾,
 - having regard to the Commission proposal of 6 June 2018 for a regulation of the European Parliament and of the Council establishing the Digital Europe programme for the period 2021-2027 (COM(2018)0434),
 - having regard to Rules 123(2) and (4) of its Rules of Procedure,
- A. whereas the EU must drive forward its cybersecurity agenda in order to fulfil its potential in becoming a leading player in cybersecurity and use this to its industry's advantage;
- B. whereas vulnerabilities in 5G networks could be exploited in order to compromise IT systems, potentially causing very serious damage to economies at European and national levels; whereas a risk analysis-based approach across the value chain is necessary in order to minimise the risks;
- C. whereas the 5G network will be the backbone of our digital infrastructure, extending the possibility to connect various devices to networks (internet of things, etc.), and will bring new benefits and opportunities to society and businesses in many areas, including critical sectors of the economy such as the transport, energy, health, finance, telecoms, defence, space and security sectors;
- D. whereas establishing an appropriate mechanism to respond to security challenges would give the EU the opportunity to actively take steps in setting standards for 5G;
- E. whereas concerns were raised about third-country equipment vendors that might present a security risk for the EU due to the laws of their country of origin, especially after the enactment of the Chinese State Security Laws, which impose obligations on all citizens, enterprises and other entities to cooperate with the state to safeguard state security, in connection with a very broad definition of national security; whereas there is no guarantee that these obligations are not applied extraterritorially, and whereas reactions to the Chinese laws have varied in different countries, ranging from security assessments to outright bans;

⁽¹⁾ Texts adopted, P8_TA(2019)0121.

⁽²⁾ Texts adopted, P8_TA(2018)0343.

⁽³⁾ OJ C 307, 30.8.2018, p. 144.

⁽⁴⁾ OJ L 119, 4.5.2016, p. 1.

⁽⁵⁾ OJ L 348, 20.12.2013, p. 129.

Tuesday 12 March 2019

- F. whereas in December 2018, the Czech national authority for cybersecurity issued a warning against security threats posed by the technologies provided by the Chinese companies Huawei and ZTE; whereas subsequently, in January 2019, the Czech tax authorities excluded Huawei from a tender to build a tax portal;
 - G. whereas a thorough investigation is needed to clarify whether the devices involved, or any other devices or suppliers, pose security risks due to features such as backdoors to systems;
 - H. whereas solutions should be coordinated and dealt with at EU level in order to avoid creating different levels of security and potential gaps in cybersecurity, while coordination at a global level is needed in order to provide a strong response;
 - I. whereas the benefits of the single market come with the obligation to comply with EU standards and the Union's legal framework, and whereas suppliers should not be treated differently on the basis of their country of origin;
 - J. whereas the regulation on screening of foreign direct investment, which should enter into force by the end of 2020, reinforces Member States' ability to screen foreign investment based on security and public order criteria, and establishes a cooperation mechanism which allows the Commission and the Member States to cooperate in their assessment of security risks, including cybersecurity risks, posed by sensitive foreign investments, and also covers projects and programmes that are of EU interest, such as the Trans-European Telecommunications Networks and Horizon 2020;
-
- 1. Believes that the Union must take the lead on cybersecurity, by means of a common approach based on the effective and efficient use of EU, Member State and industry expertise, since a patchwork of divergent national decisions would be detrimental to the digital single market;
 - 2. Expresses deep concern about the recent allegations that 5G equipment developed by Chinese companies may have embedded backdoors that would allow manufacturers and authorities to have unauthorised access to private and personal data and telecommunications from the EU;
 - 3. Is equally concerned about the potential presence of major vulnerabilities in the 5G equipment developed by these manufacturers if they were to be installed when rolling out 5G networks in the coming years;
 - 4. Underlines that the implications for the security of networks and equipment are similar around the world and calls for the EU to draw lessons from the experience available, in order to be able to ensure the highest standards of cybersecurity; calls on the Commission to develop a strategy that puts Europe in a leading position in cybersecurity technology and is aimed at reducing Europe's dependency on foreign technology in the field of cybersecurity; is of the view that whenever compliance with security requirements cannot be guaranteed adequate measures must be applied;
 - 5. Calls on the Member States to inform the Commission of any national measure they intend to adopt in order to coordinate the Union's response so as to ensure the highest standards of cybersecurity throughout the Union, and reiterates the importance of refraining from introducing disproportionate unilateral measures that would fragment the single market;
 - 6. Reiterates that any entities providing equipment or services in the EU, irrespective of their country of origin, must comply with fundamental rights obligations and with EU and Member State law, including the legal framework as regards privacy, data protection and cybersecurity;
 - 7. Calls on the Commission to assess the robustness of the Union's legal framework in order to address concerns about the presence of vulnerable equipment in strategic sectors and backbone infrastructure; urges the Commission to present initiatives, including legislative proposals where appropriate, to address in due time any shortfalls detected, since the Union is in a constant process of identifying and addressing cybersecurity challenges and enhancing cybersecurity resilience in the EU;

Tuesday 12 March 2019

8. Urges those Member States that have not yet fully transposed the NIS Directive to do so without delay, and calls on the Commission to monitor this transposition closely so as to ensure that its provisions are properly applied and enforced and that European citizens are better protected from external and internal security threats;

9. Urges the Commission and Member States to make sure that the reporting mechanisms introduced by the NIS Directive are properly applied; notes that the Commission and the Member States should follow up thoroughly on any security incidents or inappropriate reactions of suppliers, so as to address detected gaps;

10. Calls on the Commission to assess the need to further enlarge the scope of the NIS Directive to other critical sectors and services that are not covered by sector-specific legislation;

11. Welcomes and supports the agreement reached on the Cybersecurity Act and the reinforcement of the mandate of the EU Agency for Network and Information Security (ENISA), in order to better support Member States in tackling cybersecurity threats and attacks;

12. Urges the Commission to mandate ENISA to make it a priority to work on a certification scheme for 5G equipment in order to ensure that the rollout of 5G in the Union meets the highest security standards and is resilient to backdoors or major vulnerabilities that would endanger the security of the Union's telecommunication networks and dependent services; recommends that special attention be given to commonly used processes, products and software that by their sheer scale have a significant impact on the day-to-day life of citizens and the economy;

13. Warmly welcomes the proposals on cybersecurity competence centres and a network of national coordination centres, which are designed to help the EU retain and develop the technological and industrial capacities in cybersecurity that are needed to secure its digital single market; recalls, however, that certification should not exclude competent authorities and operators from scrutinising the supply chain in order to ensure the integrity and security of their equipment that operates in critical environments and telecom networks;

14. Recalls that cybersecurity demands high security standards; calls for a network that is secure by default and by design; urges the Member States, together with the Commission, to explore all available means to ensure a high level of security;

15. Calls on the Commission and the Member States, in cooperation with ENISA, to provide guidance on how to tackle cyber threats and vulnerabilities when procuring 5G equipment, for example by diversifying equipment from different vendors or introducing multi-phase procurement processes;

16. Reaffirms its position on the Digital Europe programme, which imposes security requirements and Commission oversight on entities established in the EU but controlled from third countries, in particular for cybersecurity-related actions;

17. Calls on the Member States to ensure that public institutions and private companies involved in ensuring the proper functioning of critical infrastructure networks such as telecoms, energy, health and social systems, undertake relevant risk assessments that take into account the security threats specifically linked to technical features of the respective system or dependence on external suppliers of hardware and software technologies;

18. Recalls that the current legal framework on telecommunications mandates the Member States to ensure that telecoms operators comply with the integrity and availability of public electronic communication networks, including end-to-end encryption where appropriate; highlights that under the European Electronic Communications Code, Member States have extensive powers to investigate products on the EU market and apply a wide variety of remedies in the event of their non-compliance;

Tuesday 12 March 2019

19. Calls on the Commission and the Member States to make security an obligatory aspect in all public procurement procedures for relevant infrastructure at both EU and national level;
 20. Reminds Member States of their obligation under the EU legal framework, notably Directive 2013/40/EU on attacks against information systems, to impose sanctions on legal persons that have committed criminal offences such as attacks against such systems; emphasises that Member States should also make use of their ability to impose other sanctions on these legal entities, such as temporary or permanent disqualification from practicing commercial activities;
 21. Calls on the Member States, cybersecurity agencies, telecoms operators, manufacturers and providers of critical infrastructure services to report to the Commission and ENISA any evidence of backdoors or other major vulnerabilities that could compromise the integrity and security of telecoms networks or infringe Union law and fundamental rights; expects national data protection authorities as well as the European Data Protection Supervisor to thoroughly investigate indications of data breaches of personal data by external vendors and to impose appropriate penalties and sanctions in line with European data protection law;
 22. Welcomes the upcoming entry into force of a regulation establishing a framework for the screening of foreign direct investments (FDI) for reasons of security and public order, and underlines that this regulation establishes for the first time a list of areas and factors, including communications and cybersecurity, which are relevant for security and public order at EU level;
 23. Calls on the Council to speed up its work on the proposed ePrivacy Regulation;
 24. Reiterates that the EU needs to support cybersecurity across the entire value chain, from research to the deployment and uptake of key technologies, disseminate relevant information, and promote cyber hygiene and educational curricula including cybersecurity, and believes that, among other measures, the Digital Europe programme will be an efficient tool for that;
 25. Urges the Commission and the Member States to take the necessary steps, including robust investment schemes, to create an innovation-friendly environment within the EU, which should be accessible to all businesses in the EU digital economy, including small and medium-sized enterprises (SMEs); urges, furthermore that such an environment should allow European vendors to develop new products, services and technologies which would enable them to be competitive;
 26. Urges the Commission and the Member States to take into account the above requests in the framework of the upcoming discussions on the future EU-China strategy, as preconditions for the EU to remain competitive and for ensuring the security of its digital infrastructure;
 27. Instructs its President to forward this resolution to the Council and the Commission.
-