**Follow up to the European Parliament non-legislative resolution on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them**

(Security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them)

1. **Resolution tabled pursuant to Rule 123(2) and (4) of the European Parliament’s Rules of Procedure**
2. **Reference numbers**: 2019/2575 (RSP) / B8-0154/2019 / P8\_TA-PROV(2019)0156
3. **Date of adoption of the Resolution:** 12 March 2019
4. **Competent Parliamentary Committee**: N.A.
5. **Brief analysis/assessment of the resolution and requests made in it:**

The resolution expresses deep concerns about the recent allegations of embedded vulnerabilities in 5G equipment provided by Chinese vendors. It also emphasises the need for a common EU approach to cybersecurity threats, in particular with regard to 5G network infrastructures that will constitute the backbone of the digital economy. In particular, the European Parliament calls on Member States to coordinate among each other, with the Commission and European Agency for Cybersecurity (ENISA) to avoid a patchwork of interventions that would be detrimental to the Digital Single Market.

The resolution stresses the need to make the utmost of the existing and forthcoming legal instruments to counter cyber threats, with reference to the NIS Directive, the European Electronic Communication Code, the Cybersecurity Act, and the proposal for the Cybersecurity Competence centre and network (currently under negotiations). In particular, the Member States are invited to finalize without delay the transposition of the NIS Directive, while the Commission is invited to closely supervise the implementation process.

The resolution also calls on the Commission to devise a future course of action that would allow the EU to become a leader in cybersecurity technology and reduce dependencies from foreign solutions. As part of the process, the Commission should consider the revision of the robustness of the current cybersecurity legal framework, including the possible extension of the scope of the NIS Directive to other critical sectors, and the mandate to ENISA to work on a cybersecurity certification scheme on 5G equipment as a priority. Finally, the Commission and the Member States are requested to take into account the resolution in the development of the future EU - China strategy.

1. **Response to requests and overview of action taken, or intended to be taken, by the Commission:**

In relation to the overall request for the Union to take a common approach to and a leading role in cybersecurity (paragraphs 1 to 4), the Commission is pursuing this objective through a set of concrete policies, in particular the 2017 Cybersecurity package and the follow-up actions (such as the recently adopted Cybersecurity Act and the proposal for a European Competence Centre).

As regards the NIS Directive (paragraphs 8 and 9), the Commission notes that most Member States have transposed it into national law. The Commission is monitoring thoroughly, through in-depth checks, the implementation of the NIS Directive and it stands ready to support the Member States in this process. The deadline for the review of the NIS Directive is in 2021; the Commission, based on a thorough evaluation, will consider, among the possible areas for improvement, whether to extend the scope of the directive to other critical sectors (paragraph 10).

In relation to the cybersecurity of 5G networks (paragraphs 5, 7, 12, 15 and 19), the Commission has taken due account of the resolution of the European Parliament and, with the support of the European Council, has issued on 26 March a Recommendation to the Member States. The Recommendation, which was announced in the joint Communication on EU-China relations (paragraph 26), sets out a series of operational measures:

* at national level, each Member State should complete a national risk assessment of 5G network infrastructures by 30 June 2019 (and transmit it to the Commission and ENISA by 15 July) and, on that basis, should update existing security requirements for network providers and include conditions for ensuring the security of public networks, especially when granting rights of use for radio frequencies in 5G bands;
* at EU level, a coordination process under NIS Cooperation was launched on 30 April 2019. Member States, with the support of the Commission and ENISA, should complete a coordinated European risk assessment by 1 October 2019. On that basis, by 31 December 2019, Member States should agree on a set of mitigating measures (toolbox) that can be used at national level and by the Commission for the development of common requirements.

In addition, Member States, together with the Commission, should identify the conditions concerning the security of networks to be attached to the general authorisation for the provision of electronic communications networks. They should also actively engage in the development of relevant EU-wide certification schemes for 5G equipment, including by supporting the definition of specific protection profiles, and, once it is in place, Member States should make certification of 5G mandatory. Finally, Member States should develop specific security requirements that could apply in the context of public procurement related to 5G networks, including mandatory requirements as regards cybersecurity certification.

The Recommendation provides that the coordination work should take place in the Cooperation Group of competent authorities, as set out under the NIS Directive, with the help of the Commission and ENISA.