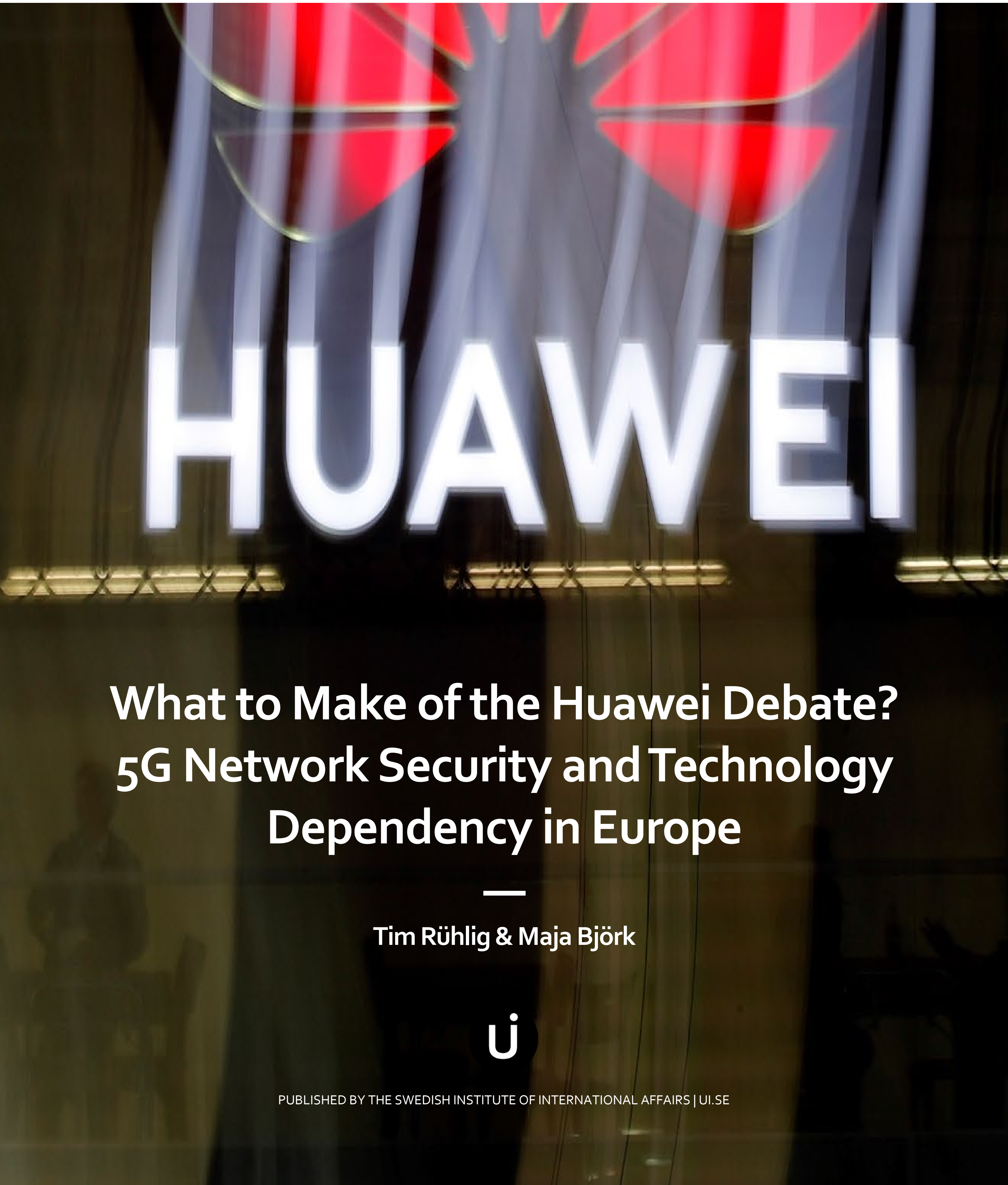
paper

1/2020



What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe

Tim Rühlig & Maja Björk

PUBLISHED BY THE SWEDISH INSTITUTE OF INTERNATIONAL AFFAIRS | UI.SE

Abstract

Europe is controversially discussing whether to ban the Chinese tech-giant Huawei from the roll-out of the new generation of mobile infrastructure, better known as 5G, not least due to conflicting pressures from the governments of the United States and the People's Republic of China. 5G is a critical infrastructure and will penetrate European society and its economy to an unprecedented extent. Proponents of a ban argue that Huawei is closely allied with the authoritarian Chinese party-state, which could utilise Huawei equipment for espionage and sabotage. The argument is that banning Huawei is a matter of increasing network security in Europe. This paper explains that while scepticism is reasonable, and the security concerns are valid, a ban on Huawei is not an effective solution for generating network security. Other technological measures – first and foremost better encryption, and redundancies coupled with vendor diversity – would be more effective, although complete network security can never be achieved. Scepticism of China's influence over Huawei is reasonable. However, the idea of banning Huawei stems, rather than from concerns over network security, from a geopolitical logic. In this context, a ban on Huawei would help decrease European technological dependency on China. The geopolitical fear is that China could leverage this dependency to extract political concessions from Europe in the future. We argue that Europe should indeed respond to this challenge but instead of striving for technological self-reliance, we discuss how the European Union could preserve access to strategic technology by means of diversification of the supply chain and underlying patents, coupled with "protectionism light". We believe this could help respond to the emerging geopolitical rivalry over high-technology such as 5G while at the same time attempting to preserve free trade as far as possible. In short, our sceptical view on the idea of banning Huawei from the roll-out of 5G in Europe does not stem from a trust in China or Chinese tech companies, but rather from the perspective that it is not the most effective response to the future challenges of 5G networks and technology dependence.

Tim Rühlig
Research Fellow
The Swedish Institute of International Affairs

Maja Björk
Analyst
The Swedish Institute of International Affairs

© 2020 The Swedish Institute of International Affairs
Language editing: Andrew Mash
Cover photo: Stefan Wermuth / AFP

Content

© 2019 The Swedish Institute of International Affairs

Introduction

The new "fifth" generation of mobile internet connectivity (5G) will unlock new and improved ways of using wireless technology and is expected to revolutionise multiple spheres of society, not least manufacturing, construction, electricity networks, transportation and health care. The new networks will support innovative technologies and enable a powerful increase in the application of artificial intelligence (AI) and the Internet of Things (IoT), while also allowing societies to become significantly more connected. The 5G mobile internet has already been tested and launched in certain locations, but is expected to launch more widely in 2020,[1] and account for around 20% of global mobile connections by 2025.[2] While 5G will not change the world overnight, its importance to society will grow over time to achieve an unprecedented level.[3]

For 5G networks to be deployed, huge investments in new digital infrastructure will be needed. The ongoing competition over 5G, however, is not solely among giant tech companies racing for market share and royalty payments. It is also turning into a geopolitical conflict among states, first and foremost the United States (US) and the People's Republic of China (PRC). China has taken an active role in technology and innovation, and Chinese technology companies have become significant players in 5G equipment and infrastructure in recent years. The most prominent supplier is the Chinese tech-giant Huawei Technologies Co., which is also one of the world's largest telecom companies.

Huawei currently finds itself at the centre of a heated international debate over 5G deployment, which has also raised serious security concerns and accusations against the company. Western intelligence services and observers have expressed concerns about Huawei's ties to the PRC as well as the company's legal obligations to cooperate with the Chinese security apparatus.[4] The main concern is that Huawei equipment could be used as an inroad for Chinese espionage, and China gaining access to data on and control over critical infrastructure. Such security concerns led the US earlier this year to place a ban on Huawei and the Chinese state-owned telecom equipment manufacturer, ZTE, preventing Huawei from participating in the country's 5G roll-out, a measure also taken by Australia and Japan.[5] Many governments have been pressured to follow suit, and a number of countries have either

[1] Matthew Wall, "What is 5G and What Will It Mean for You?," *BBC*, July 24, 2018, at: https://www.bbc.com/news/business-44871448. John McCann and Mike Moore, "5G: Everything You Need to Know," *Rechradar*, August 20, 2019, at: https://www.techradar.com/news/what-is-5g-everything-you-need-to-know.

[2] David Bond and James Kynge, "China Spying Risk Hits Huawei's UK Ambitions," *Financial Times*, 3 December 2018.

[3] Steve Lo and Kevin Lee, *China Is Poised to Win the 5G Race*, Hong Kong: EY, 2018.

[4] RWR Advisory Group, *Assessing Huawei Risk: How the Track Record of the CCP Should Play into the Due Diligence of Huawei's Partners and Customers*, Washington DC: RWR Advisory Group, 2019. Christopher Ashley Ford, "Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications," *Remarks at the Multilateral Action on Sensitive Technologies (MAST) Conference, 11 September 2019*, Washington DC: US State Department, 2019. Tom Uren, "Weighing the Risks in Building a 5G Network," *ASPI The Strategist*, Barton: ASPI, 2019.

[5] Li Tao, "Japan Latest Country to Exclude Huawei, ZTE From 5G Roll-out Over Security Concerns," *South China Morning Post*, December 10, 2018, at: https://www.scmp.com/tech/tech-leaders-and-founders/article/2177194/japan-decides-exclude-huawei-zte-government.

implemented or are currently considering various forms of restrictions on Huawei's access to domestic markets for 5G infrastructure. Not only New Zealand, Canada and India, but also member states of the European Union (EU), namely Denmark, the Czech Republic and Poland consider taking a similar approach.[6] Estonia,[7] Poland[8] and Romania[9] have signed documents with the US voicing scepticism about Chinese 5G vendors, while Germany and the United Kingdom (UK) among others remain more hesitant toward such a decision. While EU member states have initially adopted different responses, moves are now under way to coordinate an EU-wide approach. The first step has been a coordinated risk assessment and a joint communication from the Council of the European Union, and recommendations to all member states will follow.[10]

Europe finds itself in a difficult situation, positioned between the US and China, and facing pressure from both sides. European states are in a close security alliance with the US, which includes comprehensive intelligence cooperation. China, on the other hand, is emerging as the technological leader in 5G and many European telecommunication operators already cooperate with Huawei. Outside of China, Europe is the region in which Huawei has grown its market position the most in recent years.[11] Pressure from western allies combined with the authoritarian nature of the Chinese party-state give many Europeans a sense of unease over cooperating with Huawei, while European governments are under increasing pressure to decide their position.

This UI Paper engages with the debate about whether to ban Huawei from the roll-out of 5G in Europe. We take a sceptical view of such a ban, even though we believe that the concerns regarding Chinese party-state control over Huawei are valid, and that the security concerns raised are genuine and need to be addressed We do not follow the mainstream argument put forward by critics of a ban that the use of Huawei technology is essential to avoid losing ground in the development and roll-out of 5G. If banning Huawei was an effective means of containing the security risks, it would be worth paying an economic price for it. The problem with a ban on Huawei, however, is that it does not offer an effective solution to the security challenges. China would be able to shut down 5G networks regardless of whether Huawei

[6] Andreas Kluth, "Huawei Is a Paralyzing Dilemma for the West," *Bloomberg*, November 23, 2019, at: https://www.bloomberg.com/opinion/articles/2019-11-23/huawei-s-5g-networks-are-a-paralyzing-dilemma-for-the-west.

[7] White House, *United States – Estonia Joint Declaration on 5G Security*, November 1, 2019, at: https://www.whitehouse.gov/briefings-statements/united-states-estonia-joint-declaration-5g-security/.

[8] White House, "US-Poland Joint Declaration on 5G," *The White House*, September 5, 2019, at: https://www.whitehouse.gov/briefings-statements/u-s-poland-joint-declaration-5g/.

[9] White House, *Joint Statement from president of the United States Donald J. Trump and President of Romania Klaus Iohannis*, August 20, 2019, at: https://www.whitehouse.gov/briefings-statements/joint-statement-president-united-states-donald-j-trump-president-romania-klaus-iohannis/.

[10] NIS Cooperation Group, *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*, October 9, 2019, Brussels: European Commission. Council of the European Union, *Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G. Council Conclusions, 14519/19*, December 3, 2019. Brussels: Council of the European Union.

[11] Worldwide Asset Management, *The New Tech War and the Geopolitics of 5G*, 2019, at: https://cworldwide.com/media/PDF/WP_2019_The_New_Tech_War_and_the_Geopolitics_of_5G.pdf.

© 2020 The Swedish Institute of International Affairs

technology were included in the build-up of European infrastructure. Similarly, a ban on Huawei would not be an effective measure for significantly reducing Chinese espionage, which is mainly carried out through applications and phishing rather than infrastructure. Even where infrastructure is necessary for espionage, there is little reason to believe that China needs Huawei equipment for its operations. Banning Huawei would instead increase political tensions and contribute to a technological divide between a western and a Chinese sphere, ultimately fuelling the existing rivalry and fears of a major confrontation between the PRC and the US. Most importantly, however, there are other more effective means of containing the security risks than banning Huawei. Instead, banning Chinese companies from, or limiting their access to, Europe's build-out of 5G adheres more to a geopolitical logic, by addressing politically motivated issues and trust. A ban on Huawei would aim to weaken China's political and technological influence in the world rather than effectively addressing network security risks. We believe instead that reducing European technology dependency on Chinese vendors should be the policy goal of the EU. This ties in with ongoing European discussions on European strategic autonomy and European sovereignty. We are sympathetic to this approach but believe that the debate should not fully focus on strengthening the digital industrial base of Europe, since this tends to put the focus on protectionism rather than the preservation of global cooperation. We therefore discuss a different take on reducing dependency on Chinese and US technology: the question of how Europe can secure access to strategically important technology by means of diversification and "protectionism light".

To unfold this line of argument, we first summarise the central innovations and revolutionary potential of 5G, before turning to the current debate over 5G network security and what measures would best address the main security concerns. We then turn to the underlying geopolitical logic of a Huawei ban and its potential consequences. Finally, we address the European position and recommended response before concluding with a brief summary.

Centrality and innovation of 5G

While previous generations of wireless technology – from 1G to 4G – have brought improvements and new capabilities to cellular communications, the shift to 5G is predicted to be the most significant since the invention of the mobile phone.[12] The fifth generation of mobile technology will not only bring changes for consumers but also transform entire industries in a way not previously possible.[13] This also means that society will become increasingly dependent on mobile networks and rely on them for some of its most critical functions, including services such as autonomous vehicles, health care monitoring and remote medical surgery, as well as emergency service response. As a consequence, society will become more vulnerable to attacks on, and the malfunction of, its 5G networks, and the damage potential of such incidents could be catastrophic as connectedness and dependence increase.

[12] Miriam Tuerk, "How 5G Networks Will Change America," *Forbes*, February 27, 2019, at: https://www.forbes.com/sites/miriamtuerk/2019/02/27/how-5g-networks-will-change-america/#4466acae11b5.

[13] Edison Lee and Timothy Chau, "Telecom Services. The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, Hong Kong: Jefferies, 2017.

The shift from 4G to 5G will also be more complicated than past mobile communications revolutions, as the intentions of 5G go beyond previous goals which were focused mainly on increasing data speeds and serving the needs of mobile handsets. Instead of just focusing on person-to-person or person-to-device communications, 5G will also support machine-to-machine networking. This makes 5G entirely different from previous technology. 5G technology is expected to deliver three significant new capabilities:

1) *Enhanced mobile broadband* (eMBB): higher data service speeds, managing more traffic and more demanding services (e.g. faster download and upload speeds, as well as virtual and augmented reality (VR/AR)).

2) *Ultra-reliable and low latency communications* (URLLC): with response times as low as one millisecond, enabling close to real-time services (e.g. remote medical surgery, self-driving cars and industry automation).

3) *Massive machine-type communications* (mMTC): connection for a very large number of devices (enabling e.g. the Internet of Things, smart cities and automated agricultural processes).[14]

In Europe, the introduction of 5G technology will take place first as non-standalone (NSA) 5G, which will use existing 4G infrastructure and mainly provide higher data speeds, to eventually be followed by standalone (SA) 5G, which will require an entirely new network architecture.[15] A cellular mobile network functions essentially through the connections between mobile devices, through a Radio Access Network (RAN) that consists mainly of base stations (such as antenna towers) and a core network. Standalone 5G technology will bring changes to both base stations and the core network, and make the distinction between their functions less clear.[16] One of the most important changes with the shift to standalone 5G is its new virtualised core technology. By replacing the previous core network (Evolved packet core), which relies mainly on physical network elements, 5G will introduce a virtualised core designed for software-based infrastructure running on standard servers.[17] This will enable features such as Network Function Virtualisation (NFV) and network slicing.[18] While cloud computing is not new in itself, these features enable new aspects of cloud use that extend beyond storage to include communication and remote real-time services. In other words, software and cloud functions are essential to the new 5G technology and will therefore become increasingly important with the development of 5G networks.

NFV allows network functions that have traditionally run on function-specific

[14] Christian de Looper, What is 5G?, *Digital Trends*, November 18, 2019, at: https://www.digitaltrends.com/mobile/what-is-5g/.

[15] Edison Lee and Timothy Chau, "Telecom Services. The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, Hong Kong: Jefferies, 2017.

[16] Jan-Peter Kleinhans, *Whom to Trust in a 5G World. Policy Recommendations for Europe's 5G Challenge*, Berlin: Stiftung Neue Verantwortung, 2019, pp. 7-8.

[17] Iwan Price-Evans, "Introducing the 5G Core Network Functions,"*Metaswitch*, February 7, 2019, at: https://www.metaswitch.com/blog/introducing-the-5g-core-network-functions.

[18] Stephane Teral, *IHS Markit Technology White Paper: 5G Best Choice Architecture*, London, IHS Markit, 2019.

hardware to be replaced by virtual servers, which essentially share one physical server and can be available at any location. NFV technology concentrates these functions in centralised data centres.[19] This technology also enables network slicing, which entails subdividing different flows of data traffic in the network for different services, to ensure that each network slice makes use of the kind of connectivity it requires. For example, the communication necessary for self-driving cars might be different from, and more latency-sensitive than, other services within the network.[20] Some of the expected use cases of 5G mobile technology also create the need for so-called edge computing, which reduces latency and improves data speeds by enabling data processing closer to the end-users, presenting – in this sense – a less centralised architecture.[21]

Network security concerns: the current debate

Given the importance and potential of 5G technology, there is much to be gained from achieving leadership in its development. China holds a very strong position in the global value chains of Information and Communications Technology (ICT) equipment, and Huawei has, not least with the help of the Chinese state authorities, become the leading supplier of 5G equipment and infrastructure.[22] Huawei has also become the focus of the ongoing debate around 5G deployment that results from a number of security concerns raised over the company's ties to the Chinese government. While all global Chinese firms are subject to some level of party-state control,[23] Huawei is thought to have particularly strong ties to the PRC security apparatus.[24] Reports suggest the existence of a high degree of personal overlap between China's security apparatus and the company. There have long been concerns over the background of the company's founder, Ren Zhengfei, as a former Director of General Staff of the People's Liberation Army (PLA). Ren's daughter and Huawei's Chief Financial Officer, Meng Wanzhou, held a "Public Affairs" passport (i.e. a diplomatic passport) for many years.[25] A much-debated article studying the CVs of Huawei employees, published earlier in 2019, similarly suggests close ties between Huawei personnel and the party-state's security apparatus.[26]

[19] Yuri Gittik, "Distributed Network Functions Virtualization. An Introduction to D-NFV," *RAD White Paper*, March 2014, at: http://crezer.net/Newsletter/archivos/Distributed-NFV-White-Paper.pdf.

[20] EMF Explained Series, *5G Explained – How 5G Works*, without year, at: http://www.emfexplained.info/?ID=25916.

[21] Robert Gibb, "What is Edge Computing?" *Stackpath*, June 18, 2019, at: https://blog.stackpath.com/edge-computing/. Kris Beevers, "Why 5G is Bringing Edge Computing Automation Front and Center," *Network World*, February 14, 2018, at: https://www.networkworld.com/article/3255426/why-5g-is-bringing-edge-computing-and-automation-front-and-center.html.

[22] David Bond and James Kynge, "China Spying Risk Hits Huawei's UK Ambitions," *Financial Times*, 3 December 2018.

[23] Mark Wu, "The "China, Inc." Challenge to Global Trade Governance," *Harvard International Law Journal* 57: 2, pp. 261-324, 2016.

[24] Douglas Black, "Huawei and China. Not Just Business as Usual," *Journal of Political Risk* 8:1, 2019.

[25] Ashley Feng, "We Can't Tell if Chinese Firms Work for the Party," *Foreign Policy*, February 7, 2019, at: https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/.

[26] Christopher Balding, "Huawei Technologies' Links to Chinese State Security Services," *SSRN*, July 9, 2019, at:

Huawei, along with other Chinese tech-giants, not only facilitates the build-out of surveillance systems within China, but also exports these technologies to third countries facilitating what has been called "digital authoritarianism".[27] Chinese engagement in the development of international technical standards of facial recognition technology is only one of the most recent subjects of western concern regarding the spread of digital authoritarianism.[28] There can be little doubt that Huawei is more than just a normal company and plays a strategic role in the policy of the PRC.[29] More recent concern, however, has focused on various pieces of Chinese legislation, in particular China's Cyber Security Law of 2017, which legally requires Chinese companies to turn over information and comply with China's intelligence and security services, essentially on all matters, – not just domestically (article 14) but also internationally (article 10).[30] This concern becomes especially significant with regard to Huawei, given the company's strong position in the 5G equipment market.

Huawei's ownership structure is not transparent, raising suspicions of effective party-state control over the company.[31] Moreover, of Huawei's 160,000 employees, 12,000 are party members, and they form no fewer than 300 party cells within the company. Furthermore, Huawei receives preferential treatment, not least by means of soft loans which already amounted to more than US $30 billion before 2011, mostly from the state-controlled China Development Bank (CDB). In the period 2012–2018, CDB and another state-controlled bank, the China Import Export Bank, granted the company at least another US $9.8 billion for overseas projects.[32] Strikingly, however, Huawei is not that different from any other Chinese company. In fact, even the subsidiaries and joint ventures of non-Chinese tech companies, such as Ericsson and Nokia, face Chinese Communist Party (CCP) control not least by means of party cells and the need to comply with domestic Chinese laws – including the Intelligence Law of 2017.[33]

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726.

[27] Danielle Cave et al., "Mapping China's Technology Giants," *ASPI Issues Paper Report* 1/2019, Barton: ASPI.

[28] Georgina Torbet, "Chinese Companies Want to help Shape Global Facial Recognition Standards," *Engadget*, December 2, 2019, at: https://www.engadget.com/2019/12/02/china-facial-recognition-standards/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKcP2n-viXPHG8Lg5mkOjmdZu8gmP9WLUrOWrFcjGHpxN-yxHCjDcTZSfaFTBeohbvNR4w3_oo4FaKswdCGYj8tBBq30GZyrjCEYY-OuAKozXYYjm1IzV9_tm36fHDrg12n6OsuLVllKqNYXAi37gDPBTQTycuU-lbLPX4jZv8cc.

[29] Rick Umback, "Huawei and Telefunken: Communications Enterprises and Rising Power Strategies," *ASPI Strategic Insights* 135. Barton: ASPI, 2019.

[30] Huawei has denied this interpretation of the Cybersecurity law, but experts are not convinced. Jichang Lulu, "Synopsis: Huawei's Lawfare by Proxy," *China Digital Times*, February 2019, at: https://chinadigitaltimes.net/2019/02/sinopsis-huaweis-lawfare-by-proxy.

[31] Christopher Balding and Donald Clarke: "Who Owns Huawei?," *SSRN*, May 8, 2019, at: https://ssrn.com/abstract=3372669/.

[32] Mathieu Duchâtel and Francois Godement, *Europe and 5G: The Huawei Case*, Paris: Institut Montaigne, 2019. Bob Seely et al., *Defending Our Data: Huawei, 5G and the Five Eyes*, London: Henry Jackson Society, 2019.

[33] Richard Baker, "Top 5G Suppliers Linked to China's Communist Party," *Sydney Morning Herald*, August 13, 2018, at: https://www.smh.com.au/business/companies/top-5g-suppliers-linked-to-china-s-communist-party-20180812-p4zwzt.html.

There is indeed reason not to trust PRC authorities and Chinese vendors. Huawei has an opaque governance structure,[34] has been accused of multiple intellectual property thefts and of ignoring international sanctions against authoritarian states,[35] does not issue financial statements since it is not a publicly listed company,[36] and shows significant software engineering and cyber security problems.[37] Not least the example of the Chinese company Lenovo demonstrates that even in the authoritarian PRC, corporates can do more to reassure their international customers.[38] Most Chinese companies, however, have done little to increase transparency over its organisational structure[39] and the party-state has failed to reassure international partners of its legal framework, first and foremost the Intelligence Law.[40] Hence, the Council of the European Union states in a communication that "also non-technical factors such as the legal and policy framework to which suppliers may be subject to in third countries, should be considered."[41]

In addition, while there have also been cases of US espionage in Europe, significant differences remain between the US and China. After the Snowden revelations, US companies signed public letters advocating surveillance law reform, filed lawsuits for more transparency, and brought cases against breaking encryption of digital communication to court; which has led to changes in US policy.[42] It is unrealistic to think that a company like Huawei or ZTE

[34] Colin Hawes and Grace Li, "Transparency and Opaqueness in the Chinese ICT Sector. A Critique of Chinese and International Corporate Governance Norms," *Asian Journal of Comparative Law* 12: 1, 2017, pp. 41-80. Christopher Balding and Donald Clarke: "Who Owns Huawei?," *SSRN*, May 8, 2019, at: https://ssrn.com/abstract=3372669/.

[35] RWR Advisory Group, *Huawei Risk Tracker*, 2019, at: https://huawei.rwradvisory.com/.

[36] Andrew Foster and Nicholas Borst, "Time Is Ripe for Huawei to Launch an IPO, to Address Political and Security Concerns Once and for All," *South China Morning Post*, May 27, 2019, at: https://www.scmp.com/comment/insight-opinion/article/3011510/time-ripe-huawei-launch-ipo-address-political-and-security.

[37] Huawei Cyber Security Evaluation Centre Oversight Board, *Annual Report: A Report to the National Security Adviser of the United Kingdom*, March 2019, at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

[38] Alliott Zaagman, *Thinking About Working For a Chinese Company? First, Find Out If It's a "Lenovo" or A "Huawei"*, October 9, 2017, at: https://supchina.com/2017/10/09/thinking-working-chinese-company-first-find-lenovo-huawei/.

[39] The Russian tech company Kaspersky, in contrast, has moved storage and processing of its data to Switzerland, a measure that is far more reassuring than the cybersecurity centres opened by Huawei. Kaspersky Lab, *Kaspersky Lab Starts Data Processing for European Users in Zurich and also Opens First Transparency Center*, November 13, 2018, at: https://www.kaspersky.com/about/press-releases/2018_kaspersky-lab-starts-data-processing-for-european-users-in-zurich-and-also-opens-first-transparency-center. Alliott Zaagman, *Huawei's Problem of Being too "Chinese"*, January 24, 2019, at: https://supchina.com/2019/01/24/huaweis-problem-of-being-too-chinese/.

[40] Donald Clarke, "The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law," *SSRN*, March 28, 2019, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354211

[41] Council of the European Union, *Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G. Council Conclusions, 14519/19*, December 3, 2019. Brussels: Council of the European Union, p. 4.

[42] Jan-Peter Kleinhans, *Whom to Trust in a 5G World. Policy Recommendations for Europe's 5G*

would bring cases about government surveillance practices to Chinese courts, and even if they did they would face a judiciary subordinate to CCP rule.

These concerns have led to discussions across many western states about whether Huawei should be excluded from the build-out of 5G infrastructure. The US and Australia in particular favour a ban, and the US has been pressuring European and other states to fall in line, warning about future European-US security cooperation.[43]

Focus on espionage and sabotage

While concerns have been raised over various risks, including privacy issues and dual-use technology, the overwhelming focus has been on the risks of espionage and sabotage. The fear is that 5G equipment from Chinese vendors would allow the Chinese government to control critical domestic infrastructure and to gain access to the information that travels on it.

In discussions about the risk of sabotage, the main – and probably the most crucial – concern is about the ability to shut down networks – a scenario often referred to as a "kill-switch". Western observers fear that a large-scale deployment of Huawei network equipment would provide such a kill switch and make it easier for China to shut down 5G infrastructure. While it is unlikely that China would shut down an entire 5G network and risk irreparable damage to Huawei's reputation in times of peace, such a switch could be used for partial shutdowns, accompanied by coercive threats, or used in the event of an interstate war.

Commentators and policymakers in the west also fear that Huawei's 5G equipment could come with backdoors that would allow undetected Chinese access and enable economic and political espionage. There are similar concerns that the company might simply hand over sensitive information to the Chinese government, especially in the light of the Chinese cybersecurity laws. China has a worrying track record of espionage in general and cyber theft in particular.[44] There have been allegations of backdoors, espionage and technology theft against the company.[45] Thus far, however, no "smoking gun" has been discovered to confirm these,[46] but

Challenge, Berlin: Stiftung Neue Verantwortung, 2019, p. 16.

[43] Nikos Chrysoloras and Richard Bravo, "Huawei Deals for Tech Will Have Consequences, US Warns EU," *Bloomberg*, February 7, 2019, at: https://www.bloomberg.com/news/articles/2019-02-07/huawei-deals-for-tech-willhave-consequences-u-s-warns-eu. Paul Triolo, et al., "One Company, Many Systems. US Forces Governments to Choose Sides on Huawei," *Special Report Prepared by Eurasia Group*, Washington DC, Eurasia Group, 2019.

[44] Kadri Kaska et al., *Huawei, 5G and China as a Security Threat*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2019, pp. 10-11. US Department of Justice, *Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers*, December 20, 2018, at: https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers.

[45] For example, Vodafone allegedly found backdoors in Huawei equipment they used in Italy in 2011 and 2012; Huawei was found liable for stealing robotic technology in a US court in 2017; and in early 2019 a Huawei employee was arrested in Poland on grounds of suspected espionage. See: Bloomberg News, How Huawei Became a Target for Governments, *Bloomberg*, January 23, 2019, at: https://www.bloomberg.com/news/articles/2019-01-23/how-huawei-became-a-u-s-government-target-quicktake.

[46] Ole Moehr, My Way or the Huawei: 5G at the Center of US-China Strategic Competition, *The Atlantic Council*, July 23, 2019, at: https://www.atlanticcouncil.org/blogs/econographics/my-way-or-the-huawei-5g-at-the-center-of-us-china-strategic-competition.

© 2020 The Swedish Institute of International Affairs

nobody can rule out the possibility of the Chinese government exploiting technical vulnerabilities – in any manufacturer's equipment.[47] However, experts have also pointed out that mobile internet infrastructure has not been the main focus of Chinese espionage, and that spear-phishing and social engineering are more efficient for such purposes.[48]

Assessments made by the United Kingdom's Huawei Cyber Security Evaluation Centre (HCSEC) suggest that Huawei's equipment comes with serious weaknesses, a problem irrelevant to the origin of the vendor that indicates that access could easily be obtained even without built-in backdoors. In addition, British experts at the HCSEC make clear that no certification can rule out the existence of backdoors and malicious code.[49] Since hackers normally focus on tracking weaknesses in the equipment of competitors, non-Huawei equipment would also be a more likely target for Chinese espionage.[50] The Chinese government decided in 2018 to prevent Chinese hackers from participating in international hacking contests, which Chinese teams have often dominated, allegedly for national security reasons.

While it remains unclear whether 5G will be *more* or *less* secure than 4G networks, 5G technology will bring new challenges, mainly through its technological innovations and the increase in network dependency throughout society. New forms of technological security risk arise primarily from the increased use of virtualisation and of centralised software. The software focus, as well as the transferring of functions from the core network to edge computing, create larger attack surfaces and greater opportunities to introduce vulnerabilities, which, in turn, enables methods to access and control data on the network.[51] In addition, as virtual servers replace specialised hardware, different parts of the network technology will no longer be physically isolated from each other, which means that if one vulnerability is found, it could potentially be exploited to access other parts of the network. In other words, it could make the damage much more dramatic if a vulnerability is found and exploited.[52]

Security concerns also arise from the use of network slicing, which entails separating flows of data on a network, and creating slices that can be used for different services by tailoring their use of functions to the requirements of each service. Ensuring that each network slice is secure will be a challenge, and there are potential risks that vulnerabilities in one slice could be used to access traffic on other slices.[53] There are

[47] Jan-Peter Kleinhans, *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung, 2019.
[48] Jan-Peter Kleinhans, *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung, 2019.
[49] Huawei Cyber Security Evaluation Centre Oversight Board, *Annual Report: A Report to the National Security Adviser of the United Kingdom*, March 2019, at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.
[50] Author interview with an anonymous engineer, Berlin, May 2019.
[51] Christopher Ashley Ford, "Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications," *Remarks at the Multilateral Action on Sensitive Technologies (MAST) Conference, 11 September 2019*, Washington DC: US State Department, 2019.
[52] Author interview with Pontus Johnson, professor in cyber security at KTH, Stockholm, June 2019.
[53] NIS Cooperation Group, *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*,

also concerns that targeted attacks on specific slices could be motivated if what each slice is used for becomes known.[54]

Security risks also arise from the existence of large numbers of connected devices. Another form of sabotage that 5G technology is likely to facilitate, by enabling massive machine communication and IoT, is distributed denial-of-service (DDoS) attacks. Such attacks are carried out by finding and hacking machines with weak security and using them to overwhelm a website or machine with more traffic than it can handle. With the development of IoT, the number of internet-connected devices is expected to grow from 14.2 billion to 25 billion by 2021, which increases the potential for and power of DDoS attacks.[55] This essentially means that DDoS attacks can be used to shut down parts of the internet, which could be very serious for 5G networks given the importance and scale of the services that it is planned to support.

In a nutshell, the specific vulnerabilities of 5G networks lie mainly in the *complexity* of 5G infrastructure resulting from technological innovation (discussed above) and the multitude of use cases penetrating future societies. It is the centrality of 5G to the economies and societies of the future that makes this issue such a crucial one. In addition to the services that will be enabled by 5G technology, increasing amounts of personal and sensitive data will be processed on the networks, which could be exploited if accessed.[56]

Would banning Huawei solve the problem?

The risks of sabotage and espionage are genuine and valid concerns and should be addressed and mitigated as best as possible. However, banning Huawei from the roll-out of 5G networks would not effectively address or remedy these concerns. Excluding Chinese companies such as Huawei from providing 5G infrastructure in Europe might make it somewhat more difficult for the Chinese authorities to access and exploit European networks. However, a ban would only marginally address the network security risks of Chinese sabotage and espionage. Experts argue that if China were interested in accessing a network for whatever reason, it would have the capacity to do so with or without the help of Huawei equipment. Already today, China carries out extensive espionage for economic, political and military purposes. APT 1, APT 3 and APT 10 are the most famous hacker groups attributed to the Chinese party-state.[57]

October 9, 2019, Brussels: European Commission.

[54] Michael Heller, "Nokia: 5G Network Slicing Could Be a Boon For Security," *Techtarget*, April 10, 2019, at: https://searchsecurity.techtarget.com/news/252461410/Nokia-5G-network-slicing-could-be-a-boon-for-security.

[55] Nick Huber, "A Hacker's Paradise? 5G and Cyber Security," *Financial Times*, October 14, 2019, at: https://www.ft.com/content/74edc076-ca6f-11e9-af46-b09e8bfe60c0.

[56] Matthew Kassel, "As 5G Technology Expands, So Do Concerns over Privacy," *Wall Street Journal*, February 26, 2019, at: https://www.wsj.com/articles/as-5g-technology-expands-so-do-concerns-over-privacy-11551236460.

[57] PwC, "Operation Cloud Hopper," *PwC*, 2018, at: https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf. Brian Barrett, "How China's Elite hackers Stole the World's Most Valuable Secrets," *Wired*, December 20, 2018, at: https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/. FireEye, *Mandiant APT1. Exposing One of China's Cyber Espionage Unites*, February 19, 2013, at: https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html. Thomas Brewster, "Chinese Trio Linked to Dangerous APT3 hackers Charged with Stealing 407GB of

© 2020 The Swedish Institute of International Affairs

However, the main attack vectors are spear-phishing and social engineering, not using mobile communication infrastructure or hacking into base stations. In other words, regardless of a ban on Huawei, measures will be needed to strengthen the security of future 5G networks against third party access and disruption.[58] In addition, a ban would risk generating other costs and have further implications – both economic and political. Decisions about how to manage risks related to sabotage and espionage should avoid being locked into a logic that focuses entirely on the fear and presence of risk without considering other aspects of the situation, such as the potential damage linked to the risks, costs and consequences of a ban.[59]

We do not adhere to the popular argument promoted by critics of a Huawei ban that focuses on the economic costs and competitive disadvantages that would be caused by the resulting delay in 5G roll-out, or other negative impacts on western competitiveness not least stemming from Chinese retaliation.[60] Another argument suggests that the debate over excluding Huawei from 5G participation is merely part of the current trade dispute between China and the US. Such arguments might be true, but this is also not what we are saying. The risks of espionage and sabotage are valid concerns. We are rather addressing the compatibility of issue and response and suggest that there are more effective and appropriate means available to address the network security concerns at the centre of the 5G debate than to ban Huawei from

Data from Siemens," *Forbes*, November 27, 2017, at: https://www.forbes.com/sites/thomasbrewster/2017/11/27/chinese-hackers-accused-of-siemens-moodys-trimble-hacks/.

[58] Author interviews (including telephone and Skype interviews) with hackers, engeneers, and technical experts in several European cities, February-October 2019. The German IT expert Jan-Peter Kleinhans exemplarily summarizes: "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. [...] A skilled, persistent state actor with a practically limitless budget will always be able to compromise networks and exploit assets." Jan-Peter Kleinhans, *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung, 2019, p. 9, 16.

[59] Jeffrey D. Sachs makes a comparison of the United States' policy on Huawei and the US decision to invade Iraq, and argues that the same tactic is being used. He refers to it as ‚the Chaney Doctrine' and involves the use of fear over small risks to motivate drastic and ultimately misguided action. See Jeffrey D. Sachs, "America's War on Chinese Technology," *Project Syndicate*, November 7, 2019, at: https://www.project-syndicate.org/commentary/cheney-doctrine-us-war-on-chinese-technology-by-jeffrey-d-sachs-2019-11.

[60] Handelsblatt, "Deutsche Telekom warnt. Huawei-Ausschluss würde 5G-Einführung verzögern," *Handelsblatt*, January 29, 2019, https://www.handelsblatt.com/unternehmen/it-medien/neuer-mobilfunkstandard-deutsche-telekom-warnt-huawei-ausschluss-wuerde-5g-einfuehrung-verzoegern/23921762.html?ticket=ST-38734491-9lY7UMOoLFLoPSMFVweD-ap5. Telecomlead, *Huawei Grabs 28% Share in Global Telecom Equipment Market*, December 7, 2018, at: https://www.telecomlead.com/telecom-equipment/huawei-grabs-28-share-in-global-telecom-equipment-market-87863. Andreas Kluth, "Huawei Is a Paralyzing Dilemma for the West," *Bloomberg*, November 23, 2019, at: https://www.bloomberg.com/opinion/articles/2019-11-23/huawei-s-5g-networks-are-a-paralyzing-dilemma-for-the-west. Jodi Xu Klein, "The Huawei Dilemma. Washington Still Stuck Trying to Balance National Security Against US Tech Spremacy," *South China Morning Post*, November 1, 2019, at: https://www.scmp.com/news/china/article/3035832/huawei-dilemma-washington-still-stuck-trying-balance-national-security-against.

European 5G mobile infrastructure. In addition, excluding Huawei from European markets would not change the fact that non-Chinese companies, such as Ericsson and Nokia, will continue to face the same challenges and legal environment as Huawei in any production or business they have located in China.
Responding to recent developments, in September 2019, Huawei founder Ren Zhengfei offered to sell access to the company's 5G code, patents, licences, technical blueprints and production expertise to a foreign company in return for a one-off fee. However, this offer is irrelevant as long as there is no buyer. Ericsson and Nokia have no technological need to purchase Huawei's source code, and US companies have no interest, not least due to the lack of political will. Regardless of which company provides it, security concerns would persist over Huawei equipment, as well as the fact that any buyer would still probably need to produce much of it in China.[61] The case has also been made that Huawei licences will continue to come under Chinese law, which would require compliance with the PRC's security services.[62]

In short, the existing vulnerabilities of 5G networks need to be addressed, but neither a ban on Huawei nor the purchase of its source code would provide a sufficient solution beyond marginal improvements in European mobile network security. A number of other measures are more promising.

Remedies to network security risks

While there is no solution that would effectively eliminate these network security risks, there are ways to reduce them and make it more difficult for anyone – not just China – to disrupt future networks. A number of possible measures have been brought up for discussion, such as greater redundancy of equipment and diversity of vendors, as well as the use of encryption, certification and assessments, and network flow monitoring.

Redundancy and *diversity* are interlinked and about improving resilience and securing availability of coverage. Their purpose is to provide an overlap of equipment and vendors in case of network failures, to ensure that there is always some back-up available. Given the critical services that are expected to rely on future 5G networks, ensuring a reliable connection will be one of the most important aspects of network security. Time and again, technical experts have emphasised how crucial redundancy and diversity are, most recently during an expert hearing in the German Parliament.[63] Diversity of vendors means ensuring that many different actors participate in the market, in order to prevent networks from becoming fully reliant on a single supplier.[64] The logic is essentially that different vendors are unlikely to be subject to the same problems at the same time.[65] Most

[61] The Economist, "Ren Zhengfei May Sell Huawei's 5G Technology to a western Buyer," *The Economist*, September 12, 2019, at: https://www.economist.com/business/2019/09/12/ren-zhengfei-may-sell-huaweis-5g-technology-to-a-western-buyer.
[62] BBC, "Huawei Chief Offers to Share 5G Know-how for a Fee," *BBC*, September 12, 2019, at: https://www.bbc.com/news/technology-49673144.
[63] Deutscher Bundestag, „Experten gegen Ausschluss von Anbietern beim Mobilfunkstandard 5G,“ *Deutscher Bundestag*, November 11, 2019, at: https://www.bundestag.de/dokumente/textarchiv/2019/kw46-pa-auswaertiges-5g-665414.
[64] Mathieu Duchâtel and Francois Godement, *Europe and 5G: The Huawei Case*, Paris: Institut Montaigne, 2019.
[65] Government Offices of Sweden, Ministry of Infrastructure, *national 5G Risk Assessment-Sweden's Response*, memorandum (unpublished), 2019.

© 2020 The Swedish Institute of International Affairs

recently, the Council of the European Union explicitly acknowledged the importance of vendor diversity.[66] Similarly, network redundancy refers to building additional layers of equipment within the network infrastructure (for example base stations) provided by multiple vendors.[67] The aim is to ensure that alternative equipment is available for network connections to fall back on to ensure continuous coverage in the event of network outages or malfunctions. While ensuring network redundancy can be costly, it is also effective at minimising the risk of large-scale network failures.[68]

Encryption addresses the safety of data traffic by protecting the information that flows on a network from unauthorised access. End-to-end encryption refers to a system in which only the communicating parties can access the encrypted information sent between them, and no third party in between.[69] Improving data security by means of encryption from a policy point-of-view could involve devising standards of encryption requirements that operators must meet. There is, however, a tension between strong encryption and the ability of law enforcement to access data for judicial purposes.[70] While encryption is a reliable method of securing data, law enforcement and intelligence agencies demand access to enable lawful interception of data, so there are usually ways to get around encryption in order to access information.

Another approach to strengthening network security has centred on *evaluation and certification* of products and processes, which aims to reduce the risk of backdoors or vulnerabilities that could be easily exploited by hackers. Products can be more or less secure, and security audits have the potential to assess the overall product quality, while also testing products and processes against certification requirements. One measure relevant to discussions on assessments is source code review, a process of evaluating the programming language of a device or other equipment to confirm it works as intended and to search for potential defects that could be exploited.[71] Since reviews are costly and time-consuming, however, there are limited incentives for companies to undertake them in any number internally. Regulation could be one way to create such incentives.[72]

One example of such auditing is the HCSEC, which was established in the UK in 2010 with the purpose of providing insight into Huawei's products and strategies there. In its most recent annual report, from March

[66] Council of the European Union, *Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G. Council Conclusions, 14519/19*, December 3, 2019. Brussels: Council of the European Union, p. 5.
[67] Jamie Davies, "*Germany Outlines Its 5G Security Requirements," Telecom News*, March 8, 2019, at: http://telecoms.com/496135/germany-outlines-its-5g-security-requirements/.
[68] Dali Wireless, *Whitepapers: Fault-Tolerant Public Safety System*, November 22, 2017, at: http://www.daliwireless.com/whitepapers/
[69] Andy Greenberg, "Hack Lexicon. What Is End-to-End Encryption?" *Wired*, November 25, 2014, at: https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.
[70] Council of the European Union, *Law Enforcement and Judicial Aspects Related to 5G*, 8983/19, May 6, 2019, Brussels: Council of the European Union.
[71] Douglas Busvine, "Exclusive: China's Huawei Opens Up to German Scrutiny Ahead of 5G Auctions," *Reuters*, October 23, 2018, at: https://www.reuters.com/article/us-germany-telecoms-huawei-exclusive/exclusive-chinas-huawei-opens-up-to-german-scrutiny-ahead-of-5g-auctions-idUSKCN1MX1VB.
[72] Author interview with Pontus Johnson, professor in cyber security at KTH, Stockholm, June 2019.

2019, the HCSEC oversight board highlights serious vulnerabilities in Huawei product code and systematic defects in the company's software engineering and cybersecurity competences.[73] Aiming to replicate the UK approach, Huawei has erected transparency centres in Bonn, Germany and Brussels.[74] In contrast to the UK, however, these centres are not under the oversight of state authorities.

Even more crucially, auditing and certification have their technological limitations, not least that the heavy reliance on software-based solutions instead of hardware in 5G technology requires extensive maintenance work, updates and security patches. This means that a certified source code will be continuously updated, providing opportunities to include new vulnerabilities or backdoors. Hence, even if auditing and certification could prove a level of security of the source code at the time of its assessment, it would be practically impossible to review all patches individually, leaving aside the vulnerabilities that can result from a combination of updates. Due to the complexity of today's IT systems, it is impossible to cover the millions of lines of code present in devices and equipment, or to confirm the absence of backdoors. In other words, occasional audits are ineffective, and attempts to assess new code before every update unrealistic.[75]

What complicates this issue even further is the fact that this work is complex and many operators involve vendors in the maintenance work on the mobile infrastructure, providing them with direct access to the core functions of the system. Even if restrictions were to be imposed on access for maintenance purposes, however, such as excluding certain vendors from making VPN connections to certain equipment for remote maintenance or assigning maintenance work to specific qualified and vetted personnel (as is the case in the UK), auditing and certification would be insufficient measures for providing meaningful reassurance of the security of any given mobile infrastructure technology.[76]

Another suggested measure to mitigate attempts at espionage as well as sabotage is *network flow monitoring*, which essentially entails gathering and analysing metadata. Operators have access to information about the data that flows into and out of their core network, and could therefore track data in order to detect and investigate abnormalities, such as traffic rerouting or leaks in which information could be redirected or transferred from the network to some third party.[77] However, while network flow monitoring can be used to create comprehensive views of network activity, it might be less useful for tracking specific targets or individuals.[78] In addition,

[73] Huawei Cyber Security Evaluation Centre Oversight Board, *Annual Report: A Report to the National Security Adviser of the United Kingdom*, March 2019, at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf, p. 20.

[74] Adam Satariano, "Huawei Security "Defects" Are Found by British Authorities," *The New York Times*, March 28, 2019, at: https://www.nytimes.com/2019/03/28/technology/huawei-security-british-report.html.

[75] Achour Messas et al., *5G in Europe: Time to Change Gear!* Paris: Institut Montaigne, 2019. We do not argue that certification is not helpful but rather emphasise that it is not sufficient. Improvement of certification such as GSMA's NESAS can only be a minor contribution to a multifaceted risk mitigation.

[76] Jan-Peter Kleinhans, *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung, 2019.

[77] Achour Messas et al., *5G in Europe: Time to Change Gear!* Paris: Institut Montaigne, 2019.

[78] Author interview with an anonymous engineer, Berlin, May 2019.

© 2020 The Swedish Institute of International Affairs

the increasing amount of data is likely to outpace the technology currently used for network flow monitoring and make it more difficult to detect malicious traffic.[79]

Overall, when it comes to increasing network security, measures must be taken with regards to technical standards for cybersecurity, their implementation, and the configuration and operation of mobile infrastructure. Technical standards can entail exploitable security vulnerabilities, an issue that needs to be addressed on a global level at the Third Generation Partnership Project (3GPP), which is the most important international standard developing organisation in this field.[80] The Council of the European Union emphasises "the need to put in place robust common security standards and measures, acknowledging international standardisation efforts on 5G, for all relevant manufacturers, electronic communications operators and service providers."[81] The implementation of these standards is the task of vendors such as Huawei while configuration is the duty of mobile network operators. Finally, the operators' dimension should involve continuous risk assessments and risk mitigation, including experienced IT security personnel and routines for network maintance.[82] This demonstrates that improving network security is not just a matter concerning mobile equipment manufacturers, but involves a number of actors, including mobile operators, which is rarely mentioned in the public debate.

Some of the remedies discussed in this section are more effective than others, but none will be sufficient alone. The most effective way to mitigate the main concerns of the debate, however, is to address the two main areas of challenges that are anticipated for future 5G networks: technological risks and increased societal dependency. The most effective measures for this are encryption against espionage, and redundancy and diversification of vendors against a kill switch. Together, these offer the most appropriate response to the risks posed by an external party. At the same time, we need to acknowledge that it is impossible to fully exclude the risk of exploitable vulnerabilities and backdoors.

Many of the risks that are expected to accompany 5G technology are risks that to some extent already exist in networks today. What is essentially new in the development of 5G networks is that we are now in a situation in which the leading suppliers are Chinese. Banning them could make it somewhat more troublesome for China to gain access to network systems, but is unlikely to prevent the PRC from gaining access where it wants to and would come instead with high costs – both economic and political. It is true that it is easier to listen in on, or shut down, an already controlled network than to seek to

[79] Jason J. Uher et al., "Investigating End-to-End Security in 5G Capabilities and IoT Extensions," *The Next Wave* 21:4, p. 18. Lorenzo Pupillo, "5G and National Security. A Complex Puzzle," *CEPS*, June 21, 2019, at: https://www.ceps.eu/5g-and-national-security/.

[80] Audun Jøsang et al., "Vulnerabilitiy by Design in Mobile Network Security," *The Journal of Information Warfare* 14:4, 2015. David Rupprecht et al., "On Security Resarch Towards Future Mobile Network Generations", *IEEE Communications Survey and Tutorials* 20: 3, pp. 2518-2542, 2018.

[81] Council of the European Union, *Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G. Council Conclusions, 14519/19*, December 3, 2019. Brussels: Council of the European Union, p. 6.

[82] Jan-Peter Kleinhans, *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung, 2019. Jan-Peter Kleinhans, *Whom to Trust in a 5G World. Policy Recommendations for Europe's 5G Challenge*, Berlin: Stiftung Neue Verantwortung, 2019.

exploit vulnerabilities in order to obtain access. However, many experts are convinced that China has enough technical knowledge and capabilities to shut down critical infrastructure or obtain sensitive information even without Huawei equipment. Thus, if the concerns really are about espionage and sabotage, other means would be more appropriate for and effective at mitigating these risks.

Geo-economics and dependencies

Even though a ban on Huawei would provide little if any help with containing existing risks to 5G network security, such action remains the main subject of the debate. One suggested approach is to ban Huawei by introducing criteria on the political and legal ecosystems of vendors. Poland, for example, is considering such an "Australian solution". The Polish Prime Minister, Mateusz Morawiecki, and the US Vice President, Mike Pence, have signed an agreement stating that "independent judicial review", a "record of ethical corporate behavior" and being "subject to a legal regime that enforces transparent corporate practices" should be criteria for a "rigorous evaluation" of any supplier.[83] Another approach, adopted for example by France and recently also Sweden, allows for the ban of suppliers on the grounds of concerns over national security, even without explicitly listing criteria.[84] Neither the "Australian" nor the "French" approach provides a solution to network security risks. Why, then, do they remain part of the political agenda? The answer lies in the increasing geopolitical tensions over technology between the US and China.

Instead of effectively mitigating network security risks, a ban on Huawei would be a severe blow to China's geopolitical ambitions. Recently, both the US and China have been testing whether they can capitalise politically on their technological leadership. Most prominently, the US administration has issued an executive order that not only bans Huawei from the US mobile infrastructure market, but also includes the Chinese tech giant on an "entity list" that prohibits US suppliers from doing business with it.[85] China responded with its own entity list and a threat to cut western suppliers off from strategically important raw materials, most notably the

[83] White House, "US-Poland Joint Declaration on 5G," *The White House*, September 5, 2019, at: https://www.whitehouse.gov/briefings-statements/u-s-poland-joint-declaration-5g/.
[84] Sveriges Riksdag, *Skydd av Sveriges säkerhet vid radioanvändning*, at: https://www.riksdagen.se/sv/dokument-lagar/arende/betankande/skydd-av-sveriges-sakerhet-vid-radioanvandning_H701TU4#stepBeredning.
[85] Ting-fang Cheng et al., "Exclusive: Huawei Stockpiles 12 Months of Parts Ahead of US Ban," *Nikkei*, May 17, 2019, at: https://asia.nikkei.com/Economy/Trade-war/Exclusive-Huawei-stockpiles-12-months-of-parts-ahead-of-US-ban. Yuan Gao et al., "Trump's Huawei Threat Is the Nuclear Option to Halt China's Rise," *Bloomberg*, May 16, 2019, at: https://www.bloomberg.com/news/articles/2019-05-16/trump-s-huawei-threat-is-the-nuclear-option-to-halt-china-s-rise. David Ignatius, "Trump Loves Walls. But He Should be Careful about a Digital Barrier with China," *The Washington* Post, May 21, 2019, at: https://www.washingtonpost.com/opinions/global-opinions/trump-loves-walls-but-he-should-be-careful-about-a-digital-barrier-with-china/2019/05/21/7280a146-7c13-11e9-a5b3-34f3edf1351e_story.html?noredirect=on&utm_term=.37ec7a374c88. Sijia Jiang and Michael Martina, "Huawei's $105 Billion Business at Stake after US Broadside," *Reuters*, May 16, 2019, at: https://www.reuters.com/article/us-usa-trade-china-huawei-analysis/huaweis-105-billion-business-at-stake-after-u-s-broadside-idUSKCN1SM123.

rare earth minerals of which China supplies 80% of the world market.[86]

This confrontation has the potential to reach far beyond the PRC and the US. For example, in the weeks after the US issued its entity list, a discussion followed on whether it covered "only" direct US business with China or all trade using technology based on US patents. If the second interpretation prevails, even European suppliers such as ARM could be forced to cease trading technology based on US patents with Huawei. ARM's semi-conductors are a crucial component of chips produced by Hisilicon, a company that is fully owned by Huawei.[87] In reaction, Huawei is aiming to develop more indigenous technology. Unless China and the US reverse their current policy trajectories, we will witness the development of two distinct supply chains with little if any overlap, or a process of technological decoupling that will split the world into two spheres of technological influence. At its most extreme, this could even involve the loss of technological interoperability and the introduction of two different sets of technology standards, although this scenario seems rather unlikely. Currently, both the US and China have adopted a tactic of combining carrots and sticks to win over third markets and draw them into their respective spheres of technological influence. At the core of this competition over third markets are the EU member states.

A ban on Huawei (and potentially also other Chinese suppliers) from the European market would further fuel this tendency for a geographical split into two spheres of technological influence. Most crucially, however, this struggle has direct political implications since it adopts a new kind of geopolitical logic. It is geopolitical since it thinks of spheres of influence in geographical terms, prioritising relative political gains compared to the respective competitor over an absolute level of economic output. In contrast to traditional geopolitics, however, China and the US aim to control geographic spaces in a new and very different way. It is not military force but control over the flow of goods, services and data that will be decisive. In essence, both the US and China are striving for control over the technology and infrastructure that enables connectivity in Europe. Mark Leonard has described this trend as the new "connectivity wars".[88] China wants to achieve "flow control" in Europe; that is, the ability to "define, monitor, and enforce the rules that enable flows",[89] and 5G will be at the heart of defining and controlling the flow of data.

[86] Eamon Barrett, "China Is Creating Its Own "Entity List" to Avenge Huawei and Punish Foreign Firms," *Fortune*, June 18, 2019, at: https://fortune.com/2019/06/18/china-entity-list-huawei/. Research and Markets, "Research Report on China's Rare Earth Industry, 2019-2023," *Research and Markets*, May 2019, at: https://www.researchandmarkets.com/reports/4771561/research-report-on-chinas-rare-earth-industry?utm_source=CI&utm_medium=PressRelease&utm_code=f3gz66&utm_campaign=1248502+-+China+Rare+Earth+Market+Report+2019-2023%3a+China%27s+Rare+Earth+Exports+to+the+United+States+Accounted+for+78%25+of+U.S.+Rare+Earth+Imports&utm_exec=chdo54prd.

[87] Dave Lee, "Huawei: ARM Memo Tells Staff to Stop Working with China's Tech Giant," *BBC*, May 22, 2019, at: https://www.bbc.com/news/technology-48363772.

[88] Mark Leonard and Ulrike Esther Franke (eds), *Connectivity Wars: Why Migration, Finance and Trade are the Geo-economic Battlegrounds of the Future*, London: European Council on Foreign Relations, 2016.

[89] Heiko Borchert, *Flow Control Rewrites Globalization: Implications for Business and Investors*, Dubai: HEDGE21 Strategic Assessments, 2019, p. 7.

© 2020 The Swedish Institute of International Affairs

The US is seeking to avoid Chinese flow control over data in Europe.

This geopolitical logic of achieving flow control by means of technological dependence plays out in at least three dimensions. First, it creates economic advantages insofar as Chinese and US companies will profit from a new wave of the digitisation driven by AI and 5G. Corporations will be able not only to sell their products, but also to gain enormous royalties for patents.

However, technological decoupling also comes at an enormous cost. Step-by-step, existing equipment produced in the respective other sphere would need to be replaced. The replacement of Huawei base stations in Germany alone is estimated to cost €6.4 billion.[90] Limited production capacities could delay the roll-out of new technology such as 5G. Large segments of the ICT manufacturing base are located in Asia. It is questionable whether – and, even if so, how – a relocation to the west would be possible. At the very least it would be costly and time-consuming, and would come with enormous delay. The exclusion of Huawei from the roll-out of 5G in the UK could lead to a delay of 18–24 months.[91] The division of the world into two separate markets would reduce the sales opportunities of individual companies to "just" half of the world. Excluding Chinese vendors would reduce competition, which should be expected to increase prices. Extra costs would prevent technological innovation, since less funding would be available for research and development, and the market for innovative technology would be limited to just one "sphere of tech influence".

Second, technological spheres of influence come with political dependencies attached. Given how deeply 5G will penetrate our future societies and economies, this makes it critical infrastructure essential for production, urban organisation, public security and reliability of supply. If a country depends on US or Chinese technology exclusively, it could be forced to make political concessions. The fear is that the EU could face a situation in which it simply could not say no to Chinese demands because it is the PRC that delivers the continent's critical infrastructure.

Another political implication is the increase in supply chain security derived from technological decoupling. If only suppliers from allied countries manufacturing exclusively in allied countries produce technology, this diminishes the risk of backdoors and spyware being installed in technology.[92] At the same time, however, banning companies might reduce the potential for diversity, such as in the case of 5G Radio Access Network technology that is essentially only supplied by Huawei, Ericsson and Nokia. A ban on Huawei would leave Europe with only two suppliers.

Third, the new dynamic entails a new systems confrontation with a US-led democratic model that aims to preserve a free market economy in competition with an autocratic China relying on a state-permeated model in which corporations cannot be clearly separated from the party-

[90] Xuewu Gu et al., "Geopolitics and the Global Race for 5G," *CGS Global Focus*, Bonn: Center for Global Studies Bonn, 2019.

[91] Jamie Doward, "UK Mobile Operators Ignore Security Fears over Huawei 5G," *The Guardian*, July 6, 2019, at: https://www.theguardian.com/technology/2019/jul/06/huawei-uk-mobile-5g-networks-operators-gamble-security-concerns.

[92] Jan-Peter Kleinhans, *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung, 2019.

state's authority.[93] This arises not least from the fact that the PRC is perfecting its authoritarian control by means of new surveillance technologies. The most prominent example is the social credit score system that not only penalises behaviour that is seen as inappropriate from the CCP's viewpoint, but also rewards citizens for what the CCP sees as good behaviour.[94] In many parts of the world, China is not only exporting such technology, but training authoritarian regimes in how to use it for surveillance purposes. Hence, a digital divide would lead not only to two spheres of technology, but also to the use of technological applications for political purposes.

China's tech giants, including Huawei, contribute to and collaborate with the party-state's authority in this regard. In fact, while Huawei should not be equated with the Chinese party-state, it remains under its tight control with strong links to the security apparatus (see above).

It is this new geopolitical dynamic that plays out in economic gains, political dependencies and a systems confrontation that has induced speculation about whether we are facing a tech "Cold War" in which two spheres of technological influence decouple from each other and face-off against each other in a new antagonism. In this context, isolating China technologically will only motivate the PRC to become more self-reliant in its technology, further reducting any potential leverage for the west.[95]

Hence, while a ban on Huawei would not significantly increase network security, it feeds into the geopolitical logic of technological decoupling since it would substantially reduce European reliance on the Chinese tech giant. What critics of Huawei fear is not network insecurity but technological dependency. Interdependence has generally been identified as a stabilising force, not least because it raises the costs of coercion and (in the extreme) war. Decoupling is certainly a worrying scenario that is already under way. Europe's technological dependency on China is already high and the trend is to China's advantage. At the same time, however, European dependency on US technology is also significant. The EU runs the risk of getting squeezed between two technological superpowers. Levels of market share and innovation provide a good estimate of European dependency.

Market share. Europe largely depends on hardware from China and software from the US. For some time now, China has been at the core of high-technology supply chains. While it competed over price for labour-intensive production for a long time, the PRC is no longer just the workbench of the world. Technology made in China is competing on quality. Factories in the PRC do not just manufacture for US, Japanese and Korean brands. Chinese companies are capturing huge market shares with their own brands too. A crucial example is Huawei's share of the mobile internet infrastructure. By 2017, Huawei had captured 28%, ahead of the Swedish tech

[93] James Lewis, *How 5G Will Shape Innovation and Security: A Primer*, Washington DC: CSIS, 2018.

[94] Sebastian Heilmann, *Digitization plays into the hands of the Communist Party*, October 11, 2017, at: https://www.merics.org/en/china-flash/19th-party-congress-ccp. Kristin Shi-Kupfer and Maraike Ohlberg, "China's Digital Rise. Challenges for Europe," *Merics Papers on China* 7, Berlin: Merics, 2019.

[95] Jodi Xu Klein, "The Huawei Dilemma. Washington Still Stuck Trying to Balance National Security Against US Tech Spremacy," *South China Morning Post*, November 1, 2019, at: https://www.scmp.com/news/china/article/3035832/huawei-dilemma-washington-still-stuck-trying-balance-national-security-against.

giant Ericsson (27%), Nokia (Finland, 23%), and Samsung (South Korea, 3%). Another Chinese company, ZTE, held 13% in 2017.[96] In Europe, dependence on Huawei mobile infrastructure ranges from 80–90% in Belgium and the Czech Republic, to 60% in Germany and Poland, 50–60% in the United Kingdom and 50% in Denmark to around 30% in France.[97] Another strength of Huawei is the company's ability to produce all the elements of the ICT supply chain for 5G networks at scale – from infrastructure to end devices.[98] Only Samsung provides the same range of products; the South Korean firm is, however, much weaker on infrastructure. Also China's roll-out plans for 5G, particularly of SA 5G, are well ahead of Europe and the US. Until the end of 2019, the PRC is expected to have 130,000 5G base stations up and running.[99] The country further experiments with 5G enabled AI, not least in the fields of smart cities and surveillance.[100]

A crucial example of a US stronghold is cloud services, which have become fundamental to 5G. Globally, Amazon has 33% of the market, followed by Microsoft (16%) and Google (8%). The largest Chinese provider is Alibaba, which is fifth behind IBM. Amazon is still bigger than all the other four combined.[101]

In terms of hardware, the US (and South Korea) are ahead of Europe and – even more so – of China when it comes to the production of semi-conductors. Among the top ten manufacturers, with a combined market share of almost 60% in 2018, six were US companies (Intel with a 14% market share, Micron technology with 6.3%, Broadcom, 3.4%, Qualcomm, 3.2%, Texas Instruments, 3.1% and Western Digital, 1.9%). Two were South Korean (Samsung with a market share of 15.5%, skhynix with 7.6%) and two were based in Europe (ST Microelectronics and NXP Semiconductors with 1.9% market share each).[102]

Innovation and patents. European operators, vendors and experts agree that Huawei's 5G technology is of high quality. Some believe that the Chinese tech giant is on a par with European manufacturers, while others argue that it is already leading. Particularly in a complex and innovative technology such as 5G, technological leadership requires massive investment in research and development (R&D). China has been prioritising 5G since 2009 and has

[96] David Bond and James Kynge, "China Spying Risk Hits Huawei's UK Ambitions," *Financial Times*, 3 December 2018.

[97] Paul Triolo, et al., "One Company, Many Systems. US Forces Governments to Choose Sides on Huawei," *Special Report Prepared by Eurasia Group*, Washington DC, Eurasia Group, 2019.

[98] CNN, "Huawei arrest: This is what the start of a tech Cold War looks like," *CNN*, December 9, 2018, at: https://m.cnn.com/en/article/h_9345b23ca7053f08332030a63d7e3329.

[99] BBC, "China Rolls Out One oft he World's Largest 5G Networks," *BBC*, November 1, 2019, at: https://www.bbc.com/news/business-50258287.

[100] William Zheng, "China's Shenzhen Is Using Big Data to become a Smart "Socialist Model City"," *South China Morning Post*, Novmber 1, 2019, at: https://www.scmp.com/news/china/politics/article/3035765/chinese-city-shenzhen-using-big-data-become-smart-socialist

[101] Synergy Research Group, "Cloud Service Spending Still Growing Almost 40% per Year; half of it won by Amazon & Microsoft," *Synergy Research Group*, July 26, 2019, at: https://www.srgresearch.com/articles/cloud-service-spending-still-growing-almost-40-year-half-it-won-amazon-microsoft.

[102] Gartner, *Gartner Says Worldwide Semiconductor Revenue Grew 12.5 Percent in 2018*, April 11, 2019, at: https://www.gartner.com/en/newsroom/press-releases/2019-04-10-gartner-says-worldwide-semiconductor-revenue-grew-12-.

poured enormous amounts of funds into R&D. Huawei spent US$ 77.1 billion on R&D between 2008 and 2018, around 10% of the company's revenues on average.[103] In 2017 alone, several sources put Huawei's 5G R&D budget between US$ 13.23 and US$ 14.3 billion, equal to around 15% of the company's revenues. With this amount of funds, Huawei can outspend the combined R&D resources of Ericsson and Nokia.[104]

China's investments in R&D pay off. One crucial indicator is its share of patented technology that is necessary to meet global 5G standards, known as standard-essential patents (SEPs). It is highly complex to calculate SEPs and data can differ significantly at times.[105] While some (such as IPlytics) calculate that China is already leading in 5G SEPs as a result of having submitted the most, and particularly important, contributions to the standardization process in 3GPP,[106] others regard Europeans slightly ahead of Chinese vendors.[107] Whatever figures will turn out to be correct, China's share of SEPs is not only significant, but rapidly increasing.

Many patents are still registered in the EU, but the share owned by European companies is decreasing. In 2008, 2,693 patents related to telecommunications and connectivity were filed in the EU, of which only 116 were filed by Chinese firms. By 2017, this number had increased 12-fold to 1,478 out of 3,717 patents. This is an increase from a 4.3% to a 39% share for Chinese patents in EU-registered telecommunications patents.[108]

Is the future Chinese? Even now, Europe is largely dependent on US and Chinese technology. Unless Europe changes course, EU member states are highly likely to fall further behind. The PRC is strategically investing in innovative technology in particular. Even though the formula "Made in China 2025", which is the official title of a state-led project to support homegrown innovation in core technologies including ICT, has been rhetorically downgraded, China will remain committed to the goals behind the initiative. Potentially, this has far-reaching implications even for market segments in which European vendors are strong. For example, today Huawei, Ericsson and Nokia share the global RAN technology market. Experts fear that within the next decade, however, Huawei could squeeze out both European vendors if nothing is done. The reason is not a lack of equipment quality from Ericsson and/or Nokia, but that Huawei receives backing from the Chinese state. In developing countries, for example, China makes loans for the roll-out of 5G infrastructure conditional on benefits for Huawei.

China itself has adopted a geopolitical approach to 5G. The PRC's strong position in global supply chains and technical standardisation does not prevent the

[103] Data according to Huawei's own declarations.
[104] Rick Nelson, "China's Huawei Seeks to Dominate 5G Standards Development," *Evaluation Engineering*, March 30, 2018, at: https://www.evaluationengineering.com/industries/communications/wireless-5g-wlan-bluetooth-etc/article/13017349/chinas-huawei-seeks-to-dominate-5g-standards-development.
[105] Ericsson, *Estimating the Future 5G Patent Landscape*, October 2018, at: https://www.ericsson.com/assets/local/patents/estimating-the-future-5g-patent-landscape.pdf.
[106] Tim Pohlmann, "Who is Leading the 5G Patent Race? A Patent Landscape Analysis on Declared SEPs and Standards Contributions", *IPlytics*, July 2019, Berlin: IPlytics.
[107] Matthew Noble et al. "Determining Which Companies Are Leading the 5G Race," *Wireless Technology* July/August 2019, pp. 35-40.
[108] John Strand, "The Chinese Cybersecurity Threat is more than Huawei Network Equipment," *New Europe*, March 21, 2019, at: https://www.neweurope.eu/article/the-chinese-cybersecurity-threat-is-more-than-huawei-network-equipment/.

© 2020 The Swedish Institute of International Affairs

country from heavily investing to gain technological independence. This is not least in response to US threats against the Chinese tech company ZTE that brought it close to a breakdown in 2018.[109] Also the Snowden revelations led to a lower level of Chinese trust in US technology. In response, the PRC strives not only for technological autarky but technological dominance. Protectionist policies of supporting national champions and forced technology transfers as a precondition for market access are only two of quite a number of unfair Chinese industrial policy practices. This endangers global competition and the diversity of the future ICT supply chain.[110] No doubt, the EU needs a toolbox to respond to Chinese industrial policies that goes far beyond investment screening.[111]

Should Europe therefore ban Huawei from the European market in order to protect its own companies and high-tech industrial base? This growing technological confrontation and Europe's increasing dependency raise the question of how the EU should react.

Towards a European response

The return of geopolitics makes US and Chinese competition over third countries crucially important. Europe appears to have become not the only, but possibly the most important battleground. At first glance, it might appear that this puts Europe in a favourable position and gives it considerable leverage. For two reasons, however, Europe is actually in a rather weak position. First, given its enormous dependence on technology from both the US and China, Europe is technologically vulnerable. Second, the EU runs the risk of fragmentation. It is a good sign that EU member states have delegated the process of coordination to the European Commission. However, despite joint efforts on a coordinated risk assessment that could result in similar responses to the current situation, significant differences remain. Poland and the Czech Republic, for example, seem to be the most willing to follow the US position on banning Huawei. Portugal, on the other hand, is deepening its cooperation with China on 5G. Germany, France and Italy are about to adopt policies that formulate stricter technical criteria that could lead to a partial ban on Huawei. Most recently, however, all three countries have considered including political criteria in their legislation that will make it more difficult for Huawei to participate in the roll-out of 5G. Initially, the German government wanted to follow the recommendations of a public technical agency, but the push for

[109] Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *CSIS*, August 2, 2018, at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf. Claire Ballentine, "US Lifts Ban that Kept ZTE From Doing Business with American Suppliers", *The New York Times*, July 13, 2018, at: https://www.nytimes.com/2018/07/13/business/zte-ban-trump.html. Cheng Ting-fang et al., "Exclusive: Foxconn Plans $9bn China Chip Project Amid Trade War," *Nikkei Asia*, December 21, 2018, at: https://asia.nikkei.com/Business/China-tech/Exclusive-Foxconn-plans-9bn-China-chip-project-amid-trade-war.

[110] Martina F. Ferracane and Hosuk Lee-Makiyama, "China's Technology Protectionism and Its Non-negotiable Rationales," *ECIPE*, June 2017, at: https://ecipe.org/wp-content/uploads/2017/06/DTE_China_TWP_REVIEWED.pdf.

[111] Mikko Huotari and Agatha Katz, *Beyond Investment Screening. Expanding Europe's Toolbox to Address Economic Risks from Chinese State Capitalism*, 2019, at: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/DA_Studie_ExpandEurope_2019.pdf.

© 2020 The Swedish Institute of International Affairs

political solutions is getting louder in the German Parliament. France and Italy have adopted technical criteria but also devised two variations on a decision-making procedure that allows political leaders the ultimate decision.[112]

Caught up in technological dependency and internal fragmentation, what should the EU do? Three different options are being discussed in the current debate. The first is for Europe to side with the US, effectively banning Huawei and building on the transatlantic partnership, not least because of the established transatlantic security alliance. The second option combines non-discriminatory criteria that help to exclude non-European vendors, not only Chinese but also other – such as US – suppliers wherever technologically achievable. Such technological protectionism would need to be combined with the development of an indigenous European technology industry. This approach ultimately aims for European strategic autonomy or "European sovereignty".[113] The third option is no change of policy, which preserves the openness of the European market, and inevitably results in a further increase in Huawei's market share and extended dependency on China. This option is also likely to see a gradual deterioration in the transatlantic partnership.

While we are most sympathetic to the second option, we regard all three as essentially suboptimal. Options 1 and 2 adopt a geopolitical logic of isolationism from either one or both great powers and decoupling, fuelling great power competition and – at worst – the emergence of a new Cold War. Option 3, in turn, aims simply to ignore the ongoing geopolitical turn in international affairs, which appears naïve. Given Europe's close security alliance with the US, it is questionable whether the third option is feasible. Even if it were, however, Europe could end up being squeezed between the two great powers with little room for manoeuvre.

Against a backdrop of these weaknesses, this paper ends with a presentation of a preliminary idea for a fourth option, which has similarities with option 2 but contains a crucial and markedly different aspect. We call this option "strategic access". The strategic access option starts from the assumption that Europe has an interest in preventing isolation and decoupling, seeks to reject the geopolitical turn to prevent a new Cold War, but needs to be realistic. It contains a combination of and balance between two elements: diversification and light protectionism.

In this paper, we can only outline the basic underlying idea and need to leave open important details of its implementation. The aim is to stimulate debate on this subject rather than offering comprehensive practical solutions at this point in the discussion. To implement the agenda we propose will require extensive discussion and creativity, ranging from digital free trade arrangements through competition law to minimum localisation requirements and a wide range of other means. Further

[112] For an overview see for example Kadri Kaska et al., *Huawei, 5G and China as a Security Threat*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, pp. 15-18. Tim Nicholas Rühlig et al., "5G, Europe and the Tech Rivalry between the US and China - a Wrestling Match. Europe caught on its Back Foot," *SWP Comment 29*, Berlin: SWP, 2019.

[113] European Political Strategy Centre, *Rethinking Strategic Autonomy in the Digital Age*, Brussels: European Commission, 2019. Council of the European Union, *Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G. Council Conclusions, 14519/19*, December 3, 2019. Brussels: Council of the European Union, p. 3.

discussion will be needed to address not just the details, but the fundamentals of such an approach, and it will profit from discussion beyond Europe, including with China and the US.[114] Crucially, however, while we have developed the idea of strategic access in relation to the current debate over Huawei's inclusion in the roll-out of the mobile network infrastructure for 5G, it is an idea that aims to address a broader set of technological dependencies and vulnerabilities of the EU.

Diversification

In sharp contrast to all three options discussed above, strategic access aims to preserve an international environment that is as open and inclusive as possible without running the risk of strong dependencies. In order to achieve this goal, diversification of supply chains will be of crucial importance. The current rise of geopolitics is about the US and China attempting to squeeze out the most political capital from threatening to cut off external actors from the supply of core resources (e.g. rare earths) and technologies (e.g. semi-conductors). A response that follows the logic of open and free trade could therefore respond to this tactic by diversifying supply chains.

Diversification of supply chains combines two dimensions. First, Europe should import technology and raw materials from as many different suppliers from as many different countries as possible. Second, Europe should avoid dependency on technology that relies on patents from one country in order to avoid being dragged into the patent wars that loom behind Trump's entity list. Preferential treatment should, for example, be granted to technology developed from open sources.

This strategy of diversification should be combined with the use of all available means under WTO law to preserve free trade and fair competition. Even in fields where European companies are strong, it faces competition from state-backed companies such as ZTE or Huawei. Hence, the EU needs to weigh the options available under international trade law to address the challenges arising from dumping and subsidies. The US could be a natural partner in these attempts.[115] On patents, in turn, the EU faces pressure from both the US and China to reduce royalty fees. A fair patent policy and the effective enforcement of Intellectual Property Rights (IPR) will be crucial for innovative companies such as Ericsson and Nokia.

Hence, strategic access does not start from the idea of locking into the digital sphere of either China or the US. Nor does it adopt an ideal of self-reliance and autarky in the digital sphere – a goal that would be unrealistic for Europe. However, the perspective acknowledges the geopolitical risks of current developments and aims to respond by emphasising the diversification of supply chains.

At the same time, diversification requires substantial political intervention in the economic sphere. While European policymakers cannot and should not make decisions about suppliers for corporations, they should provide the necessary incentives for diversification, such as free trade agreements on digital issues.

[114] See for example the excellent discussion in Elsa B. Kania, *Securing Our 5G Future: The Competitive Challenge and Considerations for US Policy*, November 2019. Washington DC: Center for a New American Security.

[115] Jennifer Hillman, "The Best Way to Address China's Unfair Policies and Practices in Through a Big, Bold, Multilateral Case at the WTO," *Testimony before the US-China Economic and Review Security Commission*, 2018, June 8, at: https://www.uscc.gov/sites/default/files/Hillman%20Testimony%20US%20China%20Comm%20w%20Appendix%20A.pdf.

Jan-Peter Kleinhans, for example has suggested a supply chain risk management system similar to existing ones in the US and the United Kingdom, as well as the promotion of supplier diversity through industrial policy. One example could be national coordination among operators to ensure RAN diversity. This could allow for national roaming guratanteeing coverage even in the case that one operator's equipment fails.[116]

Protectionism light

While diversification should be at the heart of the European approach and prioritised wherever possible, it is unlikely that the emergence of strategic dependencies can be completely avoided. Hence, diversification will need to be combined with a slimmed down version of protectionism that helps defend existing and develop new strategic sectors of the European digital industry. Protectionism should be avoided wherever possible; it should be a "last resort", which is why we speak of "protectionism light".

In some niches, the digital industry in the EU remains strong, mostly in highly specialised fields of application driven by small and medium-sized enterprises. One exception is mobile infrastructure in general and RAN technology in particular, where Ericsson and Nokia hold significant market shares. Experts fear, however, that the fact that Huawei receives so much support from the Chinese party-state could squeeze western companies, including Ericsson and Nokia, out of the global market.[117] European policymakers should therefore consider how to preserve the market presence of the two European tech companies.

Most sensitive is the question of how to support and develop indigenous IT manufacturing in Europe. The European IT industry is mostly underdeveloped and is unlikely to flourish unless it receives some degree of protection. There is no European version of Google, Microsoft, Apple, Huawei, Alibaba or Tencent. If Europe wants to facilitate the rise of a tech giant, it will need to think about preferential treatment similar to the development of Airbus in aviation.

Europe needs to address its industrial weakness but also to take action to preserve its influence on regulation and standard setting. A positive example of Europe's influence is the General Data Protection Regulation (GDPR), which has become a benchmark for global data protection even if it is not fully enforced by either European or non-European actors. The regulatory relevance of the EU relies on its market size. Hence, if the EU wants to continue to influence global rule-making in the digital sphere, it needs to deepen its integration and develop its Digital Single Market. Some standards, particularly technical standardisation, are based on technological leadership. The EU needs to increase its support for research and development, not least in basic research that is less commercially profitable in the short term. Above all, Europe needs to coordinate and cooperate more closely on the development of its digital economy, including both diversification and protectionism light.[118]

[116] Jan-Peter Kleinhans, *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung, 2019, p. 18. Jan-Peter Kleinhans, *Whom to Trust in a 5G World. Policy Recommendations for Europe's 5G Challenge*, Berlin: Stiftung Neue Verantwortung, 2019, pp. 10-13.

[117] White House, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, Washington DC: White House Office of Trade and Manufacturing Policy, 2018.

[118] Julian King, "Europe's 5G Network Will be Secure – If We Work Together," *The Guardian*, October 28, 2019, at:

© 2020 The Swedish Institute of International Affairs

Conclusion

Under the pretext of network (in-)security, Europe is discussing the roll-out of 5G networks throughout the continent. At the core of the discussion is the controversial role of Chinese vendors in general and the Chinese tech-giant Huawei in particular.

The security of Europe's 5G network is undoubtedly crucial. Technological innovation, particularly a new virtualised core network, network slicing and more edge computing, will enable a wide range of applications of next generation mobile networks. Ultra-low latency and massive machine-to-machine communication will revolutionise the economy and society. 5G will be omnipresent, running not just future "smart cities", autonomous vehicles and the health sector, but also production (industrial IoT). In short, 5G networks are truly critical infrastructure and demand all our efforts to make them as secure as possible.

The ongoing debate in Europe mainly focuses on two risks to network security: sabotage and espionage. The fear is that the inclusion of Huawei technology in 5G-critical infrastructure could allow China to conduct industrial and political espionage and even provide the authoritarian regime in Beijing with opportunities to shut down the 5G network or threaten Europe with such a scenario. These are real and serious risks. Sabotage and espionage are technically feasible and Huawei is hardly in a position to reject orders from the ruling Chinese Communist Party.

We argue, however, that the proposed solution of banning Huawei does not address network security, but rather geo-economic challenges that arise from dependency. If Europe is serious about addressing sabotage and espionage, a ban on Huawei would indeed increase security but is not the most effective means to mitigate the risks. Encryption is the best protection against espionage. Network redundancies and diversity of vendors, in turn, would be most effective reducing the risk of a kill switch. After all, there is no such thing as complete network security, and attacking critical infrastructure can only be made more complicated and more costly.

Instead of increasing network security, the proposed ban on Huawei follows a very different logic: the logic of the increasing geopolitical tensions over technology. China's Belt and Road Initiative is a major infrastructure policy that aims not just to build physical and – even more importantly – digital infrastructure, but to control the flow of goods, services and data. Third countries, first and foremost Europe, become the primary target of this rising technological confrontation between the US and China, and Europe faces the risk of further increasing its technological dependency.

The current situation demonstrates Europe's vulnerability. Europe is heavily reliant on software from the US and hardware from China. This has contributed to an internal fragmentation among EU member states in their responses to the current situation. In order to address this, three options are currently being discussed: siding with the US, strategic European autonomy and no policy change, which benefits China.

We reject all three options and sketch out a fourth alternative that we refer to as strategic access. Strategic access aims to avoid both fuelling the geopolitical turn resulting from technological decoupling and falling victim to this development. It

https://www.theguardian.com/commentisfree/2019/oct/28/europe-5g-network-technology.

combines two aspects: diversification and light protectionism. Diversification is the most crucial component, aiming for a diversification of supply in order to avoid dependency on manufacturing and the underlying patents that could be utilised in a state-run patent war. It also implies consideration of using the legal means available under WTO law to address issues of subsidies and fair competition, as well as effective implementation of a fair patent policy and IPR enforcement.

Protectionism light, in turn, should only be applied where the diversification strategy has failed. It includes defending the existing European digital industry where it runs the risk of suffering from unfair Chinese competition resulting from the state-permeated character of the Chinese economy. It further entails a limited and strategically targeted industrial policy to strengthen the EU's industrial base in core technological fields of digitisation by a variety of means from R&D support to deepening the Digital Single Market. While we discuss this approach in the context of the ongoing 5G infrastructure debate, we believe that it addresses the wider phenomenon of technological rivalry that can be expected continue beyond 5G in the future.[119]

[119] Marianne Schneider-Petsinger et al., *US-China Strategic Competition: The Quest for Global Technology Leadership*, London: Chatham House, 2019.

References

Baker, Richard, "Top 5G Suppliers Linked to China's Communist Party," *Sydney Morning Herald*, August 13, 2018, at: https://www.smh.com.au/business/companies/top-5g-suppliers-linked-to-china-s-communist-party-20180812-p4zwzt.html.

Balding, Christopher and Donald Clarke: "Who Owns Huawei?", *SSRN*, May 8, 2019, at: https://ssrn.com/abstract=3372669/.

Balding, Christopher, "Huawei Technologies' Links to Chinese State Security Services," *SSRN*, July 9, 2019, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726.

Ballentine, Claire, "US Lifts Ban that Kept ZTE From Doing Business with American Suppliers", *The New York Times*, July 13, 2018, at: https://www.nytimes.com/2018/07/13/business/zte-ban-trump.html.

Barrett, Brian, "How China's Elite Hackers Stole the World's Most Valuable Secrets," *Wired*, December 20, 2018, at: https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/

Barrett, Eamon, "China Is Creating Its Own "Entity List" to Avenge Huawei and Punish Foreign Firms," *Fortune*, June 18, 2019, at: https://fortune.com/2019/06/18/china-entity-list-huawei/.

BBC, "China Rolls Out One oft he World's Largest 5G Networks," *BBC*, November 1, 2019, at: https://www.bbc.com/news/business-50258287.

BBC, "Huawei Chief Offers to Share 5G Know-how for a Fee," *BBC*, September 12, 2019, at: https://www.bbc.com/news/technology-49673144.

Beevers, Kris, "Why 5G is Bringing Edge Computing Automation Front and Center," *Network World*, February 14, 2018, at: https://www.networkworld.com/article/3255426/why-5g-is-bringing-edge-computing-and-automation-front-and-center.html.

Black, Douglas, "Huawei and China. Not Just Business as Usual," *Journal of Political Risk* 8: 1, 2019.

Bloomberg News, How Huawei Became a Target for Governments, *Bloomberg,* January 23, 2019, at: https://www.bloomberg.com/news/articles/2019-01-23/how-huawei-became-a-u-s-government-target-quicktake.

Bond, David and James Kynge, "China Spying Risk Hits Huawei's UK Ambitions," *Financial Times*, 3 December 2018.

Borchert, Heiko, *Flow Control Rewrites Globalization: Implications for Business and Investors*, Dubai: HEDGE21 Strategic Assessments, 2019, p. 7.

Brewster, Thomas "Chinese Trio Linked to Dangerous APT3 hackers Charged with Stealing 407GB of Data from Siemens," *Forbes*, November 27, 2017, at: https://www.forbes.com/sites/thomasbrewster/2017/11/27/chinese-hackers-accused-of-siemens-moodys-trimble-hacks/.

Busvine, Douglas, "Exclusive: China's Huawei Opens Up to German Scrutiny Ahead of 5G Auctions," *Reuters*, October 23, 2018, at: https://www.reuters.com/article/us-germany-telecoms-huawei-exclusive/exclusive-chinas-huawei-opens-up-to-german-scrutiny-ahead-of-5g-auctions-idUSKCN1MX1VB.

Cave, Danielle et al. "Mapping China's Technology Giants," *ASPI Issues Paper Report* 1/2019, Barton: ASPI.

Cheng, Ting-fang et al., "Exclusive: Foxconn Plans $9bn China Chip Project Amid Trade War," *Nikkei Asia*, December 21, 2018, at: https://asia.nikkei.com/Business/China-tech/Exclusive-Foxconn-plans-9bn-China-chip-project-amid-trade-war.

Cheng, Ting-fang et al., "Exclusive: Huawei Stockpiles 12 Months of Parts Ahead of US Ban," *Nikkei*, May 17, 2019, at: https://asia.nikkei.com/Economy/Trade-war/Exclusive-Huawei-stockpiles-12-months-of-parts-ahead-of-US-ban.

Chrysoloras, Nikos and Richard Bravo, "Huawei Deals for Tech Will Have Consequences, US Warns EU," *Bloomberg*, February 7, 2019, at: https://www.bloomberg.com/news/articles/2019-02-07/huawei-deals-for-tech-willhave-consequences-u-s-warns-eu.

Clarke, Donald, "The Zhong Lun Declaration on the Obligations of Huawei and Other Chinese Companies under Chinese Law," *SSRN*, March 28, 2019, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354211

© 2019 The Swedish Institute of International Affairs

CNN, "Huawei arrest: This is what the start of a tech Cold War looks like," *CNN*, December 9, 2018, at: https://m.cnn.com/en/article/h_9345b23ca7053f08332030a63d7e3329.

Council of the European Union, *Council Conclusions on the Significance of 5G to the European Economy and the Need to Mitigate Security Risks Linked to 5G. Council Conclusions, 14519/19*, December 3, 2019. Brussels: Council of the European Union.

Council of the European Union, *Law Enforcement and Judicial Aspects Related to 5G*, 8983/19, May 6, 2019, Brussels: Council of the European Union.

Dali Wireless, *Whitepapers: Fault-Tolerant Public Safety System*, November 22, 2017, at: http://www.daliwireless.com/whitepapers/

Davies, Jamie, "*Germany Outlines Its 5G Security Requirements," Telecom News*, March 8, 2019, at: http://telecoms.com/496135/germany-outlines-its-5g-security-requirements/.

de Looper, Christian, What is 5G?, *Digital Trends*, November 18, 2019, at: https://www.digitaltrends.com/mobile/what-is-5g/.

Deutscher Bundestag, „Experten gegen Ausschluss von Anbietern beim Mobilfunkstandard 5G," *Deutscher Bundestag*, November 11, 2019, at: https://www.bundestag.de/dokumente/textarchiv/2019/kw46-pa-auswaertiges-5g-665414.

Doward, Jamie, "UK Mobile Operators Ignore Security Fears over Huawei 5G," *The Guardian*, July 6, 2019, at: https://www.theguardian.com/technology/2019/jul/06/huawei-uk-mobile-5g-networks-operators-gamble-security-concerns.

Duchâtel, Mathieu and Francois Godement, *Europe and 5G: The Huawei Case*, Paris: Institut Montaigne, 2019.

EMF Explained Series, *5G Explained – How 5G Works*, without year, at: http://www.emfexplained.info/?ID=25916.

Ericsson, *Estimating the Future 5G Patent Landscape*, October 2018, at: https://www.ericsson.com/assets/local/patents/estimating-the-future-5g-patent-landscape.pdf.

European Political Strategy Centre, *Rethinking Strategic Autonomy in the Digital Age*, Brussels: European Commission, 2019.

Feng, Ashley, "We Can't Tell if Chinese Firms Work for the Party," *Foreign Policy*, February 7, 2019, at: https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/.

Ferracane, Martina F. and Hosuk Lee-Makiyama, "China's Technology Protectionism and Its Non-negotiable Rationales," *ECIPE*, June 2017, at: https://ecipe.org/wp-content/uploads/2017/06/DTE_China_TWP_REVIEWED.pdf

FireEye, *Mandiant APT1. Exposing One of China's Cyber Espionage Unites*, February 19, 2013, at: https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html.

Ford, Christopher Ashley, "Huawei and its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications," *Remarks at the Multilateral Action on Sensitive Technologies (MAST) Conference, 11 September 2019*, Washington DC: US State Department, 2019.

Foster, Andrew and Nicholas Borst, "Time Is Ripe for Huawei to Launch an IPO, to Address Political and Security Concerns Once and for All," *South China Morning Post*, May 27, 2019, at: https://www.scmp.com/comment/insight-opinion/article/3011510/time-ripe-huawei-launch-ipo-address-political-and-security.

Gao, Yuan et al., "Trump's Huawei Threat Is the Nuclear Option to Halt China's Rise," *Bloomberg*, May 16, 2019, at: https://www.bloomberg.com/news/articles/2019-05-16/trump-s-huawei-threat-is-the-nuclear-option-to-halt-china-s-rise.

Gartner, *Gartner Says Worldwide Semiconductor Revenue Grew 12.5 Percent in 2018*, April 11, 2019, at: https://www.gartner.com/en/newsroom/press-releases/2019-04-10-gartner-says-worldwide-semiconductor-revenue-grew-12-.

Gibb, Robert, "What is Edge Computing?" *Stackpath*, June 18, 2019, at: https://blog.stackpath.com/edge-computing/.

Gittik, Yuri, "Distributed Network Functions Virtualization. An Introduction to D-NFV," *RAD White Paper*, March 2014, at: http://crezer.net/Newsletter/archivos/Distributed-NFV-White-Paper.pdf.

Government Offices of Sweden, Ministry of Infrastructure, *National 5G Risk Assessment- Sweden's Response*, memorandum (unpublished), 2019.
Greenberg, Andy, "Hack Lexicon. What Is End-to-End Encryption?" *Wired*, November 25, 2014, at: https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.
Gu, Xuewu et al., "Geopolitics and the Global Race for 5G," *CGS Global Focus*, Bonn: Center for Global Studies Bonn, 2019.
Handelsblatt, "Deutsche Telekom warnt. Huawei-Ausschluss würde 5G-Einführung verzögern," *Handelsblatt*, January 29, 2019, https://www.handelsblatt.com/unternehmen/it-medien/neuer-mobilfunkstandard-deutsche-telekom-warnt-huawei-ausschluss-wuerde-5g-einfuehrung-verzoegern/23921762.html?ticket=ST-38734491-9lY7UMOoLFLoPSMFVweD-ap5.
Hawes, Colin and Grace Li, "Transparency and Opaqueness in the Chinese ICT Sector. A Critique of Chinese and International Corporate Governance Norms," *Asian Journal of Comparative Law* 12: 1, 2017, pp. 41-80.
Heilmann, Sebastian, *Digitization plays into the hands of the Communist Party*, October 11, 2017, at: https://www.merics.org/en/china-flash/19th-party-congress-ccp.
Heller, Michael, "Nokia: 5G Network Slicing Could Be a Boon For Security," *Techtarget*, April 10, 2019, at: https://searchsecurity.techtarget.com/news/252461410/Nokia-5G-network-slicing-could-be-a-boon-for-security.
Hillman, Jennifer, "The Best Way to Address China's Unfair Policies and Practices in Through a Big, Bold, Multilateral Case at the WTO," *Testimony Before the US-China Economic and Review Security Commission*, 2018, June 8, at: https://www.uscc.gov/sites/default/files/Hillman%20Testimony%20US%20China%20Comm%20w%20Appendix%20A.pdf.
Huawei Cyber Security Evaluation Centre Oversight Board, *Annual Report: A Report to the National Security Adviser of the United Kingdom*, March 2019, at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.
Huber, Nick, "A Hacker's Paradise? 5G and Cyber Security," *Financial Times*, October 14, 2019, at: https://www.ft.com/content/74edc076-ca6f-11e9-af46-b09e8bfe60c0.
Huotari, Mikko and Agatha Katz, *Beyond Investment Screening. Expanding Europe's Toolbox to Address Economic Risks from Chinese State Capitalism*, 2019, at: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/DA_Studie_ExpandEurope_2019.pdf.
Ignatius, David "Trump Loves Walls. But He Should be Careful about a Digital Barrier with China," *The Washington* Post, May 21, 2019, at: https://www.washingtonpost.com/opinions/global-opinions/trump-loves-walls-but-he-should-be-careful-about-a-digital-barrier-with-china/2019/05/21/7280a146-7c13-11e9-a5b3-34f3edf1351e_story.html?noredirect=on&utm_term=.37ec7a374c88.
Jiang, Sijia and Michael Martina, "Huawei's $105 Billion Business at Stake After US Broadside," *Reuters*, May 16, 2019, at: https://www.reuters.com/article/us-usa-trade-china-huawei-analysis/huaweis-105-billion-business-at-stake-after-u-s-broadside-idUSKCN1SM123.
Jøsang, Audun et al., "Vulnerabilitiy by Design in Mobile Network Security," *The Journal of Information Warfare* 14:4, 2015.
Kania, Elsa B., *Securing Our 5G Future: The Competitive Challenge and Considerations for US Policy*, November 2019. Washington DC: Center for a New American Security.
Kaska, Kadri et al., *Huawei, 5G and China as a Security Threat*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2019, pp. 10-11.
Kaspersky Lab, *Kaspersky Lab Starts Data Processing for European Users in Zurich and also Opens First Transparency Center*, November 13, 2018, at: https://www.kaspersky.com/about/press-releases/2018_kaspersky-lab-starts-data-processing-for-european-users-in-zurich-and-also-opens-first-transparency-center.
Kassel, Matthew, "As 5G Technology Expands, So Do Concerns Over Privacy," *Wall Street Journal*, February 26, 2019, at: https://www.wsj.com/articles/as-5g-technology-expands-so-do-concerns-over-privacy-11551236460.

King, Julian, "Europe's 5G Network Will be Secure – If We Work Together," *The Guardian*, October 28, 2019, at: https://www.theguardian.com/commentisfree/2019/oct/28/europe-5g-network-technology.

Klein Xu, Jodi, "The Huawei Dilemma. Washington Still Stuck Trying to Balance National Security Against US Tech Spremacy," *South China Morning Post*, November 1, 2019, at: https://www.scmp.com/news/china/article/3035832/huawei-dilemma-washington-still-stuck-trying-balance-national-security-against.

Kleinhans, Jan-Peter, *5G vs. National Security: A European Perspective*. Berlin: Stiftung Neue Verantwortung, 2019.

Kleinhans, Jan-Peter, *Whom to Trust in a 5G World. Policy Recommendations for Europe's 5G Challenge*, Berlin: Stiftung Neue Verantwortung, 2019.

Kluth, Andreas, "Huawei Is a Paralyzing Dilemma for the West," *Bloomberg*, November 23, 2019, at: https://www.bloomberg.com/opinion/articles/2019-11-23/huawei-s-5g-networks-are-a-paralyzing-dilemma-for-the-west.

Lee, Dave, "Huawei: ARM Memo Tells Staff to Stop Working With China's Tech Giant," *BBC*, May 22, 2019, at: https://www.bbc.com/news/technology-48363772.

Lee, Edison and Timothy Chau, "Telecom Services. The Geopolitics of 5G and IoT," *Jefferies Franchise Note*, Hong Kong: Jefferies, 2017.

Leonard, Mark and Ulrike Esther Franke (eds), *Connectivity Wars: Why Migration, Finance and Trade are the Geo-economic Battlegrounds of the Future*, London: European Council on Foreign Relations, 2016.

Lewis, James, *How 5G Will Shape Innovation and Security: A Primer*, Washington DC: CSIS, 2018.

Li, Tao, "Japan Latest Country to Exclude Huawei, ZTE From 5G Roll-out Over Security Concerns," *South China Morning Post*, December 10, 2018, at: https://www.scmp.com/tech/tech-leaders-and-founders/article/2177194/japan-decides-exclude-huawei-zte-government.

Lo, Steve and Kevin Lee, *China Is Poised to Win the 5G Race*, Hong Kong: EY, 2018.

Lulu, Jichang, "Synopsis: Huawei's Lawfare by Proxy," *China Digital Times*, February 2019, at: https://chinadigitaltimes.net/2019/02/sinopsis-huaweis-lawfare-by-proxy.

McCann, John and Mike Moore, "5G Everything You Need to Know," *Rechradar*, August 20, 2019, at: https://www.techradar.com/news/what-is-5g-everything-you-need-to-know.

Messas, Achour et al., *5G in Europe: Time to Change Gear!* Paris: Institut Montaigne, 2019.

Moehr, Ole, My Way or the Huawei: 5G at the Center of US-China Strategic Competition, *The Atlantic Council*, July 23, 2019, at: https://www.atlanticcouncil.org/blogs/econographics/my-way-or-the-huawei-5g-at-the-center-of-us-china-strategic-competition.

Nelson, Rick, "China's Huawei Seeks to Dominate 5G Standards Development," *Evaluation Engineering*, March 30, 2018, at: https://www.evaluationengineering.com/industries/communications/wireless-5g-wlan-bluetooth-etc/article/13017349/chinas-huawei-seeks-to-dominate-5g-standards-development.

NIS Cooperation Group, *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*, October 9, 2019, Brussels: European Commission.

Noble, Matthew et al. "Determining Which Companies Are Leading the 5G Race," *Wireless Technology* July/August 2019, pp. 35-40.

Pohlmann, Tim, "Who is Leading the 5G Patent Race? A Patent Landscape Analysis on Declared SEPs and Standards Contributions", *IPlytics*, July 2019, Berlin: IPlytics.

Price-Evans, Iwan, "Introducing the 5G Core Network Functions,"*Metaswitch*, February 7, 2019, at: https://www.metaswitch.com/blog/introducing-the-5g-core-network-functions.

PwC, "Operation Cloud Hopper," *PwC*, 2018, at: https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

Research and Markets, "Research Report on China's Rare Earth Industry, 2019-2023," *Research and Markets*, May 2019, at: https://www.researchandmarkets.com/reports/4771561/research-report-on-chinas-rare-earth-industry?utm_source=CI&utm_medium=PressRelease&utm_code=f3gz66&utm_campaign=1248502+-+China+Rare+Earth+Market+Report+2019-2023%3a+China%27s+Rare+Earth+Exports+to+the+United+States+Accounted+for+78%25+of+U.S.+Rare+Earth+Imports&utm_exec=chdo54prd.

© 2020 The Swedish Institute of International Affairs

Sveriges Riksdag, *Skydd av Sveriges säkerhet vid radioanvändning*, at: https://www.riksdagen.se/sv/dokument-lagar/arende/betankande/skydd-av-sveriges-sakerhet-vid-radioanvandning_H701TU4#stepBeredning

Rühlig, Tim Nicholas et al., "5G, Europe and the Tech Rivalry between the US and China - a Wrestling Match. Europe caught on its Back Foot," *SWP Comment 29*, Berlin: SWP, 2019.

Rupprecht, David et al., "On Security Resarch Towards Future Mobile Network Generations", *IEEE Communications Survey and Tutorials* 20: 3, pp. 2518-2542, 2018.

RWR Advisory Group, *Assessing Huawei Risk: How the Track Record of the CCP Should Play into the Due Diligence of Huawei's Partners and Customers*, Washington DC: RWR Advisory Group, 2019.

RWR Advisory Group, *Huawei Risk Tracker*, 2019, at: https://huawei.rwradvisory.com/.

Sachs, Jeffrey D., "America's War on Chinese Technology," *Project Syndicate*, November 7, 2019, at: https://www.project-syndicate.org/commentary/cheney-doctrine-us-war-on-chinese-technology-by-jeffrey-d-sachs-2019-11.

Sacks, Samm and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *CSIS*, August 2, 2018, at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180802_Chinese_Cybersecurity.pdf.

Satariano, Adam, "Huawei Security "Defects" Are Found by British Authorities," *The New York Times*, March 28, 2019, at: https://www.nytimes.com/2019/03/28/technology/huawei-security-british-report.html.

Schneider-Petsinger, Marianne et al., *US-China Strategic Competition: The Quest for Global Technology Leadership*, London: Chatham House, 2019.

Seely, Bob et al., *Defending Our Data: Huawei, 5G and the Five Eyes*, London: Henry Jackson Society, 2019.

Shi-Kupfer, Kristin and Maraike Ohlberg, "China's Digital Rise. Challenges for Europe," *Merics Papers on China* 7, Berlin: Merics, 2019.

Strand, John, "The Chinese Cybersecurity Threat is More than Huawei Network Equipment," *New Europe*, March 21, 2019, at: https://www.neweurope.eu/article/the-chinese-cybersecurity-threat-is-more-than-huawei-network-equipment/.

Synergy Research Group, "Cloud Service Spending Still Growing Almost 40% per Year; Half of it Won by Amazon & Microsoft," *Synergy Research Group*, July 26, 2019, at: https://www.srgresearch.com/articles/cloud-service-spending-still-growing-almost-40-year-half-it-won-amazon-microsoft.

Telecomlead, *Huawei Grabs 28% Share in Global Telecom Equipment Market*, December 7, 2018, at: https://www.telecomlead.com/telecom-equipment/huawei-grabs-28-share-in-global-telecom-equipment-market-87863.

Teral, Stephane, *IHS Markit Technology White Paper: 5G Best Choice Architecture*, London, IHS Markit, 2019.

The Economist, "Ren Zhengfei May Sell Huawei's 5G Technology to a western Buyer," *The Economist*, September 12, 2019, at: https://www.economist.com/business/2019/09/12/ren-zhengfei-may-sell-huaweis-5g-technology-to-a-western-buyer.

Torbet, Georgina, "Chinese Companies Want to help Shape Global Facial Recognition Standards," *Engadget*, December 2, 2019, at: https://www.engadget.com/2019/12/02/china-facial-recognition-standards/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAKcP2n-viXPHG8Lg5mkOjmdZu8gmP9WLUrOWrFcjGHpxN-yxHCjDcTZSfaFTBeohbvNR4w3_004FaKswdCGYj8tBBq30GZyrjCEYY-OuAKozXYYjm1IzV9_tm36fHDrg12n6OsuLVlIKqNYXAi37gDPBTQTycuU-IbLPX4jZv8cc.

Triolo, Paul et al., *Euasia Group White Paper: The Geopolitics of 5G*, Washington, DC: Eurasia Group.

Triolo, Paul, et al., "One Company, Many Systems. US Forces Governments to Choose Sides on Huawei," *Special Report Prepared by Eurasia Group*, Washington DC, Eurasia Group, 2019.

Tuerk, Miriam, "How 5G Networks Will Change America," *Forbes*, February 27, 2019, at: https://www.forbes.com/sites/miriamtuerk/2019/02/27/how-5g-networks-will-change-america/#4466acae11b5.

© 2020 The Swedish Institute of International Affairs

Uher, Jason J. et al., “Investigating End-to-End Security in 5G Capabilities and IoT Extensions,” *The Next Wave* 21:4, p. 18. Lorenzo Pupillo, “5G and National Security. A Complex Puzzle,” *CEPS*, June 21, 2019, at: https://www.ceps.eu/5g-and-national-security/.

Umback, Rick “Huawei and Telefunken. Communications Enterprises and Rising Power Strategies,” *ASPI Strategic Insights* 135. Barton: ASPI, 2019.

Uren, Tom, “Weighing the Risks in Building a 5G Network,” *ASPI The Strategist*, Barton: ASPI, 2019.

US Department of Justice, *Deputy Attorney General Rod J. Rosenstein Announces Charges Against Chinese Hackers*, December 20, 2018, at: https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-announces-charges-against-chinese-hackers.

Wall, Matthew, “What is 5G and What Will It Mean for You?,” *BBC*, July 24, 2018, at: https://www.bbc.com/news/business-44871448.

White House, “US-Poland Joint Declaration on 5G,” *The White House*, September 5, 2019, at: https://www.whitehouse.gov/briefings-statements/u-s-poland-joint-declaration-5g/.

White House, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, Washington DC: White House Office of Trade and Manufacturing Policy, 2018.

White House, *Joint Statement from president of the United States Donald J. Trump and President of Romania Klaus Iohannis*, August 20, 2019, at: https://www.whitehouse.gov/briefings-statements/joint-statement-president-united-states-donald-j-trump-president-romania-klaus-iohannis/.

White House, *United States – Estonia Joint Declaration on 5G Security*, November 1, 2019, at: https://www.whitehouse.gov/briefings-statements/united-states-estonia-joint-declaration-5g-security/.

Worldwide Asset Management, *The New Tech War and the Geopolitics of 5G*, 2019, at: https://cworldwide.com/media/PDF/WP_2019_The_New_Tech_War_and_the_Geopolitics_of_5G.pdf.

Wu, Mark, “The “China, Inc.” Challenge to Global Trade Governance,” *Harvard International Law Journal* 57: 2, pp. 261-324, 2016.

Zaagman, Alliott, *Huawei’s Problem of Being too “Chinese”*, January 24, 2019, at: https://supchina.com/2019/01/24/huaweis-problem-of-being-too-chinese/.

Zaagman, Alliott, *Thinking About Working For a Chinese Company? First, Find Out If It’s a “Lenovo” or A “Huawei”*, October 9, 2017, at: https://supchina.com/2017/10/09/thinking-working-chinese-company-first-find-lenovo-huawei/.

Zheng, William, “China’s Shenzhen Is Using Big Data to become a Smart “Socialist Model City”,” *South China Morning Post*, Novmber 1, 2019, at: https://www.scmp.com/news/china/politics/article/3035765/chinese-city-shenzhen-using-big-data-become-smart-socialist

Zhong, Raymond, “China’s Huawei Is at Center of Fight Over 5G’s Future,” *The New York Times*, March 7, 2018, at: https://www.nytimes.com/2018/03/07/technology/china-huawei-5g-standards.html.

© 2020 The Swedish Institute of International Affairs

© 2020 The Swedish Institute of International Affairs

About UI

Established in 1938, the Swedish Institute of International Affairs (UI) is an independent research institute on foreign affairs and international relations. Any views expressed in this publication are those of the author. They should not be interpreted as reflecting the views of the Swedish Institute of International Affairs. All manuscripts are reviewed by at least two other experts in the field. Copyright of this publication is held by UI. You may not copy, reproduce, republish or circulate in any way the content from this publication except for your own personal and non-commercial use. Any other use requires the prior written permission of UI.

The Swedish Institute of International Affairs
Visiting Address: Drottning Kristinas väg 37, Stockholm
Postal Address: Box 27 035, 102 51 Stockholm
Phone: +46 8 511 768 00
www.ui.se info@ui.se Twitter: @UISweden @ResearchUI