Securing Future 5G-Networks

Categorized as a systemically relevant infrastructure, 5G plays a crucial role for a wide range of technological innovations. The technological and geopolitical challenges that converge in this context require comprehensive solutions.

By Julian Kamasa

5G, the fifth-generation mobile telecom standard, has polarized opinions across the globe. The debate surrounding the role of Chinese provider Huawei, which is often dominated by national considerations and has largely been confined to the US and the UK, has now also reached the shores of continental Europe. The politicization of the debate alongside exaggerated rhetoric on all sides has made it well-nigh impossible to discuss the real underlying issue, namely the organization of secure, resilient, reliable and future-oriented telecommunications networks by liberal democratic European states. This issue raises a number of further questions: What degree of market dominance is permissible in liberal democracies for technology companies that are unable to actively distance themselves from authoritarian states not governed by the rule of law? How can an increased susceptibility for political blackmail be avoided and, ideally, be reduced instead?

5G: More than a faster version of 4G

Between 2015 and 2020, the number of interactive terminal devices doubled to reach 30 billion. Growing data volumes are challenging the limits of our telecom network capacities. The wireless communications standard 5G is designed to counter this overload with higher transmission rates at lower latencies. Yet in many respects, 5G is much more than just a faster version of 4G.

Firstly: 5G is a systemically relevant basic infrastructure that, due to its significance, is therefore considered to constitute part of a nation's most critical infrastructures. Within the coming five to fifteen years, this infrastructure is to facilitate technological innovations and new network capabilities in sectors such as mobility (autonomous driving), energy supply (smart energy grids), industry (remote production processes), and healthcare (remote health monitoring). However, it should be noted that – similar to other technologies – 5G is subject to numerous

Key Points

- New technologies must be analyzed comprehensively. While no 5G vendors are entirely risk-free, their provenance does play a role if the rule of law is not guaranteed in the vendor's domicile country. Risks can be minimized via a reduction of potential vulnerabilities.
- The security debate surrounding 5G should be taken as an incentive to closely analyze high-tech supply chains. The EU should adopt its own approach to becoming an actor at the nexus of technology and geopolitics. Europe should share experiences with like-minded states and step-up its multilateral cooperation.

uncertainties with regard to the respective innovation dynamics. For instance, autonomous driving might be approved after years of legislative adjustments, but at a time when 5G has already been replaced by notional 6G networks. Or it may turn out that the capabilities associated with 5G have been overestimated and that the real breakthrough will only occur with the advent of such 6G infrastructures.

Secondly: Against this backdrop, rapid action is not necessarily an advantage where 5G is concerned – 'first movers' often pay a rather formidable price that may not be fully justified by later benefits. Due to the technical complexity and social importance of 5G, reliability and security are likely to be much more significant factors in determining a location's economic attractiveness than was the case with 4G. The full rollout and operationalization of 5G is a highly complex matter, since it is essentially oriented towards the virtualization of networks. Hence, the transition from 4G to 5G is often based on existing 4G hardware *(non-standalone 5G)* in order to decouple the software from the hardware component and finally arrive at a virtual cloud-based network *(standalone 5G)*. Buzzwords such as "race to 5G" therefore lead to flawed and misguided debates.

The issues raised by 5G also apply to ensuring secure high-tech supply chains.
Dado Ruvic / Reuters

Thirdly: The virtualization of networks creates a new relationship between the sensitive core and the *radio access network* (RAN), the so-called antennas on the one hand and the software and hardware on the other. In both the core and the RAN, the focus shifts from hardware to software, that is towards a *cloud-native core* and a virtualized RAN (vRAN). Software updates in these networks are carried out by the 5G vendors instead of the telecom operators. The complexity of 5G antennas makes it exceedingly difficult to clearly separate the core and radio network, and creates a new relationship between the state, the operators and the vendors.

Fourthly: Progressive consolidation among vendors has resulted in oligopolistic market structures, while global market power has shifted from the US to China. In contrast to the 4G launch, there is no globally competitive US vendor in the 5G rollout, while the Chinese vendor Huawei holds a dominating market position along with Ericsson and Nokia, and can thus play a decisive role in shaping standardization processes.

Minimizing the IT security risks associated with 5G

Just like any other emerging technology that is designed to create new network capabilities, 5G is associated with a number of risks. However, the debate about embedded backdoors implemented by the Chinese government misses the point. Excluding Huawei would not necessarily raise IT security, since cyber attacks, acts of sabotage, and espionage can be carried out against all vendors, irrespective of their national affiliation. What, then, can European states do to minimize the IT risks associated with 5G?

Firstly, new technologies must be comprehensively analyzed. The key point is that critical infrastructure such as 5G must offer above-average security, stability, resilience and reliability. This is where the quality of the vendors' products comes into play, which should primarily impress on the basis of excellence rather than low prices and speedy rollout. In the UK, for instance, so-called 'high-risk vendors' of fiber optic networks, 4G, and 5G have been analyzed from a multitude of angles since 2010 in order to generate a more nuanced picture. With respect to 5G, the UK National Cyber Security Centre (NCSC) states that Huawei stands out negatively due to very low-quality software source codes as well as numerous software bugs. Having perhaps the best global insight into the activities of the Chinese company since 2010, the NCSC has not seen any substantial improvements in these areas. Hence, the development of interdisciplinary skills for new technologies like 5G should be expedited both at the national and the supranational level to allow for the comprehensive evaluation of high-risk vendors.

Secondly, there are no 5G vendors that are entirely risk-free. Nonetheless, their provenance does play a role if the rule of law is not guaranteed in the technology vendor's domicile country. Huawei's competitors in Sweden (Ericsson) and Finland (Nokia) also have software errors that can be exploited by malicious actors. At the same time, they are private companies that due to their listing on the stock exchange, are also subject to extensive transparency requirements. Furthermore, both are registered in countries that promote and guarantee the rule of law. This is import-

ant, as it prevents any arbitrary use of these companies for political purposes. The same cannot be said for Huawei. For one, the company's stocks cannot be purchased on the free market. Even more importantly, however, China, which serves as Huawei's base, is not governed by the rule of law. Matters are further complicated if one considers the fact that Huawei provides data collection services for China's social credit system. In sum, the main problems associated with the telecom giant are the legal system in place in its domicile country, as well as its intransparent corporate structure. The extent to which the 5G vendor should be trusted is therefore essentially a question of trust in the Chinese government. Since all 5G infrastructures are associated with risks irrespective of the specific vendor, a country's trust in its own cyber defense capabilities and the entire internet architecture also plays a central role.

Thirdly, risks can be minimized by reducing potential vulnerabilities. Due to the limited choice of 5G vendors, it is difficult to achieve resilience through vendor diversification. The US, Japan, and South Korea are consequently keen to integrate software companies as additional vendors into the virtualization of the 5G radio networks. In the US, cross-party support for the funding of open radio access networks (O-RAN) has resulted in the "Utilizing Strategic Allied (USA) Telecommunications Act" which provides one billion dollars in targeted funding. By contrast, the EU has adopted a 'multi-vendor' strategy which encourages telecom providers to focus on several vendors. Hence, the EU, the US, Japan, and South Korea are all pursuing the overriding goal of preventing path dependencies leading to overreliance on individual technology vendors. In the context of our current information and communications technology (ICT), these individual measures would fail to achieve the desired effect, since millions of lines of source code make the identification of randomly or intentionally integrated errors virtually impossible. In the field of IT security, the European research landscape, including cutting-edge research in Switzerland, could play an important role (see box on page 4). Secure network architecture is likely to put both the aforementioned 'backdoor-problem' and the debate about Huawei's role into perspective, and minimize the vulnerabilities that can be exploited through acts of sabotage, cyber attacks or espionage.

Europe: Caught between the US and China

The 5G challenge illustrates the question of Europe's position in the ongoing strategic competition between the US and China. Both powers are aiming to gain leverage by exerting pressure in specific areas; the US has linked 5G with partly extraneous issues, such as intelligence cooperation, while China has intertwined 5G and trade policy. How can Europe avoid becoming, and being used as a playing field by the two superpowers?

Firstly, the security debate surrounding 5G should be taken as an incentive to closely analyze supply chains in the high-tech sector. Considering all supply chains in their entirety, the frequently cited concept of European technology sovereignty is currently neither realistic nor desirable despite the existence of two competitive European 5G-vendors. Any decoupling from non-European vendors would be associated with enormous costs, substantial geopolitical upheavals, and ultimately marginal security gains. Nevertheless, the idea of secure supply chains has gained political legitimacy in the context of the coronavirus pandemic. Particularly sensitive areas could be localized via careful evaluation of supply chains. If necessary, and possible, path dependencies, and hence susceptibility to political blackmail, could be systematically reduced by focusing on trusted vendors. In the context of the 5G rollout, the telecom operator Telenor in Norway has shown that this can be achieved through the gradual phasing out of vendors. Telenor is allowing the existing contract with Huawei for the operation of the 4G network to expire as scheduled in five years' time; working with Nokia and Ericsson to build its 5G core network; and planning to grant Huawei a future role that is yet to be defined. In this case, path dependency was reduced without any geopolitical upheaval.

Secondly, the EU must find its own approach to becoming an actor at the nexus of technology and geopolitics. Even if dependencies can be reduced in the 5G rollout, the overarching problem of dependency on Chinese technology components that are crucial for the prosperity of the continent will by no means be solved. Hence, the 5G issue should be taken as an incentive to adopt a European 'geo-tech' approach supplemented

Further Reading

Cybersecurity of 5G networks: EU Toolbox of risk mitigating measures. *EU Commission, January 2020.*
The EU Commission's 5G security 'tool box' submitted to the EU member states.

Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board – Annual Report 2019. *HCSEC, Banbury, Oxfordshire (UK), March 28, 2018.*
Annual Huawei evaluation report by the UK National Cyber Security Centre.

The Prague Proposals: The Chairman Statement on cyber security of communication networks in a globally digitalized world.
Prague 5G Security Conference, Prague, May 3, 2019.
Prague declaration on cyber security in 5G networks.

A Swiss approach to greater IT security

ETH Zurich's "Scion" internet protocol has been developed to close the existing internet software gaps in the vulnerable and obsolete Border Gateway Control (BGP) system by means of a new, decentralized protocol, and to achieve a significant increase in IT security. Contrary to the current BGP system, in which the internet servers determine the data path, the control of the Scion data flow lies with the terminal device. The aim is to instantly flag any manipulation attempts or security gaps. Scion also aims to simplify complex and sometimes incomprehensible source codes.

with a coherent China policy. Developing such an approach at the EU-level would seem even more advisable if one considers that, contrary to the EU, individual states have insufficient political clout and are thus susceptible to political blackmail. Aside from the areas already addressed, such as investment controls relating to 5G, other possibilities should also be explored, such as US export controls on high-tech, quantum computing, and the Internet of Things (IoT). Effective industrial policy incentives should be offered to enhance European expertise based on specific research and development in these areas. In addition, Europe should develop a clear position towards the two superpowers, especially China. In this context, China's significant global role should be recognized without falling prey to preemptive obedience. However, more power also means more responsibility. The EU should be more effective in communicating its position to Beijing, namely the application of the principles underpinning the rule-based world order.

Thirdly, Europe should share its experience with like-minded states and step-up multilateral cooperations. Even if European member states reap power benefits resulting from the EU's rise as a 'geo-tech' actor, any European foreign and security policy in the realm of technology should not be defined by the EU alone. Departing member states, namely the UK, as well as non-member states (Switzerland, Norway, and Iceland) share the same values relating to democracy, the rule of law, and respect for human rights. The Prague 5G Security Conference held in May 2019 showed that there is also a convergence of interests with non-European states, including the US, Canada, Israel, Japan, South Korea, Australia and New Zealand. In terms of content, the "Prague Proposals" worked out by 32 countries is very similar to the "EU Toolbox on 5G Cybersecurity". This form of multilateral ad-hoc cooperation among like-minded states aiming to design open, free, rule-based and secure communication networks is crucial for knowledge sharing and should not be restricted to 5G.

The issues raised by 5G are not limited to this domain, but apply to any future technology. High levels of complexity lead to a convergence of technological, security, foreign policy, and economic challenges that require comprehensive solutions. Although overlaps cannot be categorically ruled out, different measures will be needed to tackle IT security risks from those located at the geopolitical level and intended to address Europe's role in the US-China superpower competition. What is clear, however, is that it is only through an interplay and interaction between a wide range of tools that secure networks for the future can be guaranteed.

Julian Kamasa is a Researcher in the Swiss and Euro-Atlantic Security Team at the Center for Security Studies (CSS), focusing on Swiss and European foreign and security policy, as well as emerging technologies.

Policy Perspectives is published by the Center for Security Studies (CSS) at ETH Zurich. The CSS is a center of competence for Swiss and international security policy.

Editors: Annabelle Vuille and Oliver Thränert
Additional language editing: Michael Haas
Layout: Rosa Guggenheim

Feedback welcome: PolicyPerspectives@sipo.gess.ethz.ch
More issues and online subscription:
css.ethz.ch/en/publications/css-policy-perspectives

Most recent editions:
Obstacles Ahead: Preserving the JCPOA (8/3)
Policy Consulting in the Age of Corona (8/2)
Neo-Containment: a Strategy toward Russia (8/1)
Educating Engineers for Resilience (7/3)
A Politically Neutral Hub for Basic AI Research (7/2)

ISSN: 2296-0244; DOI: 10.3929/ethz-b-000416792