European Parliament

5G in the EU and Chinese telecoms suppliers

The spectrum auctions of fifth-generation (5G) mobile telecoms networks planned in 17 EU Member States for 2019 or 2020 have sparked a highly politicised debate in the EU about whether the use of Chinese 5G equipment in critical EU infrastructure poses a threat to security. While Australia, Japan, and New Zealand have followed the United States (US) in imposing a (partial) ban on Chinese telecom vendors, EU Member States appear to privilege EU-coordinated national risk-mitigating measures over a ban.

Global footprint of Chinese 5G vendors and security risks associated with them

With a global market share of 29 %, in 2018 nominally private Huawei Technologies ranked first among the top seven global telecoms equipment vendors, ahead of American Cisco and Ciena, Swedish Ericsson, Finnish Nokia, South Korean Samsung and Chinese state-owned ZTE Corporation. Huawei and ZTE are national champions that have benefited both from being shielded from foreign competition by means of domestic market access barriers and from indigenous innovation policies rolled out since 2006. The latter have boosted the companies' competitive edge at home and growing global footprint. Both now shape global tech standards, but have not made big inroads into the US market, as US Congress investigations conducted in 2012 into the risk they posed to US national security, owing to their ties to the Chinese government, created a hostile climate for them. Major US telecoms companies rely on Ericsson, Nokia, and Samsung. By contrast, Huawei enjoys significant market penetration in the EU on account of its competitive prices and supposedly better quality. Until recently there has been little public awareness in the EU of how the close ties Chinese public **and** private firms have with the Chinese Communist Party, in order to thrive in the Chinese eco-system, may expose liberal democracies to cyber-attacks, cyber-espionage, digital authoritarianism, and information warfare in the context of 5G. A 2018 US consultancy report points to a range of risk factors associated with Huawei, the most serious concerns being those related to cybersecurity, state-sponsored espionage, military influence and foreign political interference.

Positioning of the US and US allies towards Chinese 5G vendors

In the **US**, the related debate is driven by US-China strategic rivalry in the technology realm. This, in turn, is at the heart of the ongoing Sino-US trade war triggered by US claims that China is pursuing unfair trading practices, relating to forced technology transfer, cyber-theft, and intellectual property rights issues, under Section 301 of the 1974 Trade Act. The US recently adopted legislation that prohibits executive agencies from using Huawei or ZTE products and from contracting with entities using such products on national security grounds. Moreover, the US has put pressure on allies to follow suit, and threatened that using Chinese equipment could lead to reduced US intelligence-sharing, and affect cooperation within NATO. **Australia**, a member of the 'Five Eyes' intelligence alliance that includes Canada, New Zealand, the United Kingdom (UK) and the US, banned foreign vendors from taking part in the rollout of 5G mobile networks across the nation on security grounds. The government argued that 'the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference'. **New Zealand** has banned Huawei from providing 5G network equipment, referring to a 'significant network security risk'. **Canada** also is still considering a ban, against the backdrop of tense diplomatic relations with China. **Japan**'s government has meanwhile banned government purchases of Huawei and ZTE equipment.

Other factors weighing into the debate alongside security concerns

While taking security-related technical, legal and political considerations into account, it is vital for the EU to preserve its strategic autonomy against the backdrop of **geopolitical pressure** from the US and China and hard **economic realities**, i.e. EU telecoms operators' current high level of dependence on Chinese equipment (for instance in Germany and France). This makes its complete replacement with equipment

Author: Gisela Grieger, Members' Research Service
PE 637.912 – April 2019

from competitors fairly elusive in terms of capacities, and of the cost (UK) and potential delays this would entail for the rollout of 5G networks and the future of the EU's digital single market – although these concerns are dismissed by some telecoms vendors. Neither would it be desirable from the point of view of the EU's commitment to maintaining an open and competitive business environment with diversity of supply.

Security risks arise from a combination of **technical**, **political** and **legal concerns**. As regards technical concerns, two opposing views are prevalent: one is that risk-mitigating solutions for potential backdoors for the Chinese government to conduct cyber-espionage and cyber-attacks are adequate remedies; the other is to dismiss these kinds of remedy on basis of the argument that 5G networks operate in a very different way to 4G networks and create vulnerabilities of a different nature, blurring the lines between edge and core networks. High-risk vendors can no longer be confined to the edge, but can have an impact on the core network. Moreover, since **trust** in equipment vendors depends heavily on the **legal and regulatory system** of the jurisdiction in which they operate and its extraterritorial application to them, it is not just about trusting Huawei or ZTE but about trusting China's one-party regime. In this regard the unique nature of the Chinese authoritarian political system, which lacks the rule of law and democratic oversight, is of considerable importance. China uses advanced technologies for the systematic digital surveillance of its population, notably in its restive Xinjiang province, while the EU pursues a human-centric approach to advanced technologies, with the protection of the digital rights of the individual being key. From a legal perspective, Chinese companies and individuals are obliged under penal sanctions to cooperate in intelligence gathering under the Chinese National Intelligence Law as well as under other related Chinese laws. Hence, the US has claimed that China could use Huawei's 5G network gear as a Trojan horse, by compelling operators to spy, steal corporate, government or military secrets and transmit data to the Chinese authorities. However, the US has provided no evidence to substantiate this claim. The **Czech** national cyber- and information security agency meanwhile issued a security warning that met with a tough Chinese rebuke. A 2018 security review by the **UK**'s Huawei Cyber Security Evaluation Centre Oversight Board detected underlying defects in Huawei's software engineering and security processes, but did not call for a ban. The UK's National Cyber Security Centre had previously found that the national security risks arising from the use of ZTE could not be mitigated. **Dutch** and **Norwegian** security services have also issued related warnings. The arrest in Poland of a Huawei employee on spying charges in January 2019 has strongly undermined Huawei's **trustworthiness** and acted as a wake-up call for the EU.

Moves towards a unified and coordinated EU approach to 5G network security

EU Member States appear to be seeking to avoid (partial) bans of telecoms vendors from specific countries on national security grounds, and believe that the security risks are manageable. For **Germany**, where Huawei is a provider of core parts to telecoms operators, a ban is not an option. The favoured approach consists of mitigating security risks by setting additional security requirements, e.g. the use of critical key components being made subject to certification. Proposals for new legal provisions in **France** that would require full government access to suppliers' technology, such as encryption keys and code, are currently under discussion in the French Parliament. **Italy** recently amended its legislation to allow the government to block contracts with non-EU telecoms providers. Since EU Member States retain sole competence for matters of national security and the EU's role is merely complementary, on 26 March 2019 the European Commission issued a non-binding recommendation on the cybersecurity of 5G networks. This followed calls by the European Parliament for a common approach to cybersecurity, in its resolution of 12 March 2019, and a similar call made in Action 9 of the EU-China strategic outlook paper of 12 March 2019. The Commission recommendation sets out a roadmap until the end of 2019 for a coordinated Union risk assessment, based on Member States' risk assessments using technical and 'other' factors, and for a common set of **risk-mitigating measures**. In the absence of harmonised Union law, Member States may opt to declare the European cybersecurity **certification** scheme, due to be developed under the EU Cybersecurity Act, mandatory. This has yet to be formally endorsed by the Council. Similar schemes are available in the context of Directive 2014/24/EU on public procurement. The response from EU telecoms vendors and various telecoms lobby groups to a harmonised approach has been cautiously positive.