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) - 12/03/2019 - Text adopted by Parliament, single reading

The European Parliament adopted a resolution on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them.

The resolution was tabled by the EPP, S&D, ALDE, and Greens/EFA groups.

Parliament expressed 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. It was 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. Members noted that 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, and that in January 2019, the Czech tax authorities excluded Huawei from a tender to build a tax portal.

Parliament went on to note that 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 and enterprises to cooperate with the state, in connection with a very broad definition of national security. In particular, the Chinese state security laws have triggered reactions in various countries, ranging from security assessments to outright ban. Stressing that there is no guarantee that these obligations are not applied extraterritorially, Members indicated that the benefits of the single market come with the obligation to comply with EU standards and the Unions legal framework, and consequently, suppliers should not be treated differently on the basis of their country of origin.

Parliament called on the Commission to:

- provide guidance, in cooperation with the EU Agency for Network and Information Security (ENISA), 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;

- 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 Unions telecommunication networks and dependent services. Certification should not, however, 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;

- assess the robustness of the Unions legal framework in order to address concerns about the presence of vulnerable equipment in strategic sectors and backbone infrastructure, and present initiatives, including legislative proposals where appropriate, to address any shortfalls detected, since the Union is in a constant process of identifying cybersecurity challenges.

At the same time, Parliament called on Member States to inform the Commission of any national measure they intend to adopt in order to coordinate the Unions response. It reiterates the importance of refraining from introducing disproportionate unilateral measures that would fragment the single market. It stressed the need to develop a strategy aimed at reducing Europes dependency on foreign technology in the field of cybersecurity.

Parliament urged those Member States that have not yet fully transposed the Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (the NIS Directive) to do so without delay, and to make sure that the reporting mechanisms introduced by the NIS Directive are properly applied. The Commission was asked 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.

Member States were also asked 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;

- make security an obligatory aspect in all public procurement procedures for relevant infrastructure at both EU and national level;

- impose sanctions on legal persons that have committed criminal offences such as attacks against such systems, in accordance with Directive 2013/40/EU on attacks against information systems;

- 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.

Lastly, Parliament welcomed the upcoming entry into force of a regulation establishing a framework for the screening of foreign direct investments (FDI), underlining 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.