February 2019 · Jan-Peter Kleinhans

5G vs. National Security

A European Perspective

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Executive Summary

The transition to the fifth generation of mobile networks (5G) is often portrayed as a race – between economic systems and between companies. Who defines the standards? Which company holds critical standard-essential patents? Which nation has the most pilots to test equipment and applications? Who is the fastest to roll out the infrastructure? What are new business models? The race for 5G is truly multi-dimensional, highly complex and fast-moving. Yet, recently the debate has been dominated by one single question: does the deployment of Chinese 5G network equipment pose a threat to the national security of western countries?

Since there is no way to prove the absence of malicious code or vulnerabilities in any piece of hardware or software, ultimately one has to trust the manufacturer to keep devices secure and not exploit vulnerabilities. This trust heavily depends on the legal and regulatory system in which the manufacturer operates. So it is not just about trusting Huawei or ZTE but trusting China. There are many good reasons to distrust China. Yet, governments should be cautious not to conflate issues with China's geopolitical strategy, industrial policies or espionage with the trustworthiness and resilience of our future mobile networks.

The trustworthiness and resilience of mobile networks depend not just on the robustness of 5G standards but how those standards are implemented by the manufacturer and how securely these systems are configured and managed by the operator. On these four levels – standards, implementation, configuration and operation – proper threat modelling and risk minimization can go a long way toward addressing threats such as espionage or network disruption. Independent of the question whether to ban Chinese manufacturers, European member states should follow a risk minimization approach via regulation on all four levels.

It is important to understand that the debate about 5G and Chinese network equipment was simply the first but is not unique. China plays a key role in a variety of ICT supply chains and Europe should strategically assess potential risks that stem from these dependencies. A supply chain review process in different sectors and key technologies would enable us to identify and assess future dependencies that potentially threaten our national security. Based on these, proper risk minimization strategies should be developed.

The German Federal Foreign Office provided financial support for research for this paper. The views expressed in the paper are only those of the authors. The author wants to thank all participants of the workshop "5G vs National Security" (24 January 2019).

Introduction

Mobile networks play an increasingly important role in our economy and society. In 2017 mobile technologies and services generated 3.3% or €550 billion of GDP in Europe.[1] The transition to the next generation of mobile networks, from 4G to 5G, is often portrayed as a technological race between countries, political systems and companies.[2] Up until 4G the underlying standards, such as LTE-Advanced, and the entire architecture were mainly designed for human communication. Only with 5G does the focus shift to truly enable massive machine-to-machine communication for the industrial Internet of Things, autonomous cars or smart cities. 5G networks do not simply transmit communication anymore, but will be, next to the power grid, the central infrastructure and enabler for large parts of our economy. Yet just like any other infrastructure 5G is also not an end in itself: if and how quickly industries will develop applications, systems and services that utilize 5G networks will depend on a variety of factors. Thus, the current race for future mobile networks happens simultaneously in many different arenas: Setting the standards that define the technology, rolling out the nationwide infrastructure, developing new applications and even business models that convince established industries to invest in the technology. The race for 5G is truly global, fast-moving and highly complex.

Yet recently the debate has been dominated by one single question: Does the deployment of 5G equipment from Chinese manufacturers pose a risk to our national security?[3] By becoming such a critical infrastructure for our future economy, the resilience and trustworthiness of 5G mobile networks is of utmost importance. By infiltrating future mobile networks, an attacker potentially disrupts not just communication but paralyses parts of the economy. This is why several governments in Europe now started to worry about the issue, even though Huawei and ZTE, the two dominant Chinese mobile

1 GSMA. 2018. “The Mobile Economy Europe 2018”. https://www.gsma.com/mobileeconomy/europe/

2 Josh Chin. 2019. “The Internet, Divided Between the U.S. and China, Has Become a Battleground”. The Wall Street Journal. https://www.wsj.com/articles/the-internet-divided-between-the-u-s-and-china-has-become-a-battleground-11549688420

3 U.S.-China Economic And Security Review Commission. 2018. “Supply Chain Vulnerabilities from China in U . S . Federal Information and Communications Technology.” https://www.uscc.gov/Research/supply-chain-vulnerabilities-china-us-federal-information-and-communications-technology.

network equipment manufacturers, have been active in Europe since at least the early 2000s.

There are just a few manufacturers who produce essential 5G equipment – small cell radio units or base stations: Huawei (China), Ericsson (Sweden), Nokia (Finland), ZTE (China) and Samsung (South Korea).[4] There are countless telecommunication operators such as British Telecom, Vodafone or Telefonicà in the world and governments in general trust those (highly regulated) national operators. Yet, governments might not necessarily trust the manufacturers from which operators buy their equipment. Many western governments are not comfortable with the idea that Chinese companies build large parts of the 5G network infrastructure on which the entire economy depends.[5] Thus, some governments started to regulate the "upstream" supply chain of telecommunication operators by various means – with the intended effect to stop the operator from deploying Chinese equipment.[6]

To understand this "politicization of the supply chain" one has to understand a variety of trends in technology, economics and international relations. To this end the following section will elaborate why complexity in hardware, software and ICT systems is a challenge for IT security and why operators always have to trust the manufacturer. The second section will explain why it matters where a product is developed and why China's legal and political system impacts the trustworthiness of a Chinese ICT product. The third section will then look at China's increasing role in any ICT supply chain and their expanding participation in technology standardization, including patents – to argue that similar debates just like now with 5G will happen in other sectors. Against the background of those trends the fourth section will illustrate what could be done to make 5G mobile networks in Europe more secure. The last section will elaborate why it is dangerous to conflate different aspects of the debate and give recommendations for how European member states could position themselves.

4 Telecomlead. 2018. "RAN market: How Huawei, Ericsson, Nokia, ZTE, Samsung performed". https://www.telecomlead.com/telecom-equipment/ran-market-how-huawei-ericsson-nokia-zte-samsung-performed-85605

5 David E. Sanger, et al. 2019. "In 5G Race With China, U.S. Pushes Allies to Fight Huawei". https://nyti.ms/2S6LObM

6 Paul Triolo and Kevin Allison. 2018. "The Geopolitics Of 5G." https://www.eurasiagroup.net/live-post/the-geopolitics-of-5g

Section 1 – Complexity is the enemy of security

The complexity of today's ICT systems is hardly comprehendible: The System-on-Chip (SoC) of current smartphones have more than 8 billion transistors.[7] Current desktop operating systems have more than 50 million lines of code. Additionally, software is highly modular and often utilizes functionality from a variety of software libraries developed by third parties. It allows companies to focus on their core business, outsourcing everything else. Manufacturers might buy 99% of parts from global vendors and focus on being highly innovative in just one area – a single piece of hardware or software. This means that most if not all hardware and software products rely on a well functioning and highly complex interplay between countless actors – the supply chain. Which also means that the security of a final product or service heavily depends on every party in the entire supply chain doing their homework – consistently and constantly.[8] Understandably, this fast moving ICT market with increasingly complex products poses a real challenge for effective supply chain risk management and IT security.[9]

Yet for these highly complex and interdependent systems we lack meaningful ways to assess their security and trustworthiness.[10] Traditional IT security assessment mechanisms, such as the Common Criteria Standard, are expensive, slow and simply ineffective for interconnected systems with frequently updated software.[11] Security assessments, code reviews and penetration tests certainly help to improve the overall software quality but they cannot prove the *absence* of malicious code or "backdoors" – hidden remote access that can be exploited to gain full control over a device.[12] This *inability* to prove the absence of malicious code or backdoors in interconnected ICT

7 Joe Osborne. 2018. "Qualcomm Snapdragon 1000 for laptops could pack 8.5 billion transistors". https://www.techradar.com/news/qualcomm-snapdragon-1000-for-laptops-could-pack-85-billion-transistors

8 Richard J. Danzig. 2014. "Surviving on a Diet of Poisoned Fruit Reducing the National Security Risks of America's Cyber Dependencies." https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies

9 NIST. "Cyber Supply Chain Risk Management". https://csrc.nist.gov/Projects/Supply-Chain-Risk-Management

10 Jan-Peter Kleinhans. 2017. "Internet of Insecure Things: Can Security Assessment Cure Market Failure?". https://www.stiftung-nv.de/sites/default/files/internet_of_insecure_things.pdf

11 Jan-Peter Kleinhans. 2018. "Standardisierung und Zertifizierung zur Stärkung der internationalen IT-Sicherheit". Policy Paper. Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/standardisierung_und_zertifizierung.pdf

12 Cormac Herley. 2016. "Unfalsifiability of Security Claims." Proceedings of the National Academy of Sciences I (1): 201517797. https://doi.org/10.1073/pnas.1517797113.

systems is true for any manufacturer – not just Chinese.[13] The reliance on 5G networks makes our economy more vulnerable, no matter who builds the network. With Chinese manufacturers, such as Huawei or ZTE, the fear is that it makes it easier for Chinese intelligence agencies to conduct espionage or disrupt a foreign network.[14]

Because of this lack of technical measures to prove the trustworthiness of equipment, the legal and regulatory system in which a manufacturer operates is highly relevant. The current debate is not just about trust in Chinese manufacturers or the trustworthiness of their equipment, but the lack of trust in the Chinese government.[15] What complicates this trust relationship is the fact that manufacturers have to constantly provide software updates to keep network equipment secure: Every future software update could be exploited by state-sponsored attackers to infiltrate foreign networks.

Section 2 – Trusting China?

The previous section argued that our economy becomes more vulnerable with increasing connectivity and interconnectedness. Furthermore, there is a lack of tools to guarantee the trustworthiness of highly complex, interconnected and interdependent ICT systems, such as mobile networks. Thus, society, governments and mobile operators have to trust the manufacturer to fix vulnerabilities and this **trust depends on the legal and political system** in which the manufacturer operates: If Huawei or ZTE were not Chinese companies, there would be no debate.

Cisco owns around 60% of the global network switch market.[16] At the same time, security researchers regularly find hardcoded passwords and backdoor accounts in Cisco's hardware and software.[17] European countries trust

13 Olav Lysne. 2018. "The Huawei and Snowden Questions: Can Electronic Equipment from Untrusted Vendors be Verified? Can an Untrusted Vendor Build Trust Into Electronic Equipment?". https://www.springer.com/de/book/9783319749495

14 Stephen R. van Etten. 2016. "Cyber Supply Chain Security: Can The Backdoor Be Closed With Trusted Design, Manufacturing And Supply?" https://apps.dtic.mil/dtic/tr/fulltext/u2/1040724.pdf

15 Nicolas Botton and Hosuk Lee-Makiyama. 2018. "5G and National Security: After Australia's Telecom Sector Security Review." https://ecipe.org/publications/5g-national-security-australias-telecom-sector/

16 Forbes. 2017. "Where does Cisco stand in the Ethernet Switch Market?". https://www.forbes.com/sites/greatspeculations/2017/04/12/where-does-cisco-stand-in-the-ethernet-switch-market/#5f63f5b3434a

17 Lucian Armasu. 2018. "Backdoors Keep Appearing in Cisco's Routers". https://www.tomshardware.com/news/cisco-backdoor-hardcoded-accounts-software,37480.html

Cisco and the legal system of the USA to fix instead of systemically exploit these vulnerabilities. This is why, even after the Snowden revelations, Cisco equipment is being deployed in Europe: The Snowden documents revealed in 2014 that the US National Security Agency (NSA) had a team to install "beacon implants" on certain types of network devices (routers, servers, etc.) while being shipped to the customer.[18] NSA would intercept and open shipments, install the custom software and then send the packages on their way to the customer again. After these tactics became public, China encouraged domestic companies to avoid foreign manufacturers. As a result, Cisco lost 21% revenue in China in fiscal year 2015 compared to the year before.[19] There was no ban of Cisco equipment in European networks because of the trust in the US legal system and a mutually beneficial relationship.

Western intelligence agencies exploit vulnerabilities in telecommunication equipment, of course. But one significant difference is that western manufacturers can and do fight against this in court: Apple fought against the US Federal Bureau of Investigation about access to customer data to help in an investigation.[20] It is highly unlikely[21] that something similar would be possible with a Chinese company in front of Chinese courts.[22] Because of flawed and vulnerable ICT systems, the legal environment out of which a manufacturer operates has been and will continue to be part of the risk assessment.

What complicates matters further is the fact, that the Chinese government conducts extensive and **pervasive industrial espionage** to the direct advantage of their own economy[23], including military and defense capabilities.[24] To

18 NSA. 2010." Stealthy Techniques Can Crack Some of SIGINT's Hardest Targets". https://www.eff.org/files/2015/01/27/20150117-spiegel-supply-chain_interdiction_-_stealthy_techniques_can_crack_some_of_sigints_hardest_targets.pdf

19 Jeremy Kirk. 2015. "How Cisco is trying to keep NSA spies out of its gear". https://www.pcworld.com/article/3005709/how-cisco-is-trying-to-keep-nsa-spies-out-of-its-gear.html

20 Office of the Inspector General U.S. Department of Justice . 2018. "A Special Inquiry Regarding the Accuracy of FBI Statements Concerning its Capabilities to Exploit an iPhone Seized During the San Bernardino Terror Attack Investigation". https://oig.justice.gov/reports/2018/o1803.pdf

21 Ashley Feng. 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/

22 Erica Wiking Häger, et al. 2017. "National Intelligence Law: General Introduction of the Draft National Intelligence Law." https://www.mannheimerswartling.se/globalassets/publikationer/national-intelligence-law.pdf.

23 Elsa B. Kania. 2018. "Testimony before the House Permanent Select Committee on Intelligence: China's Threat to American Government and Private Sector Research and Innovation Leadership." https://www.cnas.org/publications/congressional-testimony/testimony-before-the-house-permanent-select-committee-on-intelligence.

24 William C. Hannas, et al. 2013. "Chinese Industrial Espionage: Technology Acquisition and Military Modernisation". Routledge.

this end the Chinese government uses any means necessary: Hiring or bribing spies,[25] forced technology transfers for foreign companies in exchange for market access,[26] state-sponsored hacking to steal trade secrets and conducting cyber espionage. Following are some examples of Chinese industrial espionage campaigns that exploited weaknesses in ICT systems:

- The **APT10**[27] campaign compromised managed IT service providers (MSP) to establish legitimate access to any of their customer's networks.[28] Many organizations rely on MSPs for a variety of services, such as accounting or cloud infrastructure. Instead of targeting each company individually, APT10 focused on infiltrating a handful of large MSPs. Through highly targeted spear-phishing mails, APT10 obtained credentials from system administrators. These would then be used by the attackers to impersonate users and gain legitimate access to company networks to conduct industrial espionage.[29]

- **APT1** is active since at least 2006 with clear ties to the Chinese People's Liberation Army (PLA) and the government. The campaign attacked over 140 companies within roughly 20 different industries. On average APT1 would hide in an organization's network for almost one year. A report states that, "*as with most other APT groups, spear phishing is APT1's most commonly used technique.*"[30]

- Members of the **APT3** group were charged with cyber crime offenses by the US Department of Justice – among other things, they stole 407GB of confidential data from Siemens' "*energy, technology and transportation businesses*".[31] Similar to other groups, they used malicious spear-phishing mails and zero-day exploits (Adobe Flash).[32]

25 Garrett M. Graff. 2018. "China's 5 Steps for Recruiting Spies". https://www.wired.com/story/china-spy-recruitment-us/

26 BDI. 2019. "Partner and Systemic Competitor – How Do We Deal with China's State-Controlled Economy?". Policy Paper. https://e.issuu.com/embed.html#2902526/66954145

27 APT stands for Advanced Persistent Threat, a term often used for state-sponsored cyber attacks

28 PwC UK and BAE Systems. 2017. "Operation Cloud Hopper". https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf

29 Brian Barrett. 2018. "How China's Elite Hackers Stole the World's Most Valuable Secrets". https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/

30 FireEye Mandiant. 2013. "APT1: Exposing One of China's Cyber Espionage Units". https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

31 Thomas Brewster. 2017. "Chinese Trio Linked To Dangerous APT3 Hackers Charged with Stealing 407GB of Data from Siemens". https://www.forbes.com/sites/thomasbrewster/2017/11/27/chinese-hackers-accused-of-siemens-moodys-trimble-hacks/#9a8efc19ef74

32 FireEye. 2015. "Demonstrating Hustle, Chinese APT Groups Quickly Use Zero-Day Vulnerability (CVE-2015-5119) Following Hacking Team Leak". https://www.fireeye.com/blog/threat-research/2015/07/demonstrating_hustle.html

Chinese industrial espionage is a direct threat to western companies and economies. The US Department of Justice states that, "*more than 90 percent of the Department's cases alleging economic espionage over the past seven years involve China. More than two-thirds of the Department's cases involving thefts of trade secrets are connected to China.*"[33] As mentioned before, China seems to conduct industrial espionage by any means necessary. But the above examples also indicate that mobile communication networks do not seem to be an attack vector to conduct industrial espionage: It seems much more efficient to utilize social engineering, spear-phishing and network exploitation rather than trying to hack into a mobile base station. Successful APT groups have not used mobile networks to steal confidential data or gain access to an organization's network. Of course, state-sponsored attackers might shift toward exploiting mobile networks in the future if those networks carry valuable data *and* can be exploited more easily than traditional (office) IT systems. It is important to fight any type of Chinese industrial espionage[34] and call China out on their tactics – both Europe[35] and European industry associations[36] seem to do that more openly – but this has little to do with the security and trustworthiness of our mobile infrastructure.

The current public debate around Huawei implies that a 5G network built with Chinese equipment makes it easier for the Chinese government to conduct industrial espionage – this assumption is at least questionable. Today's ICT systems are complex, interconnected and vulnerable and provide more than enough attack surface for any state-sponsored attacker. Chinese industrial espionage relies on these ICT systems and (so far) not on mobile communication networks, no matter who the manufacturer may be.

33 US Department of Justice. 2018. "Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers". https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers

34 Office Of The United States Trade Representative Executive Office Of The President. 2018. "Update Concerning China's Acts, Policies And Practices Related To Technology Transfer, Intellectual Property, And Innovation." https://ustr.gov/sites/default/files/enforcement/301Investigations/301%20Report%20Update.pdf

35 European Commission. 2018. "EU steps up WTO action against China's forced technology transfers". http://trade.ec.europa.eu/doclib/press/index.cfm?id=1963

36 BDI. 2019. "Partner and Systemic Competitor – How Do We Deal with China's State-Controlled Economy?". Policy Paper. https://e.issuu.com/embed.html#2902526/66954145

Section 3 – Rise of China

The previous sections argued that with the advancing interconnectedness and digitalization our economy becomes more vulnerable: today's ICT systems are too complex to prove the absence of malicious code. Thus the chain of trust extends from the product to its manufacturer and the legal and political system out of which the manufacturer operates. That explains why the current debate is to a large extent about the (missing) trust in the Chinese government – instead of purely technical aspects of Huawei's or ZTE's equipment. This lack of trust does not simply stem from China's pervasive industrial espionage but also from Europe's struggle with China's increasing geopolitical power.[37]

China has a clear vision of technological dominance in certain, if not all, high-tech sectors.[38] The Chinese government supports this vision with highly protectionist industrial policies that foster the development of indigenous innovation and national champions, especially in the ICT sector.[39] At the same time foreign companies experience forced technology transfer almost as a precondition for market access.[40] Looking at the ICT sector one of the direct outcomes is that China is not (just) the factory of the world anymore.[41] Not just with 5G China strongly pushed into standardization organizations to ensure that Chinese companies hold Standard Essential Patents.[42] With Huawei, maybe for the first time, China has a highly competitive, highly in-

37 James Dobbins, et al. 2019. "Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue: Different Challenges, Different Responses". https://www.rand.org/pubs/perspectives/PE310.html.

38 Gregory C. Allen. 2019. "Understanding China's AI Strategy : Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security." https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

39 Martina F. Ferracane and Hosuk Lee-Makiyama. 2017. "China's Technology Protectionism and Its Non-Negotiable Rationales." http://ecipe.org/publications/chinas-technology-protectionism/

40 Theodore Moran. 2015. "Should US Tech Companies Share Their "Source Code" with China". http://blogs.piie.com/china/?p=4542

41 Esther Majerowicz and Carlos Aguiar de Medeiros. 2018. "Chinese Industrial Policy in the Geopolitics of the Information Age: The Case of Semiconductors". https://doi.org/10.1590/198055272216

42 John Chen, et al. 2018. "China's Internet of Things – Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission." https://www.uscc.gov/Research/chinas-internet-things;
Tim Pohlmann. 2018. "Who is leading the 5G patent race?". https://www.lexology.com/library/detail.aspx?g=64ea84d0-f9ce-4c2b-939b-dec5c2560e06

novative[43] company that quite quickly became the market leader in a key infrastructure.[44]

This is why much of the debate around Huawei has to be seen in the context of the current "tech war" and the fight between different economic systems.[45] This will not go away: China finished their own global positioning system (BDS) ahead of time.[46] In certain high-tech fields China is already publishing the majority of leading scientific papers.[47] In the future we will likely see more Chinese companies becoming global market leaders in certain areas – or at least play central roles in ICT supply chains.[48]

Even though (a) many countries significantly depend on China in their ICT supply chains and (b) China plays an increasingly dominant role in technology standardization and patents, (c) the Chinese government strongly encourages the substitution of foreign ICT with national equipment.[49] A strategic move to become more independent from foreign ICT suppliers. In the future the Chinese government wants to avoid a recurrence of what happened to ZTE in 2018: The US Department of Commerce forbid American suppliers to do business with ZTE – bringing the Chinese company to the brink of bankruptcy in a matter of months.[50] Of course, this independence from foreign ICT will take a long time – since 2014 China imports more semiconductors

43 Iain Morris. 2018. "Huawei Dwarfs Ericsson, Nokia on R&D Spend in 2017". https://www.lightreading.com/artificial-intelligence-machine-learning/huawei-dwarfs-ericsson-nokia-on-randd-spend-in-2017/d/d-id/741944

44 Lee Edison and Tomothy Chau. 2017. "Telecom Services The Geopolitics of 5G and IoT". Jefferies Franchise Note. http://www.jefferies.com/OurFirm/2/1307

45 Nicolas Botton and Hosuk Lee-Makiyama. 2018. "5G and National Security: After Australia's Telecom Sector Security Review." https://ecipe.org/publications/5g-national-security-australias-telecom-sector/

46 Shunsuke Tabeta. 2018. "China's alternative to GPS starts global service ahead of schedule". https://asia.nikkei.com/Business/China-tech/China-s-alternative-to-GPS-starts-global-service-ahead-of-schedule

47 Yuki Okoshi. 2019. "China's research papers lead the world in cutting-edge tech". https://asia.nikkei.com/Business/China-tech/China-s-research-papers-lead-the-world-in-cutting-edge-tech

48 U.S. Department of Defense. 2018. "Assessment on U.S. Defense Implications of China's Expanding Global Access." https://media.defense.gov/2019/Jan/14/2002079292/-1/-1/1/EXPANDING-GLOBAL-ACCESS-REPORT-FINAL.PDF

49 Samm Sacks and Manyi Kathy Li. 2018. "How Chinese Cybersecurity Standards Impact Doing Business in China." https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

50 Claire Ballentine. 2018. "U.S. Lifts Ban That Kept ZTE From Doing Business With American Suppliers". https://nyti.ms/2mf9toP

than crude oil.[51] And compared to the US, Taiwan or South Korea China's semiconductor industry is still not competitive.[52] Yet the Chinese government identified ICT as a crucial sector for economic prosperity and invests heavily in semiconductor projects.[53]

These three trends – dependency on China in ICT supply chains, China's push toward standardization and patents while becoming less dependent on foreign ICT – are the reasons 5G and the debate about whether to ban Huawei and ZTE is not unique and will happen more often in a variety of ICT sectors in the future: Alibaba's AI and quantum computers[54] or smart city solutions from Huawei[55], to name just a few. No matter how governments decide on 5G and Chinese manufacturers, similar questions will soon surface in other industries.

Section 4 – Securing the network

The previous sections demonstrated that the current debate about Huawei and national security has to be seen in the context of larger dynamics regarding the complexity of ICT systems, the fight against Chinese industrial espionage and China's push toward standardization and technological independence. Against this background, this section will discuss different ways to strengthen the resilience and trustworthiness in Europe's current and future mobile networks – beside banning certain manufacturers.

Just like one cannot prove the absence of malicious code, one cannot rule out the possibility that the Chinese government would exploit such a vulnerability – in any manufacturer's equipment. So how much easier is it for the Chinese government to either pressure Huawei or ZTE into surrendering data or exploit their legitimate access to customer networks? Such a risk could be minimized on different levels because the security of a mobile network

51 Cheng Ting-Fang. 2018. "China's upstart chip companies aim to topple Samsung, Intel and TSMC". https://asia.nikkei.com/Spotlight/Cover-Story/China-s-upstart-chip-companies-aim-to-topple-Samsung-Intel-and-TSMC

52 Edward White. 2019. "China's ability to make computer chips still 'years behind' industry leaders". https://www.ft.com/content/a002a9e4-1a42-11e9-b93e-f4351a53f1c3

53 Cheng Ting-Fang, et al. 2018. "Exclusive: Foxconn plans $9bn China chip project amid trade war". https://asia.nikkei.com/Business/China-tech/Exclusive-Foxconn-plans-9bn-China-chip-project-amid-trade-war

54 Yiting Sun. 2018. "Why Alibaba is betting big on AI chips and quantum computing". https://www.technologyreview.com/s/612190/why-alibaba-is-investing-in-ai-chips-and-quantum-computing/

55 Matt Schrader. 2018. "Huawei's Smart Cities and CCP Influence, At Home and Abroad". https://jamestown.org/program/huaweis-smart-cities-and-ccp-influence-at-home-and-abroad/

depends on the interplay between *standards, implementation, configuration* and *operations*:

- The security and robustness of 5G standards (3GPP)
- How the manufacturer implements those standards in their network equipment
- Operator specific configuration of this network equipment
- Operational practices and procedures between mobile operator and manufacturer

The current public debate focused a lot on the first two layers – standards and implementation – and payed little attention to the fact that many European operators deployed Chinese equipment successfully for more than 15 years. Thus, before thinking about banning manufacturers and severely limiting competition, governments should double-check the possibilities of risk minimization at the operator's level – secure configurations of network equipment and operational practices that further limit certain risks.

The UK and their work at the Huawei Cybersecurity Evaluation Center (HCSEC) could serve as a reference: the UK National Cyber Security Center (NCSC) cooperates with Huawei and mobile network operators at the HCSEC to assess and mitigate risks and evaluate the security not just of network equipment but also their specific configuration inside an operator's network. The center has an independent oversight board that assesses and scrutinizes the cooperation with Huawei and publishes reports every year.[56] Over the years NCSC established limitations on how Huawei equipment can be deployed and operated: operators are not allowed to implement lawful interception capabilities (law enforcement) with Huawei or ZTE equipment – even though Huawei's and ZTE's switches would provide this functionality. Additionally, neither company is allowed to have direct VPN connections[57] to any mobile base station in the UK – any maintenance work has to be done through the operator. These are just two examples of limitations on Chinese equipment to minimize risk without curbing competition.

Much of the current debate is driven under the assumption that *only* the deployment of Chinese network equipment bears risks for national security, which is naive. The simple fact that the vision of 5G is to connect the entire society and economy to the Internet makes both more vulnerable: a highly interconnected industry makes risk management and the prediction of

56 HuaweiCyber Security Evaluation Center (HCSEC) Oversight Board. 2018. "Annual Report 2018". https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018

57 VPN stands for Virtual Private Network

cascading failures much harder. To support the development of trustworthy network equipment the GSMA[58] and 3GPP developed the *Network Equipment Security Assurance Scheme (NESAS)* that is being piloted at the time of writing:[59] The vendor's development processes are examined by an external auditor and network equipment is assessed and certified by independent laboratories against security requirements defined by 3GPP.[60] As mentioned before, even though these types of security assessments are unfit to prove the *absence* of malicious code, they help to increase the overall software quality in *every* manufacturer's equipment. Since the security and resilience of 5G networks will be of utmost importance it is negligent from a regulatory perspective that there are currently no mandatory IT security certification processes in place.[61] With the Cybersecurity Act[62] Europe now has a regulatory tool to establish mandatory certification schemes for mobile network equipment – GSMA's NESAS could thus be implemented as a European cybersecurity certification scheme. Furthermore, most European member states do not have in-depth requirements for the operator that address secure operation and maintenance of network equipment. Those should be developed on a national level between operators and national information security agencies. For any measures that address the secure configuration and operation of mobile networks, collaboration in ETIS could be incentivized to support knowledge-sharing among European operators.[63]

As mentioned before, none of these measures implemented alone will be enough. In synergy, however, they would significantly increase the resilience and trustworthiness of our mobile networks – and could be implemented independently from a discussion about banning Chinese manufacturers:

58 international trade body of mobile network operators: https://www.gsma.com/

59 GSMA. n.d. "Network Equipment Security Assurance Scheme". https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group/network-equipment-security-assurance-scheme

60 GSMA. 2016. "Network Equipment Security Assurance Scheme Overview Version 0.3". https://www.gsma.com/aboutus/workinggroups/wp-content/uploads/2017/03/FS.13-NESAS-Overview-Pilot-Release_0.3.pdf

61 Volker Briegleb. 2019. „Huawei-Debatte: Telekom schlägt unabhängige Überprüfung vor". https://heise.de/-4295699

62 Council of the European Union. 2018. "Cybersecurity Act". 2017/0225(COD). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_15786_2018_INIT&from=EN

63 ETIS. n.d. "Information Security Working Group". https://www.etis.org/page/Information_Security

Standards & Implementation

- Security assessment of manufacturer's development processes and product-based IT security certification (GSMA NESAS)
- Development of mandatory EU cybersecurity certification schemes for mobile network equipment under EU Cybersecurity Act (based on or complementary to GSMA NESAS)

Configuration

- Development of national requirements regarding secure configuration of mobile network equipment between operators and national information security agencies.

Processes & Operations

- Development of national requirements regarding secure operation of mobile networks (e.g. requirements for software update processes or remote maintenance)
- Continous risk analysis and mitigation between operator, manufacturer and national information security agencies[64]

Another aspect is the **transparency and organizational structure** of the manufacturer: After Kaspersky's software has been banned from public procurement in the US[65] and experienced a loss of trust in European member states, the company relocated its data storage and processing to Switzerland.[66] Such an initiative can be seen as a trust-building measure and goes much further than simply opening "security centers" to analyze source code. What foreign manufacturers can and should provide in terms of transparency of business processes and organizational restructuring to build trust, should be part of the debate. If a company is not publicly traded, has opaque organizational structures and is intransparent about its funding and decision-making, foreign governments should ask for substantial and credible assurances.[67]

Governments, operators and manufacturers need to step up their game to ensure the economy can rely on trustworthy, resilient and efficient information networks. Of course, all these measures on different levels to minimize risk can ultimately be circumvented and played. A skilled, persistent state

64 Some countries, such as UK and China, also do penetration tests or "red teaming" of mobile networks to identify vulnerabilities

65 Dustin Volz. 2017. "Trump signs into law U.S. government ban on Kaspersky Lab software". https://reut.rs/2AwDfiq

66 Kaspersky Lab. n.d. "Kaspersky Lab Relocates Data Processing To Siwtzerland". https://www.kaspersky.com/transparency-center

67 Alliott Zaagman. 2019. "Huawei's problem of being too 'Chinese'". https://supchina.com/2019/01/24/huaweis-problem-of-being-too-chinese/amp/

actor with a practically limitless budget will always be able to compromise networks and exploit assets. But so far this fact has not stopped us from deploying ICT in all sorts of national critical infrastructure – from hospitals to nuclear power plants and the power grid. The pervasiveness and ubiquity of future 5G networks in itself makes our society more vulnerable, but industry and government are used to running critical processes on vulnerable, failing, interconnected systems.[68] A more holistic risk assessment and mitigation framework that takes into account standardization, implementation, configuration and operation would go a long way toward improving the trustworthiness and resilience of our mobile networks.

Lastly, it is important to remember that 5G is simply an infrastructure that potentially enables our industry to be more innovative and efficient. But the industry has to act on and achieve that potential – which is not a given.[69] Accepting a "zero-risk argument" and banning Chinese manufacturers from the European market because any additional risk, no matter how small, is deemed to be unacceptable, would come with **substantial costs**:

- The 5G roll-out could be delayed by several years[70] and will certainly be more expensive because of reduced competition and scarcity.[71]
- A slow 5G roll-out furthermore delays the development of applications and services that run on 5G. China, but also other countries, could develop and pilot 5G applications and services more quickly to identify viable business models and use cases.[72] In the worst case scenario this would mean that European industries rely on foreign services and applications to utilize 5G.
- Potential retaliation from China if a ban is considered arbitrary – increased tariffs or hindering market access.[73]

68 Richard J. Danzig. 2014. "Surviving on a Diet of Poisoned Fruit Reducing the National Security Risks of America's Cyber Dependencies." https://www.cnas.org/publications/reports/surviving-on-a-diet-of-poisoned-fruit-reducing-the-national-security-risks-of-americas-cyber-dependencies

69 ITU Regional Seminar. 2018. "5G Implementation in Europe and CIS". https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2018/5GHungary/FINAL%20-%20Outcome%20report_web.pdf

70 Handelsblatt. 2019. „Deutsche Telekom warnt: Huawei-Ausschluss würde 5G-Einführung verzögern". https://www.handelsblatt.com/23921762.html

71 Telecomlead. 2018. "Huawei grabs 28% share in global telecom equipment market". https://www.telecomlead.com/telecom-equipment/huawei-grabs-28-share-in-global-telecom-equipment-market-87863

72 European 5G Observatory. https://5gobservatory.eu/5g-trial/major-international-5g-trials-and-pilots/

73 Samm Sacks and Manyi Kathy Li. 2018. "How Chinese Cybersecurity Standards Impact Doing Business in China." https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.

The long-term economic costs from banning two manufacturers could very well be more severe than currently anticipated. **Thus, banning a company should be based on strong and robust evidence, transparent criteria and a clear understanding of external costs.** Neither seems to be the case for the current debate about whether to (effectively) ban Huawei and ZTE from 5G roll-outs. Yes, operators, manufacturers and government agencies have to step up their game regarding risk assessment and mitigation – not just on the technical level. But it does not seem like an impossible task.

Conclusion

The current debate in Europe about whether to ban Huawei and ZTE from 5G deployment is messy, to say the least. The previous section argued that European mobile networks would benefit from a more holistic and manufacturer-agnostic risk minimization approach. It is furthermore questionable if the risk to national security increases intolerably when deploying Chinese 5G network equipment – especially compared to other fields of national critical infrastructure. Thus, the increased technological risk alone simply does not justify the intensity of the current public debate. There are legitimate supply chain risks based on technology and operational aspects but one should not conflate those with the broader debate around **China's technological dominance** or the fight against **Chinese industrial espionage**.

China has a clear and aggressive vision of their role in ICT and other high-tech sectors. The Chinese government will likely continue to utilize **industrial espionage** as a way to help their economy gain a competitive edge and Europe should call them out on that. Recently, western nations started to name and shame Chinese cyber-espionage campaigns more openly.[74] Europe should also address China's protectionist industrial policies and **forced technology transfer**.[75] The Chinese government has a very clear idea[76] how they want to cooperate with Europe – how does a European strategy for dealing with China, especially in ICT, look like?[77] These are all complex issues,

74 Chris Uhlmann and Angus Grigg. 2018. "Secret meeting led to the international effort to stop China's cyber espionage". https://www.afr.com/news/world/asia/secret-meeting-led-to-the-international-effort-to-stop-chinas-cyber-espionage-20181213-h192ky

75 Martina F. Ferracane and Hosuk Lee-Makiyama. 2017. "China's Technology Protectionism and Its Non-Negotiable Rationales." http://ecipe.org/publications/chinas-technology-protectionism/

76 XinhuaNet. 2018. "Full text of China's Policy Paper on the European Union". http://www.xinhuanet.com/english/2018-12/18/c_137681829.htm

77 Laurence Norman. 2016. "EU Response to South China Sea Ruling Blocked by Rift". https://blogs.wsj.com/brussels/2016/07/14/eu-response-to-south-china-sea-ruling-blocked-by-rift/

worthy of in-depth policy debates but they have very little to do with the trustworthiness and resilience of our future mobile networks.[78] And banning Chinese mobile network manufacturers does not improve Europe's stance on any of these issues. In fact, the contrary may be true. Limiting competition during the deployment of 5G mobile infrastructure risks that Europe's industry will consequently fall behind in the development of viable 5G applications and services, including the exploration of new business models.

The ICT sector experiences a **"re-nationalization" of the supply chain** – the conviction that ICT can only be trusted if it is produced in one's own jurisdiction. This might be understandable under certain circumstances but ICT has been highly innovative and such an economic force because companies could rely on truly global supply chains.[79] With the deployment of ICT in highly critical environments this will certainly change in the future. Thus governments should systemically analyze ICT supply chains in different sectors and technologies to identify potentially harmful dependencies. That jurisdiction impacts the trustworthiness of technology is nothing new: With export control through the Wassenaar Arrangement[80] governments accepted the fact that it matters to where technology is exported. With foreign direct investment (FDI) screening governments realized that certain types of companies and technologies should be protected from direct investments from certain foreign countries to avoid technology transfer.[81] A governmental screening of ICT manufacturers as part of supply chain risk management (SCRM) can be seen as the logical next step and countries such as the UK[82] and USA[83] already started supply chain review processes – European member states would be well advised to follow suit.

It is good that Europe woke up to the fact that China plays a key role in our ICT supply chains and that there is a need to identify and scrutinize dependen-

78 Robert Williams. 2019. "Is Huawei a Pawn in the Trade War?". https://www.foreignaffairs.com/articles/china/2019-01-30/huawei-pawn-trade-war

79 The Economist. 2018. "The Chips Are Down." Briefing, 2018. https://www.economist.com/briefing/2018/12/01/the-semiconductor-industry-and-the-power-of-globalisation

80 The Wassenaar Arrangement. n.d. https://www.wassenaar.org/

81 European Commission. 2018. "Commission welcomes agreement on foreign investment screening framework". http://europa.eu/rapid/press-release_IP-18-6467_en.htm

82 UK Department for Digital, Culture, Media & Sport. 2018. "Telecoms Supply Chain Review Terms of Reference". https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference

83 US Department of Homeland Security. 2018. "DHS and Private Sector Partners Establish Information and Communications Technology Supply Chain Risk Management Task Force". https://www.dhs.gov/news/2018/10/30/dhs-and-private-sector-partners-establish-information-and-communications-technology

cies from foreign ICT. Yet, looking at 5G mobile networks there is a lot of manufacturer-agnostic risk minimization that should and could happen rather quickly. Since similar issues will arise in other ICT sectors European member states should also invest in **strategic supply chain reviews** to assess the risk to national security in areas such as automated driving, smart energy or artificial intelligence. In some areas Chinese equipment might negatively impact our national security – in others it might not. In any case, the exclusion of foreign manufacturers should be seen as an ultima ratio.

About the Stiftung Neue Verantwortung

The Stiftung Neue Verantwortung (SNV) is an independent think tank that develops concrete ideas as to how German politics can shape technological change in society, the economy and the state. In order to guarantee the independence of its work, the organisation 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 organise 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). He analyses how standardization, certification and market surveillance can create economic incentives for IoT manufacturers to produce secure and trustworthy IoT devices. A second focus of his work is on the security of digital infrastructures, especially the 5th generation of mobile networks (5G), which will connect the Internet of Things in the future.

How to Contact the Author

Jan-Peter Kleinhans
Project Director IT-Security in the Internet of Things
jkleinhans@stiftung-nv.de
+49 (0)30 81 45 03 78 99

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/en
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de