HEAD OFFICE
10 Rue du Commerce
1000 Brussels, Belgium
+32 2 285 41 63
yepp@epp.eu

RESOLUTION

Coordinated EU Strategy to 5G Security

Adopted at the YEPP Council Meeting via Zoom, 24.04.2021

Recognizing that:

- The fifth generation of mobile and wireless telecommunication systems (5G), by allowing ultra-high-speed connection between a wide range of devices, is a crucial building block of our digitalized economies and societies. This technology is used in critical sectors such as energy, transport, agriculture, banking, and health, as well as industrial control systems carrying sensitive information. Among these benefits, it has to be noted that a delocalized network architecture based on multiple entry points, a larger number of antennas and software dependency may facilitate hacker attacks[1].

- The Commission introduced the 5G Action Plan in September 2016 and adopted the Recommendation on cyber security of 5G networks in March 2019[2].

- The EU 5G toolbox launched by the European Commission in January 2020 summarizes the measures agreed by the Member States to cope with the security risks related to the development of the 5G. The toolbox aims at mitigating risks by strengthening the security requirements and adopting a multi-vendor strategy to limit dependencies.

- The European Union Agency for Cybersecurity (ENISA) published in December 2020 a set of new guidelines for European actors in the telecommunication sector[3] with the goal of assisting the implementation of the European Electronic Communications Code (EECC) and the EU 5G toolbox. Previously the agency published in November 2019 the *Threat Landscape for 5G Networks* that maps the key assets exposed to security risks[4].

- The EU Directive 2016/1148 on security of network and information systems (NIS Directive) established a cooperation network in order to facilitate the collaboration across

[1] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-initiatives
[2] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123
[3] https://www.enisa.europa.eu/news/enisa-news/new-guidelines-for-telecom-and-5g-security
[4] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

HEAD OFFICE
10 Rue du Commerce
1000 Brussels, Belgium
+32 2 285 41 63
yepp@epp.eu

the Union in the field of cyber security. The NIS Cooperation Group is composed of representatives of the EU Member States, the European Commission and the ENISA[5]. The Group presented the Coordinated EU report in October 2019 on 5G networks security[6].

- The European Court of Auditors presented the ECA Review No 3/2020 on the EU's response to China's state-driven investment strategy, which showed the risks related to the usage of Chinese 5G equipment in key EU infrastructure in the absence of a clear strategy at Union level for 5G security[7].

Acknowledging that:

- In the UK the purchase of Huawei 5G equipment was banned and the company will be removed from UK's 5G networks by the end of 2027. These rules were adopted with the goal of increasing the security and resilience of the British telecommunication infrastructure[8].

- In Sweden Huawei was banned from taking part in the procurement of 5G technologies, as the company was defined as a national security threat due to the risk of Chinese cyber espionage[9].

- In France telecoms operators were prohibited from using Huawei equipment for the development of 5G technologies, so as to safeguard the interests of the defence and of the national security from the risks of espionage[10].

- Mobile video traffic is forecast to grow by around 50 percent annually through 2023, accounting for 75 percent of all mobile data traffic.[11]

YEPP calls for:

- The Member States to apply coordinated and harmonized security requirements together with a clear multi-vendor strategy in order to guarantee a diversified and safe supply chain of this technology based on risk assessments of high-risk suppliers for key assets in

[5] https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive
[6] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group
[7] https://www.eca.europa.eu/Lists/ECADocuments/AP20_14/AP_5G_Security_EN.pdf
[8] https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027
[9] https://sverigesradio.se/artikel/7596262
[10] https://www.bfmtv.com/economie/5g-le-conseil-constitutionnel-valide-la-loi-anti-huawei_AD-202102050146.html
[11] https://www.ericsson.com/en/mobility-report
https://www.bfmtv.com/economie/5g-le-conseil-constitutionnel-valide-la-loi-anti-huawei_AD-202102050146.html

HEAD OFFICE
10 Rue du Commerce
1000 Brussels, Belgium
+32 2 285 41 63
yepp@epp.eu

telecommunication systems. However, our major goals are data security as well as data protection, any sign of espionage and/or security breach will be consequential and not tolerated.

- The European Commission to foster synergies between 5G (ecosystem) research carried out through Horizon, the ENISA and the European Cybercrime Centre EC3 in order to adopt a preventive approach in the management of technologies that will have a serious impact on our society and industries. The goal is to facilitate a smooth technological transition while safeguarding the security of the Union.

- The European Commission to set a normative framework for the Member States to stimulate Communication Service Providers (CSPs) to expand the bandwidth through the use of Network Function Virtualization (NFV) -namely the replacement of physical network appliances into virtualized network functions through cloudification or virtual machines, to achieve a critically important higher degree of flexibility and scalability needed to ensure integrity[12].

- The ENISA to share guidelines for the constant update of protocols on data transmission in the field of telecommunications and of the Internet of things to preserve the integrity of the data, the security and to prevent data tampering.

- The European Commission to work on the development of communication strategies in parallel with the development of a security framework for 5G technology that would address citizens' distrust of 5G technology due to exposure to numerous disinformation as well as educate citizens about the benefits of 5G technology in everyday life.

[12] https://www.ibm.com/thought-leadership/institute-business-value/report/cspnetwork#