December 2019 · Jan-Peter Kleinhans

Whom to trust in a 5G world?

Policy recommendations for Europe's 5G challenge

Stiftung Neue Verantwortung

Think Tank at the Intersection of Technology and Society

Executive Summary

The fifth generation of mobile networks is already changing the telecoms market and in the near future every industry will rely, at least to some extent, on mobile networks – not just for communication but first and foremost value creation: even though telecommunication networks have been built to enable human-to-human communication, they increasingly transport machine-to-machine communication, such as in smart factories or autonomous vehicles. Being connected to the mobile network will be almost as critical as being connected to electricity: disrupting mobile networks has thus severe impacts on ever more industries. This is why the security and resilience of those future networks is of utmost importance. Recent debates around 5G have almost exclusively focused on the question of whether or not it is safe for European countries to include Chinese vendors in the 5G rollout. A strong focus was on Huawei and the search for the "smoking gun" – a "kill switch" or "backdoor" in the source code of Huawei's products on behalf of the Chinese Communist Party (CCP) to compromise foreign networks. This debate stole attention away from more systemic challenges: Securing our mobile networks is a much bigger task than deciding about the trustworthiness of a particular company.

The European Commission's (EC) consolidated 5G risk assessment is the right step to identify those systemic challenges. The task ahead is now to identify policy initiatives to address those challenges. This paper argues that the EC's upcoming "5G toolbox" will have to utilize different policy domains to properly address the three dimensions – IT security of mobile networks, trustworthiness of foreign suppliers and industrial policy for Europe. It provides an analysis of each of these dimensions and provides policy recommendations:

1. The **IT security of mobile networks** has to be addressed on four different levels – standards, implementation, configuration, operations. Certifying network equipment or source code analysis, two heavily discussed strategies, should only be small pieces of a broader strategy: 5G is first and foremost about software-defined, highly modular and complex networks that blur the line between vendor and operator. This in itself creates severe challenges for policy makers to define requirements and responsibilities.
2. The origin of technology matters – especially with software-defined products. Policy makers will have to define criteria to reliably assess the **trustworthiness of suppliers**, not just for 5G. The EC has the chance to

inform future debates of national security threats emerging from certain technology suppliers by establishing a framework that considers technical and non-technical criteria that impact the trustworthiness of a supplier.

3. Lastly, Europe has to be pragmatic about a **necessary industrial policy**: Supplier diversity is a precondition for resilient networks and there are strong indicators that Chinese suppliers have systemic competitive advantages, not just through state subsidies. The EC will need to utilize industrial policy to strengthen a diverse supplier market and avoid vendor-lock-ins.

Introduction

Should Europe continue to rely on Chinese mobile network equipment vendors, namely Huawei and ZTE, to supply European mobile network operators with equipment and services? This question has been debated in Europe for more than a year. During that time, one thing became apparent – answering this question is a multi-dimensional challenge that forces policy makers to escape their silos to identify interdependencies and define integrated policy solutions.

The first dimension to the question is that of **IT security**: How to build and maintain secure and resilient mobile networks? From the start, policy makers in Europe focused almost exclusively on that dimension. Member states and the European Commission conducted risk assessments[1] to have a better understanding in how many different ways today's mobile networks can be exploited and compromised. Ideally, the result will be common requirements for operators and vendors to strengthen the security and resilience of mobile networks in Europe.

By assessing the threat landscape of mobile networks, it becomes clear that vendors, hypothetically, are in the perfect position to exploit and compromise their operators' networks: because of increasingly complex networks, it is impossible to build trustworthy systems without trusting the developer of those systems. The **trustworthiness of a vendor** is furthermore affected by its country of origin. The origin of technology matters – this is nothing new but opens the door for geopolitics and protectionism all in the name of national security (see chapter II of this paper).

IT security and trustworthiness are interlinked to some extent but have to be addressed by different policies. Conflating those dimensions poses the danger of ineffective and inefficient regulation. Additionally, only through a clear distinction can conflicting goals be addressed and weighed against each other. This paper identifies key questions and policy recommendations for each dimension to help European policy makers to properly address each of them. To this end the first section of the paper focuses on IT security and recommends certain policy measures that have to be considered as part of the upcoming 5G toolbox from the European Commission. The second section of the paper deals with the trustworthiness of vendors, why it is relevant but distinct from the technical dimension of IT security. Lastly, the paper ar-

1 European Commission. 2019. „Security of 5G networks: EU Member States complete national risk assessments". https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_4266.

gues that Europe has now a window of opportunity to identify non-technical criteria to assess the trustworthiness of vendors since there will be similar debates about national security and trustworthiness in other emerging technologies, such as AI or Internet of Things.

I. IT security – How to strengthen the IT security of mobile networks

"The telecoms market is not working in a way that incentivises good cyber security"
UK Telecoms Supply Chain Review Report, Department for Digital, Culture, Media and Sport

The security of mobile networks is a shared responsibility between operators, vendors and governments. With UK's Telecoms Supply Chain Review[2], EU's Consolidated 5G Risk Assessment[3] (based on national risk assessments from member states) and ENISA's Threat Assessment for 5G Networks[4] there is now a much better understanding among policy makers of the myriad challenges of securing current and future mobile networks. These shortcomings regarding IT security have to be addressed independent of other measures in the national security domain. The overall IT security posture of mobile networks depends on four different factors – standards, implementation, configuration and operations:

1. **Standards**
   Technical standards, just like software, can have security vulnerabilities. Since mobile networks have to comply to certain standards, vulnerabilities in technical standards are especially severe since they can potentially be exploited in any equipment that implements a particular standard. Research has shown that there are several exploitable vulnerabilities in

2 UK DCMS. 2019. UK Telecoms Supply Chain Review Report. https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference.

3 NIS Cooperaton Group. 2019. "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks." https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

4 ENISA. 2019. "ENISA Threat Landscape for 5G Networks." https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

current[5] and future[6] standards. Developing secure and trustworthy technical standards is the responsibility of operators, vendors and governments as part of their work in 3GPP, the global standardization body for mobile equipment.

2. **Implementation**
   Vendors then implement those technical standards when developing mobile network equipment. While technical standards simply define *what* has to be done, it is up to the vendor *how* to achieve that. This is obviously another source for security vulnerabilities due to poorly written software.[7] Policy ideas such as device certification or source code review all try to assess and improve the software quality of deployed mobile network equipment. The secure implementation is the vendor's responsibility.

3. **Configuration**
   During deployment, operators then configure network equipment to properly work in a particular network architecture. Since mobile networks become increasingly complex and operators have to also support older protocols (2G, 3G)[8], secure network configuration is a significant challenge for operators.[9] At the same time, attacks against mobile networks also become easier: With 4G, mobile networks started to utilize the Internet Protocol (IP) and can thus be attacked very similarly to common Internet infrastructure.[10] Even though 5G entails many IT security improvements,

5 Jøsang, A, L Miralabé, and L Dallot. 2015. "Vulnerability by Design in Mobile Network Security." The Journal of Information Warfare 14 (4). http://folk.uio.no/josang/papers/JMD2015-JIW.htm.

6 Rupprecht, David, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, and Christina Popper. 2018. "On Security Research Towards Future Mobile Network Generations." IEEE Communications Surveys and Tutorials 20 (3): 2518–42. https://doi.org/10.1109/COMST.2018.2820728.

7 HCSEC. 2019. "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board – Annual Report 2019." https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019.

8 Jover, Roger Piqueras. 2019. "The Current State of Affairs in 5G Security and the Main Remaining Security Challenges" 1282: 1–8. http://arxiv.org/abs/1904.08394.

9 Shaik, Altaf, Ravishankar Borgaonkar, Shinjo Park, and Jean Pierre Seifert. 2019. "New Vulnerabilities in 4G and 5G Cellular Access Network Protocols : Exposing Device Capabilities." In WiSec 2019 - Proceedings of the 2019 Conference on Security and Privacy in Wireless and Mobile Networks, 221–32. Association for Computing Machinery, Inc. https://doi.org/10.1145/3317549.3319728.

10 Positive Technologies. 2017. "Threats To Packet Core Security of 4G Network." https://positive-tech.com/articles/epc-research/.

it also makes the network much more complex and modular.[11] The secure configuration of mobile networks is the operator's responsibility.

4. **Operations**
   Even with well-defined standards, securely developed network equipment and robust network configurations in place, the operator's processes and operations can have a significant impact on a mobile network's overall security posture. From continuous risk assessment and mitigation, to experienced IT security personnel and routines for network maintenance and disaster recovery – all these have an impact on the "real-world" security of mobile networks.[12] At the same time, many cost-driven, commercial operators do not necessarily prioritize those.

The European Commission's forthcoming "5G toolbox" needs to address those different levels to meaningfully improve the security and resilience of mobile networks. This means creating incentives for operators to build and maintain secure and resilient mobile networks, as well as ensuring that vendors design reasonably trustworthy equipment. Following are **key recommendations for the future 5G toolbox**:

A Distinction between radio access network and core network is not sustainable

At its heart, 5G is about virtualization – decoupling software from hardware. In the past, operators would buy network equipment in which proprietary hardware is coupled with proprietary software. This will change significantly with 5G. By decoupling software from hardware, network deployment is much more agile, modular and scalable – but also increasingly complex. This is true not just for the core network, but also for the Radio Access Network (RAN). Operators in Europe are already moving their core networks to cloud environments[13] and there are multiple industry initiatives for virtualized RAN.[14] Network functions are not tied to network equipment but mere

11 NIS Cooperaton Group. 2019. "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks." https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132.

12 Bundesnetzagentur. 2019. "Katalog von Sicherheitsanforderungen Version 2.0." https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=2.

13 Light Reading. 2019. "Three UK Builds 5G-Ready Cloud Core Network with Nokia". https://www.lightreading.com/mobile/5g/three-uk-builds-5g-ready-cloud-core-network-with-nokia/d/d-id/752815

14 Kapko, Matt. 2019. „Ericsson, Nokia, Samsung Hype Open Virtualization". https://www.sdxcentral.com/articles/news/ericsson-nokia-samsung-hype-open-virtualization/2019/11/

pieces of software that are quickly deployed in cloud environments, running on general purpose hardware.[15] This flexibility and modularity blurs the line between core and RAN, making it very difficult for governments to define "sensitive" network functionalities that should not be built by "high-risk" vendors. It is thus at least questionable how effective a continued distinction between core network and RAN on the policy level would be for IT security.

IT security certification is of limited use

Both the European Commission[16] and the German government[17] emphasize the importance of IT security certification for (sensitive) mobile network equipment to increase the trustworthiness and resilience of mobile networks. But certification can only be one piece of a broader strategy since it merely evaluates a vendor's software quality – aforementioned shortcomings on the level of the operator (network configuration, operations) are not addressed. Following are key arguments against a strong focus on Common Criteria-based[18] (CC) certification:

- Certification is a one-time assessment that quickly loses validity with every successive software update.[19]
- Certification is neither efficient nor effective to identify malicious code or "backdoors" since today's network equipment is built on millions of lines of code.[20]

15 Kitindi, Edvin J., Shu Fu, Yunjian Jia, Asif Kabir, and Ying Wang. 2017. "Wireless Network Virtualization with SDN and C-RAN for 5G Networks: Requirements, Opportunities, and Challenges." IEEE Access 5: 19099–115. https://doi.org/10.1109/ACCESS.2017.2744672.

16 European Commission. 2019. "Commission Recommendation – Cybersecurity of 5G Networks." C(2019) 2335 Final. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154.

17 Bundesnetzagentur. 2019. "Katalog von Sicherheitsanforderungen Version 2.0." https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=2.

18 Kleinhans, Jan-Peter. 2018. "Standardisierung Und Zertifizierung zur Stärkung der Internationalen IT-Sicherheit." Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/standardisierung_und_zertifizierung.pdf.

19 Nissen, Chris, John Gronager, Robert Metzger, and Harvey Rishikof. 2019. "DELIVER UNCOMPROMISED: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War." MITRE, no. 18. https://www.mitre.org/publications/technical-papers/deliver-uncompromised-a-strategy-for-supply-chain-security.

20 Lysne, Olav. 2018. The Huawei and Snowden Questions. Can Electronic Equipment from Untrustred Vendors Be Verified? Can an Untrusted Vendor Build Trust Into Electronic Equipment? Simula Springer Briefs on Computing 4. https://doi.org/10.1007/978-3-319-74950-1.

- Certification does not help if the equipment vendor has legitimate network access for maintenance or support purposes. (so-called "insider threat")
- CC-based certification is time consuming, expensive and creates market entrance barriers.[21]

Certification has its place, especially in Europe to ensure “basic” software quality and a level playing field. Such a certification could be implemented under the new European cybersecurity certification framework and be based on GSMA’s Network Equipment Security Assurance Scheme (NESAS)[22] – a much leaner and quicker approach than CC-based certification. Instead of investing a lot of time and resources to establish in-depth CC-based certification for certain types of network equipment, regulators should address the myriad shortcomings by operators, such as network configuration and operations. Lastly, the UK’s National Cyber Security Center (NCSC) – the cybersecurity agency in Europe that has arguably the most experience in assessing the IT security of mobile network equipment – also does not think that IT security certification helps to improve the security of mobile networks.[23]

Source code analysis only assesses maturity of software development
Source code audits can provide insights into the maturity and thoroughness of a company’s software development process. But because of the complexity and modularity of today’s software products, source code analysis is not fit to identify “backdoors” or malicious code. Additionally, vulnerabilities can be hidden in the compiler: The source code needs to be compiled into an actual program that then runs on a base station or router, backdoors or vulnerabilities can be introduced during compilation, after the source has been analyzed.[24] In short, source code analysis has its justification, but it is the wrong tool against purposely hidden vulnerabilities.

21 Kleinhans, Jan-Peter. 2018. “Standardisierung Und Zertifizierung zur Stärkung der Internationalen IT-Sicherheit.” Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/standardisierung_und_zertifizierung.pdf.

22 GSMA. 2018. “Network Equipment Security Assurance Scheme (NESAS)”. https://www.gsma.com/security/network-equipment-security-assurance-scheme/

23 UK DCMS. 2019. UK Telecoms Supply Chain Review Report. https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference.

24 Thompson, Ken. 1984. “Reflections on Trusting Trust.” Communications of the ACM 27 (8): 761–63. https://doi.org/10.1145/358198.358210.

Avoid fragmented mobile network security regulation in EU

When it comes to IT security requirements and certification in general, the EU single market is already fragmented[25] – the EU Cybersecurity Act wants to put an end to this. Different EU member states will have different approaches toward Chinese 5G vendors, because of the geopolitical dimension of the 5G debate (see next section about trustworthiness). Nonetheless, the EU can and should establish common IT security requirements for vendors and operators through the EU cybersecurity certification framework, the Electronic Communication Code[26] and the NIS Directive.[27] Fragmented national regulations (i.e. smart meter gateways) should be avoided at all costs since they create unnecessary costs for operators and vendors and do not incentivize new players to enter the market.

Disaster recovery: RAN diversity and national roaming

Nation state backed attackers will continue to successfully infiltrate[28] and sabotage mobile networks. That is why regulatory measures should not just focus on prevention – hardening the security of network equipment, configuration and operations – but also on recovery.[29] Two policy efforts would potentially limit the damage of a successful network attack: RAN diversity, and national roaming.

- RAN diversity should be established on the national level instead of just looking at each operator individually. The national regulatory authorities should discuss together with all national operators which equipment from which vendor they plan to deploy in which regions. Only by comparing the operators' RAN maps can overdependencies in certain regions be identified. A truly diverse RAN on the national level is much harder to completely shut down than monocultures are.

25 European Commission. 2017. „Commission Staff Working Document – Impact Assessment – EU Cybersecurity Act". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2017:500:FIN.

26 European Council. 2019. "EU telecoms reform". https://www.consilium.europa.eu/en/policies/eu-telecoms-reform/.

27 European Commission. 2019. „The Directive on security of network and information systems (NIS Directive)". https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

28 FireEye. 2019. „MESSAGETAP: Who's Reading Your Text Messages?". https://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html.

29 Saslow, Kate. 2019. „Global Cyber Resilience: thematic and sectoral approaches". https://www.stiftung-nv.de/sites/default/files/saslow_cyber_resilience.pdf.

- National roaming helps in the event of a successful attack but relies on RAN diversity on a national level: If operator A's network has been shut down in a certain region by an attacker, and operator B in that same region deploys RAN from a different vendor, it is highly likely that operator B's network is still up and running. In that event customers from operator A should be able to access operator B's network resources. On a smaller scale this is already the case today for emergency numbers (police, fire fighters, etc.).

Improving network configuration and operations

Poorly configured network equipment and sloppy operations have a significant impact on the overall security posture of mobile networks. Additionally to IT security requirements for network equipment (IT security certification and evaluation), there should be requirements or at least enforceable guidelines for the secure and privacy preserving configuration and maintenance of mobile networks in Europe. The new draft IT security catalog for German telecommunication providers[30] already talks about mandatory logging for remote sessions or security clearance for maintenance personnel. This can only be the start. Working groups, potentially lead by ENISA and/or BEREC, should develop guidelines for the secure configuration of network equipment and best practices for maintenance processes and operations.

Evaluate IT security of deployed mobile networks

There should be economic incentives for operators to evaluate the security of deployed mobile networks. Those economic incentives could be positive, such as tax reduction for security audits by independent third parties, or negative, such as fines if vulnerabilities are found. With all the different measures that will be implemented by the 5G toolbox regulators should evaluate which of the implemented measures are most effective to strengthen the security of mobile networks. Independent security audits and penetration tests of mobile networks would provide the necessary transparency to later evaluate at which level (standards, implementation, configuration, operations) security needs to be further improved.

30 Bundesnetzagentur. 2019. "Katalog von Sicherheitsanforderungen Version 2.0." https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen2.pdf?__blob=publicationFile&v=2.

Strengthen supplier diversity through industrial policy

Diversity on the level of components, equipment, software and suppliers is a precondition for resilient networks.[31] To make it harder for attackers to take down an entire network, diversity is key: no matter how secure a monoculture is, once compromised, it potentially allows the attacker to sabotage the entire network. If a network is built with equipment based on different architectures from different suppliers, it is much harder to compromise the entire network. Additionally, single-vendor networks create a strong lock-in for the operator, making it much harder to swap equipment and switch vendors.[32]

- Interoperability enables diversity, because it allows for operators to switch and use equipment from a different supplier. Interoperability has to be tested extensively, because future 5G networks are so complex. That's why China Mobile, Samsung, Intel, Mavenir, Lenovo and others collaborate at the Open Test and Integration Center (OTIC).[33] Europe's 5G toolbox should support long-term supplier diversity by requiring certain levels of interoperability.
- The ongoing virtualization of both radio access and core networks provides a window of opportunity for new players to enter the market. European policy makers should analyze synergies with industry-lead initiatives, such as O-RAN Alliance[34] and the Telecom Infra Project[35], to better understand how an increasingly virtualized network might impact traditional suppliers and shift power balances.[36] As an example, in a recent request for quotes (RFQ) from Vodafone for open RAN technology, regarding over 100.000 cell sites, none of the incumbent suppliers responded. Out of the seven companies that responded, five are US-based, one is South Kore-

31 "The Prague Proposals." 2019. Prague 5G Security Conference. https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

32 Morris, Iain. 2019. „Europe Sounds Alarm About 'Single Supplier' 5G Deals". https://www.lightreading.com/carrier-security/mobile-security/europe-sounds-alarm-about-single-supplier-5g-deals/d/d-id/754727.

33 Le Maistre, Ray. 2019. "Orange Issues Plea for Help With O-RAN Integration". https://www.lightreading.com/testing/mobile-wireless-testing/orange-issues-plea-for-help-with-o-ran-integration-/d/d-id/754349

34 O-RAN Alliance. https://www.o-ran.org/specifications

35 Telecom Infra Project. https://telecominfraproject.com/.

36 Morris, Iain. 2019. „A Kodak Moment May Await Ericsson, Huawei & Nokia". https://www.lightreading.com/mobile/5g/a-kodak-moment-may-await-ericsson-huawei-and-nokia/d/d-id/755251.

an and one French.[37] This exemplifies how quickly the RAN market could potentially diversify and why these developments should be supported by future regulation.

Vulnerabilities can be introduced into mobile networks at different levels – standards, implementation, configuration and operations. All these levels can and should be addressed by Europe's upcoming 5G toolbox. There are many technical measures that have to be applied no matter how member states individually deal with Chinese 5G vendors. National regulatory authorities and cybersecurity agencies will need to step up their game to define requirements together with national operators, continuously assess new risks, update certification schemes and inform network planning on the national level. Very few European member states will be able to establish their own cybersecurity centers dedicated to mobile network security. Thus, Europe needs to approach the challenge of securing mobile networks by division of labor, smart processes that scale and clearly distributed responsibilities between vendors, operators and governments. Additionally, special attention should be paid to the intersection of IT security and industrial policy: Interoperability supports diversity, which is a precondition for resilience. With increasingly software-defined networks, Europe has a window of opportunity to actively support a diversification of the market through industrial policy.

II. Trustworthiness – Why the origin of technology matters

"Hostile third countries may exercise pressure on 5G suppliers in order to facilitate cyberattacks serving their national interests."
NIS Cooperation Group, EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks

The previous section discussed the challenge of building and maintaining secure mobile networks. The analyzed measures would make it harder for an attacker to exploit vulnerabilities (prevention) or they would at least limit the potential damage of a successful attack (recovery). But apart from exploiting vulnerabilities in software or configuration mobile networks can also be compromised by exploiting legitimate network access: mobile network operators depend on the help of equipment vendors and -suppliers to

37 Hardesty, Linda. 2019. „Vodafone just gave open RAN vendors a huge opportunity". https://www.fiercewireless.com/wireless/vodafone-just-gave-open-ran-vendors-a-huge-opportunity.

provide security updates and help in case of network malfunctions. In these situations, the vendor is often granted administrative remote access to the mobile network: *"This privileged access to the operation, administration and management (OAM) of the network provides an advantage to untrustworthy third parties' personnel to access various type of data such as (subscriber's, system and network configuration, telemetry data)."*[38] In the case of Chinese 5G vendors, namely Huawei and ZTE, the fear is that the Chinese Communist Party (CCP) would coerce its vendors into exploiting their legitimate access to foreign networks for malicious purposes, such as network sabotage.

How to mitigate the risk of exploiting legitimate network access?

The risk of exploiting legitimate network access is hard to mitigate. Most importantly, it cannot be reduced by equipment certification, source code inspection or other technical requirements on the level of standards, implementation or configuration. Certain operational practices can potentially reduce the risk – strictly controlling a vendor's remote access, extensive logging of remote support sessions, anomaly detection, to name a few.[39] It furthermore depends on the business relationship between vendor and operator: Operators do not just buy network equipment from vendors anymore, because of the increasing complexity of mobile networks. They now require "managed services". The vendor will take care of network management, maintenance and potentially many other operations.[40] In such a scenario the vendor has essentially full control over an operator's network – effectively blurring the line between vendor and operator.

In a software-defined world the origin of technology matters

Ultimately, the network operator has to trust the vendor not to abuse this privileged access to network resources for malicious purposes. To complicate things further, it is not just about trusting a vendor now, but for several years to come – the lifetime of deployed mobile network equipment. There are two dimensions to this trust relationship between vendor and operator: How trustworthy is the vendor, and how trustworthy is the vendor's domestic regulatory environment.

38 ENISA. 2019. "ENISA Threat Landscape for 5G Networks." https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

39 UK DCMS. 2019. UK Telecoms Supply Chain Review Report. https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference.

40 Arthur D Little. 2015. „Managed services for telecom operators". https://www.adlittle.com/sites/default/files/viewpoints/ADL_ManagedServicesforTelecomOperators.pdf.

Trusting Huawei and ZTE?

A lot has been written about Huawei's trustworthiness and it is not the goal of this paper to reproduce it all. Indeed, from a Western government's perspective there seem to be reasons not to trust the company.

- The opaque corporate governance structure[41] makes it almost impossible to understand management hierarchies, ownership structures[42] or ties to the CCP.
- There are several cases of intellectual property (IP) theft and at least collusion for espionage throughout the company's history.[43]
- Huawei is not a public company and thus does not have to file any financial statements.[44]
- Huawei seems to have "significant software engineering and cyber security problems".[45]

Both Chinese mobile network equipment vendors have to step up their game to prove their trustworthiness: ZTE is a State-Owned Enterprise (SOE) under the direct leadership and control of the CCP while Huawei is a very opaque private company[46] whose history is filled with allegations of IP theft and espionage. Yet, this should not lead to a general distrust against Chinese ICT companies[47] and there are examples of more transparent, internationalized and publicly accountable tech companies out of China.[48]

41 Hawes, Colin, and Grace Li. 2017. "Transparency and Opaqueness in the Chinese ICT Sector: A Critique of Chinese and International Corporate Governance Norms". Asian Journal of Comparative Law. Vol. 12. https://doi.org/10.1017/asjcl.2017.8.

42 Balding, Christopher, and Donald Clarke. 2019. "Who Owns Huawei?" https://dx.doi.org/10.2139/ssrn.3372669.

43 RWR Advisory Group. 2019. „Huawei Risk Tracker". https://huawei.rwradvisory.com/.

44 Foster, Andrew, and Nicholas Borst. 2019. „Time is ripe for Huawei to launch an IPO, to address political and security concerns once and for all". https://www.scmp.com/comment/insight-opinion/article/3011510/time-ripe-huawei-launch-ipo-address-political-and-security.

45 HCSEC. 2019. "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board – Annual Report 2019." https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019.

46 Zaagman, Elliott. 2019. " Huawei's Problem Of Being Too 'Chinese'". https://supchina.com/2019/01/24/huaweis-problem-of-being-too-chinese/

47 Feng, Ashley. 2019. „We Can't Tell if Chinese Firms Work for the Party". https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/

48 Zaagman, Elliott. 2017. "Thinking About Working For A Chinese Company? First, Find Out If It's A 'Lenovo' Or A 'Huawei'". https://supchina.com/2017/10/09/thinking-working-chinese-company-first-find-lenovo-huawei/.

Trusting the Chinese government?

A company's trustworthiness cannot be assessed in a vacuum but has to be put in context with its regulatory environment since any company has to follow its national laws. The 2013 Snowden revelations are the best example for how government action affects the trustworthiness of their companies: The leaked documents presented proof of the US government's systemic exploitation of Internet infrastructure for surveillance purposes and how their companies could be forced or coerced to cooperate.[49] Europe and China[50] lost trust in US ICT companies which lead to lost revenues for the latter.[51] During the years after the Snowden revelations US ICT companies publicly advocated for reforming signal intelligence laws and practices. They signed public letters for surveillance law reform[52], advocated through lawsuits for more transparency about surveillance practices[53], fought in court against breaking the encryption of digital communication[54] and ultimately pushed the government toward at least some form of reform. In the years since 2013 the US government became more transparent about its surveillance practices[55] and there is now a rich ecosystem of independent think tanks and universities all engaged in the debate about the legitimacy of government surveillance laws and practices. The US government is certainly no role model[56] when it comes to democratic control of signal intelligence and law enforcement agencies.[57] But it realized the detrimental effect of its regulations and practices to the

49 Tréguer, Félix. 2018. "US Technology Companies and State Surveillance in the Post-Snowden Context: Between Cooperation and Resistance." https://halshs.archives-ouvertes.fr/halshs-01865140.

50 Interos Solutions. 2018. "Supply Chain Vulnerabilities from China in U.S. Federal Information and Communications Technology." U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION. https://www.uscc.gov/research/supply-chain-vulnerabilities-china-us-federal-information-and-communications-technology.

51 Miller, Claire Caine. "Revelations of N.S.A. Spying Cost U.S. Tech Companies". https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

52 Reform Government Surveillance. https://www.reformgovernmentsurveillance.com/news-press/

53 Google. 2016. „Sharing National Security Letters with the public". https://www.blog.google/outreach-initiatives/public-policy/sharing-national-security-letters-public/.

54 Kahney, Leander. 2019. „The FBI Wanted a Backdoor to the iPhone. Tim Cook Said No". https://www.wired.com/story/the-time-tim-cook-stood-his-ground-against-fbi/.

55 Joyce, Rob. 2016. „Disrupting Nation State Hackers". Presentation at ENIGMA conference. https://www.usenix.org/node/194636.

56 Wetzling, Thorsten, and Kilian Vieth. 2018. „Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations". https://www.stiftung-nv.de/sites/default/files/upping_the_ante_on_bulk_surveillance_v2.pdf.

57 Center for Demcoracy & Technology. 2018. „Tech Talk: The State of Surveillance in the US and Europe". https://cdt.org/insights/tech-talk-the-state-of-surveillance-in-the-us-and-europe/.

perceived trustworthiness of US ICT companies abroad. Due to an independent judicial system, a strong public sphere, a free press, a critical parliament and independent academic research it was possible to voice grievances, advocate for change and take the government to court.

In stark contrast to that, the Chinese government did very little since summer 2018 to address critique against its Anti-Terrorism Law, Counterespionage Law, Cybersecurity Law and most importantly its National Intelligence Law.[58] It is furthermore highly unlikely that either Huawei or ZTE would take the CCP to court to fight for more transparency about the government's surveillance practices or its interpretation of the relevant laws. After realizing that foreign governments are not just worried about Huawei's trustworthiness but even more so about the trustworthiness of the CCP, Huawei offered to essentially sell its blueprints, source code and knowledge how to build network equipment to any Western company.[59]

The geopolitics of trusting foreign vendors

How likely it is that a foreign government coerces one of their vendors into exploiting legitimate network access for malicious activities depends on geopolitics, not technology. Ultimately, the decision whether to trust Chinese 5G vendors has three dimensions: trustworthiness of the network equipment, trustworthiness of the company itself and geopolitics with China. This is why governments have varying responses to Chinese 5G vendors, ranging from blanket bans to unfettered market access. This makes it highly unlikely that all European member states will follow the same approach. While Estonia[60], Poland[61] and Romania[62] all signed memorandums of understanding with the US to effectively avoid Chinese 5G vendors, Germany and the UK are much more reluctant to do the same. Russia fully embraces Chinese 5G vendors

58 Clarke, Donald. 2019. "The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law." https://dx.doi.org/10.2139/ssrn.3354211.

59 The Economist. 2019. "Ren Zhengfei may sell Huawei's 5G technology to a Western buyer". https://www.economist.com/business/2019/09/12/ren-zhengfei-may-sell-huaweis-5g-technology-to-a-western-buyer.

60 White House. 2019. „United States–Estonia Joint Declaration on 5G Security". https://www.whitehouse.gov/briefings-statements/united-states-estonia-joint-declaration-5g-security/.

61 Republic of Poland, and United States of America. 2019. "U.S.-Poland Joint Declaration on 5G." https://www.premier.gov.pl/static/files/files/deklaracja_en-1.pdf.

62 US Embassy in Romania. 2019. „Joint Statement from President of the United States Donald J. Trump and President of Romania Klaus Iohannis". https://ro.usembassy.gov/joint-statement-from-president-of-the-united-states-donald-j-trump-and-president-of-romania-klaus-iohannis/.

to build the country's mobile network[63] partly because the Russian government is geopolitically very much aligned with China – not just in the military domain but increasingly in form of a high-technology partnership.[64] In Japan, which has very real geopolitical tensions with China not just in the East China Sea[65], Chinese vendors of mobile network equipment never played a significant role, only one out of four Japanese operators used Huawei equipment to some extent.[66]

What does this mean for Europe? From a policy perspective, the 5G debate is so challenging because we build a critical infrastructure with technology originating from a country that Europe perceives as a "systemic rival".[67] Europe has to trust the technology vendors who, at the same time, have to follow Chinese laws and the CCP. Naturally, those laws and the (lack of) rule of law negatively affect the trustworthiness of Chinese vendors abroad – the origin of technology matters. But this argument is a slippery slope in a software-defined world: If everything will be software-defined, IT security will always be an issue. Thus, Western governments could potentially always ban Chinese vendors based on national security grounds.[68] That leads to a downward spiral of simply distrusting any piece of technology of Chinese origin. Based on this logic, the United States are already limiting research collaboration[69], technology transfer in different sectors[70] and the import of certain technology of Chinese origin.[71] Of course, Europe should not be naïve about China's

63 Simes, Dimitri. 2019. „Russia and Huawei team up as tech cold war deepens". https://asia.nikkei.com/Politics/International-relations/Russia-and-Huawei-team-up-as-tech-cold-war-deepens.

64 Bendett, Samuel, and Elsa B Kania. 2019. "A New Sino-Russian High-Tech Partnership." https://www.aspi.org.au/report/new-sino-russian-high-tech-partnership.

65 Council on Foreign Relations. 2019. „Tensions in the East China Sea". https://www.cfr.org/interactive/global-conflict-tracker/conflict/tensions-east-china-sea.

66 Satake, Minoru. 2018. „Japan's 4 carriers to shun Chinese 5G tech". https://asia.nikkei.com/Business/Companies/Japan-s-4-carriers-to-shun-Chinese-5G-tech.

67 European Commission. 2019. „EU-China – A Strategic Outlook". https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf.

68 Barnett, Jackson. 2019. „Why is DJI getting the Huawei treatment?". https://www.cyberscoop.com/dji-cybersecurity-huawei-data-breach-china/.

69 Benderley, Beryl Lieff. 2019. „U.S. academics, make sure you know the rules about foreign funding and affiliations". https://www.sciencemag.org/careers/2019/09/us-academics-make-sure-you-know-rules-about-foreign-funding-and-affiliations.

70 U.S.-China Economicy and Security Review Commission. 2019. " How Chinese Companies Facilitate Technology Transfer from the United States". Staff Research Report. https://www.uscc.gov/files/000798.

71 Wiley Rein. 2019. „Commerce Publishes Proposed Rules Implementing Communications Supply Chain Executive Order". https://www.wileyrein.com/newsroom-articles-5286.html.

ambitions[72] but it is unclear if "decoupling" is the right answer.[73] Instead, Europe should establish clear criteria to assess the trustworthiness of a technology vendor and identify certain technology domains in which suppliers and operators are scrutinized based on those criteria. The 5G toolbox should therefore include criteria for assessing the trustworthiness of a company that also address the regulatory environment.[74] The goal would be to be able to hold companies accountable in the event of malicious activity or willful wrongdoing. This would at least provide member states with a reference for their national regulation. Additionally, since 5G is just the beginning, Europe will most likely have similar debates about trustworthiness of Chinese technology providers in different areas, such as AI or smart cities or energy systems.[75] The 5G toolbox should provide the basis for a broader debate about evaluating the trustworthiness of technology providers. The assessment of a company's trustworthiness should be based on technical and non-technical criteria. While ENISA, the NIS Cooperation Group and BEREC are leading the work on IT security requirements, those requirements will not be able to address trustworthiness of companies and regulatory systems. For those the intelligence community, trade and foreign policy experts need to be involved.[76]

72 Zenglein, Max J, and Anna Holzmann. 2019. "Evolving Made in China 2025." MERICS, no. 8. https://www.merics.org/en/papers-on-china/evolving-made-in-china-2025.

73 Bloom, Nicholas, Charles I. Jones, John Van Reenen, and Michael Webb. 2016. "Are Ideas Getting Harder to Find?" https://web.stanford.edu/~chadj/IdeaPF.pdf.

74 Lee-Makiyama, Hosuk. 2019. „5G: What we talk about when we talk about trust – the EU risk assessment process". https://ecipe.org/blog/5g-eu-risk-assessment-process/.

75 Stacey, Kiran. 2019. „Huawei shuts down solar energy business in the US". https://www.ft.com/content/aa4100c4-9772-11e9-8cfb-30c211dcd229.

76 Albrycht, Izabela, and Joanna Świątkowska. 2019. "THE FUTURE OF 5G OR QUO VADIS, EUROPE?" Kosciuszko Institute. https://ik.org.pl/en/publications/the-future-of-5g-or-quo-vadis-europe/.

III. Conclusion

"A diverse and vibrant communications equipment market and supply chain are essential for security and economic resilience."
The Prague Proposals, Prague 5G Security Conference[77]

Independent of the question how to deal with Chinese 5G vendors, Europe will have to address three different policy challenges – IT security, trustworthiness and industrial policy. As mentioned in the first section, there is a lot Europe can and should do to improve the **security of mobile networks**. Since IT security is a shared responsibility between operators, vendors and governments, the focus should be on common IT security requirements in Europe – a fragmented regulatory landscape should be avoided at all costs. Those requirements should fit to increasingly virtualized, software-defined, highly heterogeneous networks. Since operators are already struggling to securely configure and run their 4G networks, this will become an even bigger challenge in a 5G world. That is why the focus should not just be on equipment vendors but even more so on mobile network operators.

The next challenge is to assess the **trustworthiness of vendors** based on transparent, verifiable and enforceable criteria. This will be necessary not just for 5G but for a variety of emerging technologies. Such an approach would try to strike a balance between furthering decoupling between Western governments and China and ignoring China's geopolitical ambitions. Identifying those criteria will not be easy and needs experts from different policy domains. With those criteria in place, there is the hope that China realizes that in the long term, certain Chinese laws and practices significantly undermine the trustworthiness of Chinese technology suppliers abroad. If this is not the case, it will at least provide a better foundation for European policy makers to strategically assess different technology domains from a national security perspective.

Lastly, Europe has to address the **industrial policy dimension of the 5G debate**. European suppliers are still doing fine in certain areas, such as 5G standard essential patents (SEP)[78] and both Nokia and Ericsson are the main suppliers for some of the leading 5G nations – US, Japan and South Korea.

77 "The Prague Proposals." 2019. Prague 5G Security Conference. https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

78 Noble, By Matthew, Jane Mutimear, and Richard Vary. 2019. "Determining Which Companies Are Leading the 5G Race." https://www.twobirds.com/en/news/articles/2019/global/pattern-team-examine-difficulties-in-leadership-of-companies-in-5g-patent.

But the supplier market is quickly changing and new players are entering the market: The advance of software-defined networks plays into the hands of the US industry.[79] Europe clearly needs "defensive measures in competition, anti-subsidy, public procurement and related policy fields" to better deal with China.[80] But it also needs a pragmatic European industrial policy and member states that believe in the single market.[81] In the case of 5G, a first step would be to actively support the diversification of the supplier market and addressing anti-competitive advantages of Chinese vendors.[82]

79 Kania, Elsa B. 2019. "Securing Our 5G Future: The Competitive Challenge and Considerations for U.S. Policy." https://www.cnas.org/publications/reports/securing-our-5g-future.

80 Huotari, Mikko, and Agatha Kratz. 2019. "Beyond Investment Screening: Expanding Europe's Toolbox to Address Economic Risks from Chinese State Capitalism." https://rhg.com/wp-content/uploads/2019/10/DA_Studie_ExpandEurope_2019.pdf.

81 POLITICO. 2019. „Ericsson boss bemoans lack of European support on 5G". https://www.politico.eu/article/borje-ekholm-global-5g-battle-ericsson-ceo-bemoans-lack-of-european-support/.

82 European Commission. 2014. „EU not to pursue the anti-dumping investigation against mobile telecommunications networks from China". https://ec.europa.eu/commission/presscorner/detail/en/IP_14_339.

About the Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent think tank that develops concrete ideas as to how politics can shape technological change in society, the economy and the state. In order to guarantee the independence of its work, the organization adopted a concept of mixed funding sources that include foundations, public funds and businesses.

Issues of digital infrastructure, the changing pattern of employment, IT security or internet surveillance now affect key areas of economic and social policy, domestic security or the protection of the fundamental rights of individuals. The experts of the SNV formulate analyses, develop policy proposals and organize conferences that address these issues and further subject areas.

About the Author

Jan-Peter Kleinhans is director of the project IT Security in the Internet of Things (IoT). Currently his work focuses on the intersection of global semiconductor supply chains, IT security and geopolitics. He has a special interest in the security and resilience of our future mobile networks – 5G. After joining SNV in 2014 Jan-Peter analyzed why the market failed to produce reasonably trustworthy consumer IoT devices. He explored if and how standardization, certification and market surveillance can create economic incentives for IoT manufacturers to produce secure and trustworthy IoT devices.

How to Contact the Author

Jan-Peter Kleinhans
Project Director "IT security and the Internet of Things"
jkleinhans@stiftung-nv.de
+49 (0)30 81 45 03 78 93
@JPKleinhans

Imprint

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok