UI paper

5/2020

Who Controls Huawei?
Implications for Europe

Tim Rühlig

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

Tim Rühlig
Research Fellow
The Swedish Institute of International Affairs

Language editing: Andrew Mash
Cover photo: TT/Shutterstock

Abstract

Europe faces pressure from both the US and China over the question of whether to exclude the Chinese technology giant Huawei from the rollout of the new generation of mobile infrastructure, better known as 5G. Proponents of a ban argue that Huawei is controlled by the authoritarian Chinese party-state and the inclusion of its equipment would provide the Chinese authorities with the ability to shut down European 5G networks and use the 5G network for political and economic espionage. Huawei counters that it is a private sector company that would not support the Chinese authorities in gaining access to European 5G infrastructure. The salience of the controversy lies in the fact that like electricity, 5G will be a critical enabler that makes possible new applications that revolutionise methods of production, and of the provision of healthcare and transport, to name just two.

From a purely technological perspective, a ban on Huawei would not be effective at increasing 5G network security. China is capable of shutting down Europe's 5G network regardless of whether Huawei equipment is included in it. Chinese cyberespionage presents a huge challenge but almost all economic or political spying is carried out by means of applications and phishing, rather than through infrastructure. Network redundancies coupled with vendor diversity and better end-to-end encryption are much more effective means of mitigating these risks.

The idea of excluding Huawei instead follows a geopolitical logic at a time when states are using economic dependencies for political purposes. The fear is that the Chinese party-state could leverage technological dominance and dependence on Huawei equipment to gain political concessions from Europe. However, this would require that Huawei functions not as a normal corporation, but effectively be controlled by the Chinese Communist Party. This paper provides a very detailed analysis of how the Chinese party-state can exercise control over the company. Huawei is a fully privately owned company, but I contend that the owners do not have complete control over it.

All this raises the question of what measures Europe should take. The United Kingdom (UK) and the European Union have drafted policies that are widely characterised as compromise proposals. This paper demonstrates that this assessment is misleading. The UK's draft decision, which is to be adopted by parliament before the summer, provides far-reaching opportunities for Huawei to participate in the rollout of 5G. The EU's "toolbox" – a legally non-binding document jointly developed by all member states, the European Commission and its cybersecurity agency, ENISA – provides a roadmap away from Huawei technology but remains open to interpretation.

EU member states should adopt a unitary interpretation of the toolbox. A complete ban on Huawei from the rollout of European 5G might not be necessary, but the EU and its member states should strive for a significant reduction in Huawei's market share.

Introduction

When the US delegation arrived at the Munich Security Conference in mid-February 2020, it had a rare bipartisan message for Europe: let us unite against China! At its core was the US call to exclude the Chinese technology giant Huawei from the rollout of the new generation of mobile infrastructure in Europe, better known as 5G. US Secretary of Defence Mark Esper called on all European Union (EU) member states to follow the US example and exclude Huawei.[1] The Democratic Speaker of the House of Representatives, Nancy Pelosi, argued that Europe had a choice between autocracy (by allowing Huawei in) or defending democracy.[2]

Like electricity, 5G is a critical enabler that could bring with it new applications and opportunities that cannot yet be imagined; it has true revolutionary potential. Apart from increasing upload and download capacities, 5G comes with ultra-low latency coupled with high reliability and offers the ability to connect a high number of devices. This will be necessary for a wide range of applications ranging from self-driving cars to a new wave of automation of production by means of mass machine-to-machine communication: 5G could permeate and change entire societies.[3]

The enormous potential of 5G comes with risks. If a malign actor were to take control of the network, it would affect almost all spheres of economic and social life. Australian and US intelligence agencies (among others) warn that such risks could materialise if Chinese technology is included in 5G infrastructure. The fear is that Chinese equipment could enable the Chinese party-state to spy on the users of the infrastructure and to shut down the mobile network entirely.[4] This could provide China with political leverage. I refer to these two challenges – espionage and sabotage through 5G infrastructure – as network security risks. Concerns over Chinese espionage and attacks on the availability of 5G infrastructure are well-grounded.

Apart from network security risks, concerns over the inclusion of Chinese 5G equipment stem from the potential for technological dependencies to develop. Recent years have witnessed a "weaponisation of economics". Trade, investment and technology have not just been about competition among commercial entities, but states considering whether and how they can utilise technological dependencies to press for political concessions. The basic idea is that a state that relies on the technology of another state will behave more favourably towards that state because it is aware of the dependencies that result from the need to maintain increasingly software-defined high technology and to further build out its critical infrastructure. I refer to this as the geopolitical challenge of technology dependencies. For this geopolitical challenge to materialise, states

[1] Mark T. Esper, "Secretary of Defense Speech. As Prepared Remarks by Secretary of Defense Mark T. Esper at the Munich Security Conference " *U.S. Department of Defense*, accessed: 2020-03-27, at: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2085577/remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security-conference/.
[2] Nancy Pelosi, "Speaker Pelosi Remarks at Munich Security Conference," *U.S. House of Representatives*, accessed: 2020-03-27, at: https://www.speaker.gov/newsroom/21420-1.
[3] Edison Lee and Timothy Chau, *Telecom Servies. The Geopolitics of 5G and IoT. Jefferies Franchise Note*, Hong Kong, Jefferies, 2017; EMF Explained Series, "5G Explained – How 5G Works," *EMF Explained*, accessed: 2019-04-16, at: http://www.emfexplained.info/?ID=25916; Matthew Wall, "What is 5G and What WIll It Mean for You?," *BBC*, accessed: 2020-03-27, at: https://www.bbc.co.uk/news/business-44871448.
[4] David Bond and James Kynge, "China Spying Risk Hits Huawei's UK Ambitions," *Financial Times*, 3 December 2018.

must control technological supply.[5] The geopolitics of technological dependencies raise the question of whether and, if so, how the Chinese party-state is controlling Huawei, which claims to be a private sector company owned by its employees.

Network security risks and the geopolitics of technological dependencies are serious concerns for Europe. However, the widely discussed exclusion of Huawei does not address the network security challenge. If anything, the exclusion of Huawei instead follows a geopolitical logic.

Since issues of network security have been discussed in depth elsewhere,[6] this paper only summarises this aspect and focuses instead on party-state control over Huawei. Given that the exclusion of Huawei is a geopolitical question, party-state control over technology companies is decisive for the question of how Europe, be it the EU or the United Kingdom (UK), should react to US demands for a ban on Huawei.

First, I briefly summarise why network security risks are severe but not decisive for the question of whether to ban Huawei from the buildout of 5G infrastructure in Europe. Next, I turn to the question of whether Huawei is controlled by the Chinese party-state and thus serves as a potential political instrument of China. Not least based on information provided by the company itself, I contend that the party-state has mechanisms that allow it to exercise control over Huawei. While network security risks do not justify a ban on Huawei, the Chinese state's control over the company could make such a decision reasonable from a geopolitical perspective. Bearing these two perspectives in mind, I review two recent developments: the UK's draft decision on the rollout of 5G technology, which is to be adopted by the British parliament before the summer, and the toolbox of recommendations jointly developed by the EU member states, the European Commission and its cybersecurity agency, ENISA. Both documents have been widely interpreted as compromises. I demonstrate that the UK's decision leaves plenty of room for Chinese vendors to participate in the rollout, and that while the EU toolbox recommends a restrictive approach, the toolbox contains some vagueness that is likely to allow EU member states to interpret the document in different ways.

This leads me to the final conclusion that if I am correct in my contention that the party-state can control Huawei and other tech giants, this should remind the EU that the issue is not just about network security, but has a geopolitical dimension. The toolbox takes this into account by considering strategic measures without ruling out the possibility that the geopolitical risks could be mitigated without a full ban of Huawei. This would require a unitary interpretation and implementation of the toolbox across the continent, which is unlikely, coupled with a diversification strategy. The latter should generate strategic access to technology, reduce the EU's dependency on Chinese technology and remove the risk of the EU having to accept political concessions due to its technological dependency. I am sceptic of whether a complete ban on Huawei is desirable, but EU member states should strive for a reduction in Huawei's market share.

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

[6] Tim Rühlig and Maja Björk, "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe," *UI Paper 1/2020*, Stockholm, The Swedish Institute of International Affairs, 2020.

Huawei: a risk for the 5G networks in Europe?

Over the past 18 months, a heated debate over 5G infrastructure deployment has developed in Europe with the Chinese tech giant Huawei at its centre. At the core of the discussions are concerns over network security. While it is not clear that 5G is generally less secure than the current 4G/LTE networks, the complexity of 5G networks poses a new security challenge. This complexity is the result of the multitude of applications and devices that will be part of future 5G networks. This is made possible by the increased use of software-defined virtualisation, which shifts sensitive operations from the core network to the edge. This makes the attack surface larger and means that a distinction between a sensitive core network technology and a less-sensitive edge and its radio access network (RAN) no long applies.[7]

The sensitivity and vulnerability of 5G networks has led to fears that the participation of Chinese vendors in the deployment of 5G could come with inherent security risks. At the heart of these concerns are two fears: Chinese sabotage of and espionage through 5G infrastructure. *Sabotage* is the most severe concern: China could gain access to European 5G infrastructure that would allow it to shut down the entire network, and thereby target the whole of European society and its economy. This "kill switch", as it is commonly known, would essentially undermine the availability of 5G networks that will be necessary for machine-to-machine communication as well as for self-driving cars or interconnected medical devices, such as pacemakers.

The risk of Chinese *espionage* describes a scenario in which China uses its access to 5G infrastructure for economic and political espionage on European companies, governments and individuals. China is already responsible for the lion's share of global cyber espionage.[8]

These two risk scenarios appear more feasible since a British evaluation centre found significant software engineering and cybersecurity problems in Huawei equipment and reported that the Chinese company is failing to resolve these challenges.[9] Despite all the reporting about a "smoking gun", however, there is no proof that China is using such vulnerabilities or that Huawei is designing backdoors.[10] This assessment has not changed even after the German newspaper *Handelsblatt* reported that the US administration had presented evidence of a smoking gun to the German authorities.[11] In the briefing, US officials argued that Huawei has had access to all mobile communication since 2009 by means of lawful interception interfaces that are included in the equipment for the

[7] Tim Rühlig and Maja Björk, "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe," *UI Paper 1/2020*, Stockholm, The Swedish Institute of International Affairs, 2020.
[8] Kadri Kaska et al., *Huawei, 5G and China as a Security Threat*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2019.
[9] Huawei Cyber Security Evaluation Centre Oversight Board, "Annual Report," *HCSEC*, accessed: 2019-08-09, at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.
[10] Reed Steveson, "How Huawei Became a Target for Governments," *Bloomberg*, accessed: 2020-03-28, at: https://www.washingtonpost.com/business/how-huawei-became-a-target-for-governments/2019/11/22/302af044-0d4f-11ea-8054-289aef6e38a3_story.html.
[11] Reuters, "Huawei Denies German Report it Colluded with Chinese Intelligence," *Reuters*, accessed: 2020-02-27, at: https://www.reuters.com/article/us-germany-usa-huawei/huawei-denies-german-report-it-colluded-with-chinese-intelligence-idUSKBN1ZS197.

purpose of law enforcement. These officials declined, however, to provide any evidence. Apart from the German Foreign Ministry, it appears that none of the German officials present at the meeting were convinced.[12] The German operator Deutsche Telekom clarified that its legal interception interfaces are not produced by Huawei but by a German company.[13] Moreover, the accusations came at a time when the US itself was under pressure because a US supplier, Cisco, had just closed vulnerabilities in its own technology, and both German and US intelligence were facing pressure for having spied on allies for decades using an encryption manufacturer they owned, Crypto AG.[14]

This lack of a smoking gun, however, should not reassure Europeans. In the light of the wide variety of use cases mentioned above, 5G will be a critical infrastructure. It would therefore be reckless only to react to what has already happened without considering risks. The risks are real and severe. The question is how to mitigate them.

The US, Australia and Japan have decided to exclude Huawei altogether from the rollout of their 5G infrastructure. Other states are more hesitant and considering different measures. Such hesitation is well justified because a ban on Huawei would not be an effective means of mitigating the network security risks. Hackers and engineers agree that China will be able to shut down European 5G infrastructure regardless of whether Huawei participates in the rollout. Moreover, most espionage is not carried out through 5G infrastructure, but through applications and phishing.[15]

At the same time, more effective means are available for mitigating network security risks. The most effective are better end-to-end encryption, which makes spying difficult; and network redundancies that increase the availability of coverage coupled with vendor diversity. Vendor diversity relies on the assumption that all 5G equipment will contain vulnerabilities, but different suppliers' equipment will come with different kinds of vulnerabilities which will impose higher cost for attackers to identify and effectively exploit them.[16] These means could be combined with improved evaluation and certification of products and processes, including source code reviews or network flow monitoring. Such actions would be of limited value,

[12] Patrick Beuth and Marcel Rosenbach, "Eine Hintertür, die nur die USA sehen," *Der Spiegel*, accessed: 2020-02-27, at.
[13] Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *Wall Stree Journal*, accessed: 2020-02-27, at: https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.
[14] ZDF, "Operation Rubikon. Wie BND und CIA die Welt belauschten. Fontal 21 vom 11. Februar 2020," *ZDF*, accessed: 2020-03-28, at: https://www.zdf.de/politik/frontal-21/operation-rubikon-100.html.
[15] Jan-Peter Kleinhans, *5G vs. National Security. A European Perspective*, Berlin, Stiftung Neue Verantwortung, 2019. Compare to reports on previous Chinese hacks: PwC, "Operation Cloud Hopper," *PwC*, accessed: 2020-03-28, 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*, accessed: 2020-03-28, at: https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/; FireEye, "Mandiant APT1. Exposing One of China's Cyber Espionage Unites," *FireEye*, accessed: 2020-03-28, at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; Thomas Brewster, "Chinese Trio Linked to Dangerous APT3 Hackers Charged with Stealing 407GB of Data from Siemens," *New York*, accessed: 2020-03-28, at: https://www.forbes.com/sites/thomasbrewster/2017/11/27/chinese-hackers-accused-of-siemens-moodys-trimble-hacks/.
[16] Deutscher Bundestag, "Experten gegen Ausschluss von Anbietern beim Mobilfunkstandard 5G. 22 November 2019," *Deutscher Bundestag*, accessed: 2020-03-28, at: https://www.bundestag.de/dokumente/textarchiv/2019/kw46-pa-auswaertiges-5g-665414.

however, since evaluation is made more difficult by the need for extensive maintenance work on the software through regular and extensive updates and security patches, as well as the large amounts of data flows. However, coupled with end-to-end encryption, redundancies and vendor diversity, they could contribute to network security, particularly if remote access for maintenance work is made impossible.[17]

In sum, a ban on Huawei would not effectively address the risks of sabotage or espionage. Instead, such exclusions decrease Huawei's technological influence in the world and reduce the company's global market share. From a purely network security perspective this does not help. If the geopolitical considerations of states aiming to utilise technological dependencies to extract political concessions are taken into account, a reduced market share could harm Chinese global political ambitions. A precondition for such a conclusion would be, however, that Huawei is controlled by the Chinese party-state and can be utilised by the Chinese Communist Party (CCP).

Technical dependency and the issue of party-state control over Huawei

Underlying the geopolitical dimension of the debate over Huawei is the fear that the Chinese party-state could leverage European dependence on Huawei technology to extract political concessions. This perspective implies that Huawei cannot be treated just like any other private sector company that seeks economic profit, but should be regarded as a political tool under the control of China's authoritarian rulers.[18] Huawei has countered this view by emphasising that the company is almost fully owned by its employees and is not a state-owned enterprise (SOE) like ZTE, another Chinese technology firm. Are Huawei's critics getting it right or is the company victim of an anti-Chinese witch hunt?

While at first glance Huawei's line of defence appears convincing, there are also reasons for doubt. It is true that the company is privately owned by its employees, but there is reason to believe that ownership does not come with control, as I discuss below. While there is also little reason to believe that the company has a particular interest in serving political purposes, Huawei has not only profited from party-state support, but is operating in a specific political, legal and economic environment that makes it impossible for the company to be fully independent. At least four aspects lead me to question Huawei's independence: (a) the general level of independence of privately owned companies in China; (b) the legal environment, particularly China's Intelligence Law; (c) party-state support for Huawei; and (d) the governance structure of the company itself.

(a) The role of privately owned companies in China. The widespread distinction between privately owned enterprises (POEs) and state ownership is not decisive in China. It is not ownership but the issue of "state capture" that is pivotal. If supported by the party-state, SOEs and POEs enjoy equal treatment with regard to access to the market, state subsidies, procurement and the exercise of political guidance. Milhaupt

[17] for a more detailed discussion of 5G network security and adequate measures to mitigate the risks see Tim Rühlig and Maja Björk, "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe," *UI Paper 1/2020*, Stockholm, The Swedish Institute of International Affairs, 2020.

[18] Rick Umback, *Huawei and Telefunken. Communications Enterprieses and Rising Power Strategies. ASPI Strategic Insights 135*, Barton, ASPI, 2019.

and Zheng have rightly pointed out that "Chinese state capitalism is closely associated with state capture. That is, large firms in China – whether SOEs, POEs, or ambiguous state-private blends – survive and prosper precisely because they have fostered connections to state power and have succeeded in obtaining state-generated rents. As a result, large firms in China exhibit substantial similarities in their relationship with the state in ways that distinctions based on corporate ownership simply do not pick up".[19]

POEs and the party-state are interwoven. A large proportion of the economic elite holds positions within the CCP. Based on publicly available information, 95 of the top 100 private sector firms and eight of the top ten internet firms have a founder or de facto controller who is currently or was formerly a member of a central or local party or party-controlled state organ.[20] These figures are based on publicly available data, and are thus likely to be a conservative calculation. The days when the CCP stood in opposition to capitalism and entrepreneurs are long gone. POEs also directly profit from subsidies. When the privately owned Geely acquired the Swedish car company Volvo from Ford in 2010, for example, local governments from north-east China and the Shanghai area financed a large proportion of the $1.5 billion purchase.[21] There is control over interest rates and the state-dominated banking sector at times provides loans at below market prices, while preferential treatment in procurement and public listings as well as the protection of regional or even national monopolies in combination with corruption and coterie preserve a high level of state control over the entire economy, including POEs. Large companies in particular – regardless of ownership – as well as those in strategic sectors profit from state support, which comes with significant party-state influence. Huawei is a national champion operating in a particularly critical sector.

Following an official request, Huawei has confirmed to the author of this paper that party organisations exist within the company in accordance with Chinese law. The company has provided assurances that party organisations have no influence on the company's business operations and that it is run by an independent management team. The party organisations are mainly responsible for educating employees. The general findings on the deep linkages between the economic and political elites, however, call into question whether such differentiation is adequate in the context of China's political economy.

(b) The legal environment in China. China lacks an independent judiciary. While the CCP government speaks of strengthening the role of law in its governance, it follows a rule *by* law principle and does not intend to implement the rule *of* law. The CCP has an essentially instrumentalist understanding of law. Law is seen not as a constraint on power, but as a means of power. This means that legal certainty does not exist in areas of crucial political importance. Hence, laws do not provide reassurance against political interference in the business operations of Chinese companies.

In the context of the Huawei debate, several laws, in particular China's Intelligence Law, raise even further doubts about whether the law could shield private sector companies from political interference. Article 7 of the

[19] Curtis J. Milhaupt and Wentong Zheng, "Beyond Ownership. State Capitalism and the Chinese Firm," *The Georgetown Law Journal* 103: 3, 2015, pp. 665-722.
[20] Curtis J. Milhaupt and Wentong Zheng, "Beyond Ownership. State Capitalism and the Chinese Firm." *The Georgetown Law Journal* 103: 3, 2015, pp. 665-722.
[21] Michael Wines, "China Fortifies State Businesses to Fuel Growth," *CNBC*, accessed: 2020-03-28, at: https://www.cnbc.com/id/38910346.

Intelligence Law enacted in 2017 and amended in 2018 requires any organisation and citizen to "support, assist in and cooperate in national intelligence work".[22] Confronted with this law, Huawei refers to a legal opinion that the company would not need to cooperate with Chinese intelligence. Not least in the light of the lack of the rule of law in China, but also given the clarity of the Intelligence Law, this legal opinion does not provide any substantial reassurance that Huawei could decline to cooperate with Chinese intelligence, even if the company wanted to do so.[23]

(c) Party-state support for Huawei.
Scepticism over Huawei's independence from party-state control does not just stem from the political, legal and economic environment in which it operates. An analysis of organisational and personal linkages between the CCP and the Chinese security apparatus on the one hand and the company on the other indicates that Huawei is no exception to the general rule. Huawei's founder, Ren Zhengfei, is widely believed to have a past in China's People's Liberation Army. His daughter and the company's Chief Financial Officer, Meng Wanzhou, is suspected to have held a public affairs passport.[24] A widely discussed and controversial analysis of the CVs of leading Huawei engineers found a large overlap with China's security apparatus.[25] Anecdotal evidence suggests, however, that similar overlaps exist between US high-tech firms and the US intelligence services.

While there is no doubt that Huawei can compete with Western technology companies on both quality and price, a recent *Wall Street Journal* report indicated that the company has achieved its current position by receiving as much as $75 billion in tax breaks, financing and cheap resources in the past 25 years. According to the report, Huawei profited from $46 billion in cheap loans, credit lines and other support from state lenders alone. Between 2008 and 2018, the company saved $25 billion in taxes due to state incentives to promote the tech sector. In addition, the company would have profited from cheap loans for its customers provided by Chinese banks. The China Development Bank and the Export-Import Bank of China are reported to have lent $30 billion to Huawei customers.[26] Already in 2013, Nathaniel Ahrens was pointing out the irony of the SOE ZTE having to turn to the equity markets while the privately owned Huawei relied on state funds.[27] Huawei has denied the accusations in the *Wall Street Journal* report.

In the light of the multitude of reports of party-state assistance for the company, it seems very likely that Huawei has profited from massive party-state support. All this is not to say that Western technology companies do not receive financial support

[22] Peking University Law Database, "National Intelligence Law of the People's Republic of China. 2018 Amendment. Effective," *PKULaw*, accessed: 2020-03-28, at: https://en.pkulaw.cn/display.aspx?cgid=313975&lib=law.
[23] Donald Clarke, "The Zhong Lun Declaration on the Obligations of Huawei and Other CHinese Companies under Chinese Law," *SSRN*, accessed: 2020-03-28, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354211.
[24] Ashley Feng, "We Can't Tell if Chinese Firms Work for the Party," *Foreign Policy*, accessed: 2019-02-15, at: https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/.
[25] Christopher Balding, "Huawei Technologies' Links to Chinese State Security Services," *SSRN*, accessed: 2019-07-28, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726.
[26] Chuin-wei Yap, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, accessed: 2020-02-09, at: https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.
[27] Nathaniel Ahrens, *China's Competitiveness. Myth, Reality, and Lessons for the United States and Japan. Case Study: Huawei*, Washington D.C., CSIS, 2013.

from their governments. Both Finland's Nokia and Sweden's Ericsson, for example, benefit from export credits. The scope of their government support, however, falls far short of Huawei's.

(d) Huawei's governance structure. Huawei's ownership and governance structures are highly complex. This has sparked rumour and speculation across the West's media as well as academic and policy debate over who controls the company. Three reports in particular have contributed to the present understanding of Huawei's governance structure. Duchâtel/Godement and Seely et al. claim that Huawei's ownership structure is based on a trade union. Both papers argue that since trade unions are under the control of the CCP, it is the Party that has the ultimate say over the tech giant. Where both papers fall short, however, is in terms of a detailed description *how* the CCP exerts its control over the company.[28] Balding/Clarke, in turn, reviews publicly available documents and concludes that control is *not* carried out through a trade union because the entity that formally owns Huawei is not the trade union for Huawei Technologies.[29] At first glance, Balding/Clarke's assessment is convincing. For the purposes of this paper, I reached out to the company to ask for clarification. The results are surprising as the information provided by Huawei gives an indication of how difficult it is to run an independent company in such a crucial sector in China. Balding/Clarke's assumptions are refuted. While this paper leaves open a few questions, it provides one of the most detailed analysis of the governance structure of Huawei that to my knowledge has been published so far.

Most fundamental to the widespread confusion is that there is more than one "Huawei" entity. Most of the technology discussed is produced by an entity known as "Huawei Technologies", which is fully owned by another entity, "Huawei Holding". Huawei Holding, in turn, is owned by the Trade Union of Huawei Holding and the founder of the company, Ren Zhengfei (see figure 1).

[28] 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.

[29] Christopher Balding and Donald Clarke, "Who Owns Huawei?," *SSRN*, accessed: 2020-03-28, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669.

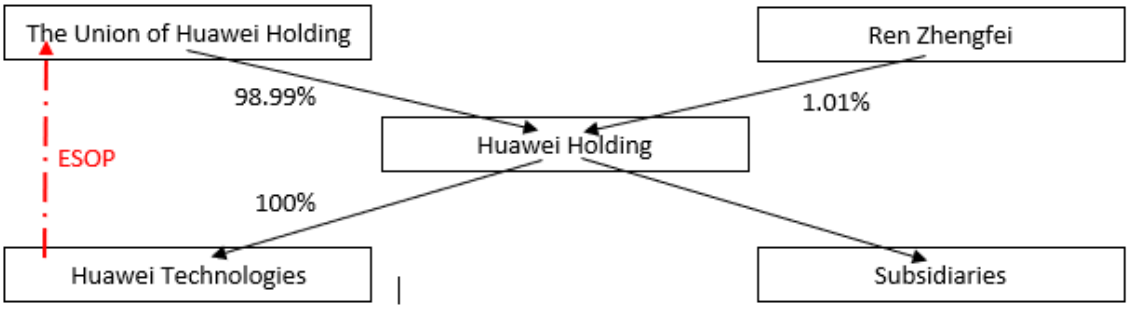


Figure 1: Ownership structure of Huawei. Source: Author's own graphic, based on information obtained from Huawei

Of crucial importance is the status of the Union of Huawei Holding, which is registered with the Shenzhen Federation of Trade Unions and operated and managed in accordance with China's Trade Union Law. Academic analyses of the official trade union system (with the All-China Federation of Trade Unions, of which the Shenzhen Federation of Trade Unions is a member, at its core) have underlined that there are no independent trade unions in China.[30] They are all controlled by the CCP and Article 4 of the Trade Union Law explicitly requires them to "insist on the leadership of the Chinese Communist Party".[31] The nature of the Union of Huawei Holding as the owner of the Huawei Company group has led observers to argue that the CCP controls Huawei Holding and by extension also Huawei Technologies.

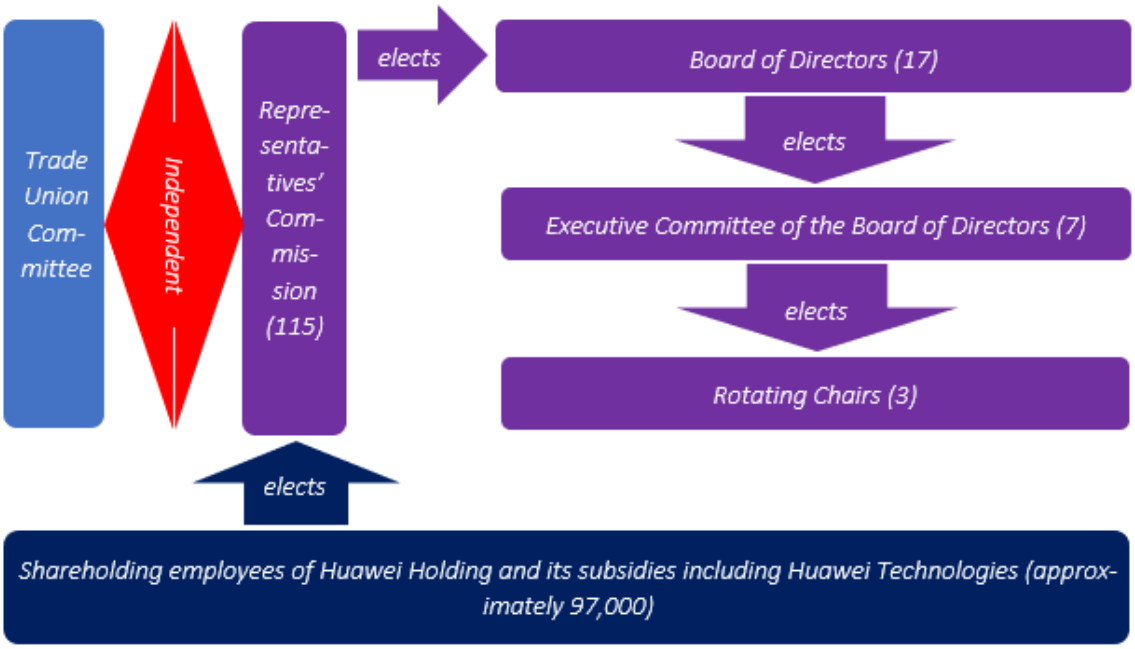
Huawei has rejected this claim. It argues instead that the Union of Huawei Holding is a single legal entity with two completely separate roles. On the one hand, the Union serves as a Trade Union with a Trade Union Committee. On the other hand, and completely separate from its first role, a so-called Employee Stock Ownership Plan (ESOP) is run through the Union. Under the ESOP, the employees of Huawei Technologies have – under certain conditions – the opportunity to purchase shares in Huawei Holding. Currently, around 97,000 employees hold more than 22 billion shares in Huawei Holding. It is important to note that only around half of Huawei's 190,000 employees participate in the ESOP. Participation depends on work performance. Non-Chinese employees of Huawei are not eligible to participate in ESOP. Huawei justifies this with reference to capital account controls. In addition, shareholders cannot sell their shares to non-Huawei employees.

Shareholders have the right to elect a Representatives' Commission comprising 115 representatives, which in turn elects the Board of Directors and the Supervisory Board. Both these vote for their respective Executive Committees. The Executive Committee of the Board of Directors has seven members and is particularly important since three of them take the role of rotating chair (see figure 2). This complex structure is necessary because China's

[30] 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.

[31] International Labour Organization, "Trade Union Law of the People's Republic of China. 2009 Amendment. Effective," *ILO*, accessed: 2020-03-28, at: https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/30352/118793/F1165849917/CHN30352%202.pdf.

Company Law limits the number of shareholders that non-listed limited liability companies such as Huawei can have.



Graph 2: Huawei's governance structure. Source: Own graphic, based on information obtained from Huawei.

Huawei claims that, even though it governs the Union of Huawei Holding, the Trade Union Committee has no power over the Representatives' Commission. Huawei is explicit that both entities are governed by different laws (the Trade Union Law and Chinese Company Law). If this is correct, the nature of the Union of Huawei Holding as a trade union does not give the party-state control over the company, as claimed by Duchâtel/Godement and Seely et al.[32]

Confronted with Huawei's statements in interviews conducted for this study, some observers doubt the claims that the Trade Union Committee does not have control over the Representatives' Commission even though it is in charge of running the trade union of Huawei Holding. They argue that it is implausible that the governing body of an entity would control only part of the organisation.[33]

While it is difficult to judge from the outside whether the company or its critics are correct, another element in the complex governance structure is remarkable: the nomination process for the election of the Representatives' Commission. For the process, the company is divided into nine sectors each of which "undergoes a democratic process of organising, discussing and agreeing on a proposed list of members for their own nomination

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

[33] Author telephone interviews with experts investigating Huawei, December 2019-March 2020.

team". This is a decisive loophole in Huawei's structure. Following a request for clarification of this process for this paper, the company responded that formation of the nomination team, which usually has 7–9 members, varies across sectors. In some sectors, a group of 40 to 50 people discusses the composition of the nomination team, while in others it is just 12–13 members of the sector. Either way, only "key employees, experts and line managers who have worked at Huawei for many years" are involved, according to the company. According to official statements to the author of this paper, Huawei has no specific rules on who can participate or how the process of forming the nomination team works in each sector. This is critical because nomination teams have far-reaching competences. First and foremost they select an initial list of 500 candidates based on relatively vague criteria. Even though this is not proof of party-state influence, the fact that only some employees influence such a crucial nomination process and that the company lacks clear criteria for the composition of nomination teams opens the door for political influence.

It is not only the procedural criteria for the formation of nomination teams that are vague, so are the criteria the nomination teams use to nominate candidates. According to the company, candidates must be current ESOP beneficiaries, they must have worked at Huawei for at least eight years, they must have exhibited outstanding work performance and they must keep contributing to the company. In addition, sectors may add specific criteria. Work performance, according to Huawei, refers to an employee's "spirit of dedication" and "passion and commitment to work" as well as to "tangible contributions to the company through day-to-day work, including having an in-depth understanding of business related to the job, achieving the major goals of the job, and providing constructive recommendations and independent assessment of Huawei's future development". Huawei also emphasises that many senior managers in US tech companies began as engineers and rose through the ranks. Sustained contributions to the company are assessed using such factors as: a candidate's contributions and accomplishments since joining Huawei; a candidate's dedication; and a candidate's willingness to develop and learn new business knowledge that can help gain the "competency required to address the company's future needs for business development".

In a next step, the nomination team narrows the resulting list of more than 500 potential candidates down to 109 names, based on presentations and questionnaires. Again, the assessment criteria are relatively vague and similar to those used in the first round. The questionnaires aim to assess the determination and passion of the potential candidate and their intentions if elected, and to obtain a summary of past achievements.

After the nomination process is completed, all the ESOP participants can elect 83 representatives from a list of 109 candidates nominated to the Representatives' Commission. A further 32 members of the Commission are ex-officio, making up the remaining seats of the 115-member Commission. This clearly demonstrates that the main control over Huawei does not lie with the employees of the company, who can only choose 83 people from a pre-selected list of 109 candidates, but with the nomination teams that hand-pick these people using vague criteria. Whoever wants to control Huawei needs to control the nomination teams. There are no adequate checks in place to ensure that it is not the Chinese Communist Party and its

organisations within the company that are the ones exercising such control.

It is important to note that Huawei claims that membership of the Chinese Communist Party "does not affect [...] the chances of becoming a Representative" or the results of any other election in the company. Huawei states that it "never checks whether or not employees are members of the Chinese Communist Party; nor do we need to do so. The Chinese Communist Party organisation does not participate in the nomination or election process of the Representatives' Commission, or extend any influence over this process". The challenge is, however, that Huawei has no mechanisms in place to guarantee that the party does not interfere. In the light of the close interlinkages between the economic and political elites in China more generally, as briefly summarised above, it appears improbable that the nomination teams are not dominated by party members. Given the widespread congruence of the political and economic establishment in China, it might not even appear unnatural or remarkable to anyone within Huawei or in China that party membership and nomination team participation should strongly correlate. Some room for speculation remains, but the loopholes are obvious.

What sparks further suspicion of the process is that none of the Huawei employees I have talked to was aware of the nomination process, even though it turns out that real power of selection lies with the nomination teams. Their composition was also apparently unclear to all the Huawei employees I asked about it. Some did not even know that there were nomination teams. While this does not prove that Huawei is controlled by the party-state, the fact that it is such an opaque and vague structure raises suspicion. What it makes exceedingly likely, however, is that contrary to Huawei's claims, employees do not effectively control the company. They can only elect pre-selected candidates and are not aware of how they are nominated. Ownership and control are separate.

In the light of these four factors – the general level of independence of the POEs, the legal environment and Intelligence Law, state support for Huawei and the company's governance structure – it is very difficult to reject the claims of Huawei critics that the company is more than just a privately run company striving for economic profit. This is, however, nothing specific to China or to Huawei. State influence over private sector companies exists in Europe too. France is famous for such linkages, and even Volkswagen is effectively governed by the German public authorities by means of a specific law (often referred to as the "VW law"). What makes Chinese party-state control over Huawei distinct is not the control as such, but that the Chinese tech giant produces equipment for critical digital infrastructure.

Europe reacts to the "Huawei challenge"

The complex picture of network security risks coupled with geopolitical concerns over technology dependency and party-state control raises questions about what Europe's response should be. Analytically, it is possible to differentiate between two different types of response.[34] One approach focuses on national security and geopolitics using political criteria. This is what underlies the "Prague Proposals" developed in 2019 by a group of Western states.[35] The second

[34] Tim Nicholas Rühlig et al., *5G and the US–China Tech Rivalry – a Test for Europe's Future in the Digital Age. SWP Comment 29*, Berlin, SWP, 2019.

[35] Government of the Czech Republic, "Prague 5G Security Conference Announced Series of Recommendations. The Prague Proposals," *Czech*

approach focuses on network security and instead considers technical measures to contain primarily technological risks. This distinction helps to understand the responses of different states. In reality, however, most states adopt a combination of both perspectives, while leaning towards either national security/geopolitics or network security/cybersecurity. Two recent and particularly important examples leaning in opposite directions are the decision taken in the UK and the EU's toolbox.

In the absence of evidence of network security challenges, the UK published its decision at the end of January 2020, mainly, but not exclusively, adopting a network security/cybersecurity perspective. Initially, the adoption of the government decision by the parliament was scheduled for early summer 2020; in wake of COVID-19, not only the timetable is questionable, but support among members of the British parliament is dwindling as negative perception of China in the context of the coronavirus is on the rise. In fact, British officials claim that they believe they can mitigate the network security risks. *The Economist* assessed the decision in a similar way to most media outlets, writing "to little surprise, a compromise".[36] However, this misrepresents the British decision, which essentially grants far-reaching access to Huawei. The British government draft comprises:

- an exclusion of high-risk vendors' (read: Huawei) technology from the Core Network;
- an exclusion of high-risk vendors' technology from the Radio Access Network close to critical facilities such as nuclear power plants and military bases;
- a reduction in Huawei's share of the remaining market to 35%.

The British decision to reduce Huawei's market share to no more than 35% is a response to the risk of technology dependency. Hence, the UK is also considering geopolitics to some extent.

The distinction between Core Network and Radio Access Network, however, is puzzling and can only be a temporary solution. In this respect, it is important that 5G will be rolled out in two phases. In a first step, 4G/LTE networks will be "updated" to "non-stand-alone 5G". The full range of 5G applications, however, requires "stand-alone" 5G that requires replacement of the existing Core Network technology. In stand-alone 5G, the distinction between Core and Radio Access Network becomes irrelevant since more and more functions carried out in the Core Network of 4G/LTE will be performed at the edge of the Radio Access Network (see above). For this reason, the British distinction between Core Network and Radio Access Network appears antiquated and will allow Huawei to deliver sensitive parts of the stand-alone 5G network in the UK. Commenting on the British decision, Simeon Gilding, a former Australian signals intelligence official, noted that:

But with [stand-alone] 5G, all network functionality is virtualised and takes place within a single cloud environment. That means there is no physical or logical separation between the core and edge of the network. A recent Financial Times *editorial approvingly cites testimony to UK parliamentary hearings last year that 'the*

Republic, accessed: 2019-09-10, at: https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[36] The Economist, "Britain Takes a Third Way on 5G with Huawei," *The Economist*, accessed: 2020-02-27, at: https://www.economist.com/britain/2020/01/28/britain-takes-a-third-way-on-5g-with-huawei.

distinction [between core and edge] would still be valid in Britain, however; geographical differences meant its networks would be designed differently from Australia's'. I struggle to understand what this means. […] If it means the relative size of the United Kingdom allows its telcos to avoid distributing sensitive data and functions right to the edge of the network, I'm still not convinced. Geography is not a factor in how core–edge works.[37]

Not surprisingly, Huawei welcomed the British decision and the US voiced its disappointment. At the same time, the Trump administration fell short of its previous threat to reduce intelligence cooperation with the UK, but instead announced it would need to develop alternative ways of intelligence sharing.[38] This could turn out to be disastrous for the US since it calls into question its threats against other states. Observers discuss whether Canada could follow the British example. Other states, primarily in Asia, such as India, Indonesia, Malaysia or Singapore, have already decided to allow Chinese vendors to participate in their 5G deployment.[39]

The European Union, by contrast, appears to be adopting a more Huawei-critical position. The "toolbox" issued by the Network and Information Systems (NIS) Cooperation Group, which comprises representatives of all member states, the European Commission and the EU's Cybersecurity agency ENISA, reads like a roadmap away from Huawei technology – although it leaves some room for interpretation.[40]
Most crucially, the EU's toolbox explicitly states that not only technological, but also strategic (read: geopolitical) concerns should drive the European approach, which requires a combination of technological and non-technological means to mitigate. "Technical measures" are supplemented by "strategic measures" and "supporting actions". In essence, the toolbox contains

- measures to strengthen network security by means of imposing requirements on mobile network operators, such as stricter access controls, monitoring and limitations on the outsourcing of sensitive functions and maintenance work;
- an assessment of the risk profile of vendors;
- restrictions on suppliers considered to be high risk, including their exclusion from critical and sensitive parts of the 5G network, which explicitly includes more than just the Core Network;
- a diversification policy to include several vendors, which aims to avoid dependencies and lock-in effects with single suppliers, in particular high-risk suppliers.

Between the lines, the toolbox goes even further, particularly highlighting the effectiveness of non-technological measures. This places the EU toolbox closer to the national (or better, European) security/geopolitics perspective mentioned

[37] Simeon Gilding, "5G Choices. A Pivotal Moment in World Affairs," *ASPI*, accessed: 2020-02-27, at: https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/.
[38] Nikos Chrysoloras and Richard Bravo, "Huawei Deals for Tech Will Have Consequences, U.S. Warns EU," *Bloomberg*, accessed: 2019-04-11, at: https://www.bloomberg.com/news/articles/2019-02-07/huawei-deals-for-tech-will-have-consequences-u-s-warns-eu.
[39] James Crabtree, "Asia Must Step Up Tech Security as it Hands Huawei 5G Green Light," *Nikkei Asia*, accessed: 2020-02-27, at: https://asia.nikkei.com/Opinion/Asia-must-step-up-tech-security-as-it-hands-Huawei-5G-green-light.
[40] NIS Cooperation Group, *Cybersecurity of 5G Networks. EU Toolbox of Risk Mitigation Measures. CG Publication 01/2020*, Brussels, European Commission, 2020.

above. Another indication that the EU takes a rather tough approach is that it is explicit about the fact that the sensitivity of the 5G network – particularly standalone 5G – cannot be restricted to the Core Network but includes the Radio Access Network. This technologically well-grounded line of argument declares all essential parts of the standalone 5G network sensitive and subject to particularly restrictive measures. In a recent assessment, Janka Oertel concluded: "[The Roadmap] suggests that member states should consider exclusions and restrictions within normal cycles of replacement, thus creating a transition period to mitigate the economic impact of replacing existing kit from Chinese vendors".[41]

Unsurprisingly, the US has voiced its appreciation of the document, calling on the EU member states to treat the full 5G network as critical infrastructure.[42] Huawei, for its part, has also reacted positively to the document.[43] Judging from private conversations with the company, this seems not to reflect the fact that the company is particularly happy with the outcome, but the room that Huawei sees the toolbox as leaving for EU member states to interpret the document.[44] In recent weeks, Huawei seems to acknowledge that the outcome is negative for the company. In particular, it considers legal means in response to the threat of a ban, particularly drawing WTO and the role of the non-discrimination principle (most-favoured national principle and national treatment), rules on import restrictions as well as exceptions on grounds of regional integration and national security.[45]

While the toolbox has been developed by all member states, making it difficult for them not to implement it in some form or another, the document is legally non-binding. Even though the toolbox reads as a rather tough statement, Huawei's hopes might not be unfounded. The member states participating in the NIS Cooperation Group apparently do intend to adopt different policies.[46]

An exemplary case of ongoing controversial discussions is Germany. The decision on whether effectively to exclude Huawei (it will never explicitly be called a ban) remains open even after the conservative group in the German parliament adopted a compromise paper. The conservative party CDU remains split.[47] Other parties in the German parliament, including the Social Democrats which form a government with the conservatives, have adopted a more Huawei-critical position.

Other EU member states have clearer positions, although they differ. Poland and the Czech Republic are likely to effectively ban Huawei. Portugal and Hungary are at

[41] Janka Oertel, "On 5G, Brussels Is Up to the Job," *European Council on Foreign Relations*, accessed: 2020-02-27, at: https://www.ecfr.eu/article/commentary_on_5g_brussels_is_up_to_the_job.
[42] Michael R. Pompeo, "United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers," *U.S. Department of State*, accessed: 2020-02-27, at: https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/.
[43] Stuart Lau, ""Better Than We Hoped For", as UK, EU Leave Door Partially Open for Chinese Tech Firm Huawei," *South China Morning Post*, accessed: 2020-02-27, at: https://www.scmp.com/news/china/diplomacy/article/3048285/better-we-hoped-uk-eu-leave-door-partially-open-chinese-tech.
[44] Author conversations with representatives of Huawei, several cities, February 2020.
[45] Thomas Voland and Michel Petite, "Cybersecurity Measures and WTO Law," *Europäische Zeitschrift für Wirtschaftsrecht* 23: 8, 2020, pp. 218-229.
[46] Author interviews with EU officials, several cities, February 2020.
[47] CDU/CSU Fraktion im Deutschen Bundestag, *Deutschlands digitale Souveränität sichern. Maßstäbe für sichere 5G-Netze setzen*, Berlin, Unions Fraktion im Bundestag, 2020.

the other end of the spectrum, and it is highly unlikely that they will exclude the Chinese tech company from 5G rollout.

At the same time, however, the EU toolbox also contains measures that the European Commission is entitled to take without the explicit consent of the member states. While network security as part of national security remains within the competence of the member states, the toolbox explicitly refers to technology dumping which can be addressed by means of anti-dumping and subsidy measures, EU competition law, procurement rules and investment screening. The toolbox explicitly references the European Commission's potential to assist vendor diversification and secure a sustainable supply chain that avoids dependencies and lock-in effects, and the use of investment screening. Even some vague indication of an active industrial policy coupled with an emphasis on technical standardisation further enriches the European Commission's tools. Quite a few such measures lie within the autonomous competence of the European Commission and could significantly reduce Huawei's market share. Member states must have reported to the European Commission on the implementation of the toolbox by 30 April 2020, and by end of June (unless the COVID-19 crisis delays the process) a report will reflect on the state of implementation in each member state. This will be followed by a period to consider effectiveness. If the review is not positive, the European Commission could decide to take action in the fields where it has sole competence.

Policy implications

The debate over the rollout of 5G has two dimensions that are often mixed up. Network and cybersecurity risks are more severe in the light of the wide range of uses that 5G offers in contrast to 4G/LTE technology. An appropriate European response would tackle network security issues by technical means rather than a ban on Huawei. Better end-to-end encryption, redundancy and vendor diversity will be the most important, albeit costly measures to implement.

Separate from such technological considerations, Europe should address the geopolitical concerns over technology dependence. It is likely that the Chinese party-state controls Huawei to such an extent that it could leverage technological dependencies to obtain political concessions. The challenge is not so much the control, but would arise if Europe chooses to base its critical digital infrastructure to any great extent on Huawei's equipment. The EU's toolbox acknowledges this and is a step in the right direction.

An outright ban on Huawei would contradict the goal of vendor diversity, particularly with regard to the Radio Access Network which is currently supplied by only three firms: Huawei, Nokia and Ericsson. Europe's technological dependency on Huawei and other Chinese equipment is currently very high. The most reasonable goal in balancing cybersecurity and geopolitical challenges is thus a significant reduction in Huawei's market share, rather than an outright ban. This will require a diversification of supply in terms of production and the underlying patents.[48] The EU should avoid overdependence on any foreign actor – not just Chinese companies, but also wherever possible with regard to US suppliers. The suggestion by US Attorney General William Barr that the

[48] Tim Rühlig and Maja Björk, "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe," *UI Paper 1/2020*, Stockholm, The Swedish Institute of International Affairs, 2020.

US should buy Nokia and Ericsson is contrary to EU interests.[49] By contrast, a strengthening of both companies, not least by means of investment in R&D – as proposed by Robert Blair, the White House Special Representative for International Telecommunications Policy – is a constructive way forward.

The EU toolbox has introduced a number of technical and non-technical criteria for assessing the risks associated with technologies and vendors. This is the right approach and requires further elaboration as well as unitary interpretation and implementation across the continent. Non-technical criteria need to take account of geopolitical factors such as security alliances and the legal environment. Transparency over control of the company and the extent of subsidies is another reasonable criterion.

Europe will need to make sure its course is in conformity with international law, including WTO law. A cap of market share is particularly difficult if based on exceptions of regional integration and national security.[50] Hence, a variety of instruments as considered by the EU is necessary including competition law.

The EU's NIS Cooperation group and the European Commission in particular are up to the job. What is needed now is a unitary and strategic implementation of the EU's toolbox by all member states that takes into consideration both cybersecurity and geopolitical risks. The goals are clear: increasing the cost of attacks on Europe's critical 5G network (cybersecurity) regardless of vendor and the reduction of technological dependencies on any non-European power, including China.

[49] Recent reports indicate that Nokia rather than Ericsson could be target of a US acquisition. See for example Jim Osman, "Trump's 5G China Security Deadline Will Force Nokia M&A," *Forbes*, accessed: 2020-04-27, at: https://www.forbes.com/sites/jimosman/2020/04/23/donald-trump-5g-us-china-security-nokia-merger-google/#447836f51b27.

[50] Thomas Voland and Michel Petite, "Cybersecurity Measures and WTO Law." *Europäische Zeitschrift für Wirtschaftsrecht* 23: 8, 2020, pp. 218-229.

Sources

Ahrens, Nathaniel, *China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan, Case Study: Huawei*, Washington DC, CSIS, 2013.

Balding, Christopher, "Huawei Technologies' Links to Chinese State Security Services," *SSRN*, accessed: 2019-07-28, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726.

Balding, Christopher, and Donald Clarke, "Who Owns Huawei?," *SSRN*, accessed: 2020-03-28, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669.

Barrett, Brian, "How China's Elite Hackers Stole the World's Most Valuable Secrets," *Wired*, accessed: 2020-03-28, at: https://www.wired.com/story/doj-indictment-chinese-hackers-apt10/.

Beuth, Patrick, and Marcel Rosenbach, "Eine Hintertür, die nur die USA sehen," *Der Spiegel*, accessed: 2020-02-27, at: https://www.spiegel.de/netzwelt/netzpolitik/huawei-und-die-spionage-vorwuerfe-eine-hintertuer-die-nur-die-usa-sehen-a-c9c40afd-51a3-43d3-a853-75d1fcdd1946.

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

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

Brewster, Thomas, "Chinese Trio Linked to Dangerous APT3 Hackers Charged with Stealing 407GB of Data from Siemens," *New York*, accessed: 2020-03-28, at: https://www.forbes.com/sites/thomasbrewster/2017/11/27/chinese-hackers-accused-of-siemens-moodys-trimble-hacks/.

Bundestag, CDU/CSU Fraktion im Deutschen, *Deutschlands digitale Souveränität sichern. Maßstäbe für sichere 5G-Netze setzen*, Berlin, Unions Fraktion im Bundestag, 2020.

Chrysoloras, Nikos, and Richard Bravo, "Huawei Deals for Tech Will Have Consequences, US Warns EU," *Bloomberg*, accessed: 2019-04-11, at: https://www.bloomberg.com/news/articles/2019-02-07/huawei-deals-for-tech-will-have-consequences-u-s-warns-eu.

Clarke, Donald, "The Zhong Lun Declaration on the Obligations of Huawei and Other CHinese Companies under Chinese Law," *SSRN*, accessed: 2020-03-28, at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3354211.

Crabtree, James, "Asia Must Step Up Tech Security as it Hands Huawei 5G Green Light," *Nikkei Asia*, accessed: 2020-02-27, at: https://asia.nikkei.com/Opinion/Asia-must-step-up-tech-security-as-it-hands-Huawei-5G-green-light.

Deutscher Bundestag, "Experten gegen Ausschluss von Anbietern beim Mobilfunkstandard 5G. 22 November 2019," *Deutscher Bundestag*, accessed: 2020-03-28, at: https://www.bundestag.de/dokumente/textarchiv/2019/kw46-pa-auswaertiges-5g-665414.

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

EMF Explained Series, "5G Explained: How 5G Works," *EMF Explained*, accessed: 2019-04-16, at: http://www.emfexplained.info/?ID=25916.

Esper, Mark T., "Secretary of Defense Speech. As Prepared. Remarks by Secretary of Defense Mark T. Esper at the Munich Security Conference," *US Department of Defense*, accessed: 2020-03-27, at: https://www.defense.gov/Newsroom/Speeches/Speech/Article/2085577/remarks-by-secretary-of-defense-mark-t-esper-at-the-munich-security-conference/.

Feng, Ashley, "We Can't Tell if Chinese Firms Work for the Party," *Foreign Policy*, accessed: 2019-02-15, at: https://foreignpolicy.com/2019/02/07/we-cant-tell-if-chinese-firms-work-for-the-party/.

FireEye, "Mandiant APT1. Exposing One of China's Cyber Espionage Unites," *FireEye*, accessed: 2020-03-28, at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

Gilding, Simeon, "5G Choices: A Pivotal Moment in World Affairs," *ASPI*, accessed: 2020-02-27, at: https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/.

Government of the Czech Republic, "Prague 5G Security Conference Announced Series of Recommendations. The Prague Proposals," *Czech Republic*, accessed: 2019-09-10, at: https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

Huawei Cyber Security Evaluation Centre Oversight Board, "Annual Report," *HCSEC*, accessed: 2019-08-09, at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

International Labour Organization, "Trade Union Law of the People's Republic of China. 2009 Amendment. Effective," *ILO*, accessed: 2020-03-28, at: https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/30352/118793/F1165849917/CHN30352%202.pdf.

Kaska, Kadri, et al., *Huawei, 5G and China as a Security Threat*, Tallinn, NATO Cooperative Cyber Defence Centre of Excellence, 2019.

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

Lau, Stuart, ""Better Than We Hoped For", as UK, EU Leave Door Partially Open for Chinese Tech Firm Huawei," *South China Morning Post*, accessed: 2020-02-27, at: https://www.scmp.com/news/china/diplomacy/article/3048285/better-we-hoped-uk-eu-leave-door-partially-open-chinese-tech.

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

Milhaupt, Curtis J., and Wentong Zheng, "Beyond Ownership. State Capitalism and the Chinese Firm," *The Georgetown Law Journal* 103: 3, 2015, pp. 665-722.

NIS Cooperation Group, *Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigation Measures. CG Publication 01/2020*, Brussels, European Commission, 2020.

Oertel, Janka, "On 5G, Brussels Is Up to the Job," *European Council on Foreign Relations*, accessed: 2020-02-27, at: https://www.ecfr.eu/article/commentary_on_5g_brussels_is_up_to_the_job.

Pancevski, Bojan, "US Officials Say Huawei Can Covertly Access Telecom Networks," *Wall Stree Journal*, accessed: 2020-02-27, at: https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

Peking University Law Database, "National Intelligence Law of the People's Republic of China. 2018 Amendment. Effective," *PKULaw*, accessed: 2020-03-28, at: https://en.pkulaw.cn/display.aspx?cgid=313975&lib=law.

Pelosi, Nancy, "Speaker Pelosi Remarks at Munich Security Conference," *US House of Representatives*, accessed: 2020-03-27, at: https://www.speaker.gov/newsroom/21420-1.

Pompeo, Michael R., "United States Welcomes the EU's Acknowledgement of the Unacceptable Risks Posed by Untrusted 5G Suppliers," *US Department of State*, accessed: 2020-02-27, at: https://www.state.gov/united-states-welcomes-the-eus-acknowledgement-of-the-unacceptable-risks-posed-by-untrusted-5g-suppliers/.

PwC, "Operation Cloud Hopper," *PwC*, accessed: 2020-03-28, at: https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

Reuters, "Huawei Denies German Report it Colluded with Chinese Intelligence," *Reuters*, accessed: 2020-02-27, at: https://www.reuters.com/article/us-germany-usa-huawei/huawei-denies-german-report-it-colluded-with-chinese-intelligence-idUSKBN1ZS197.

Rühlig, Tim, and Maja Björk, "What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe," *UI Paper 1/2020*, Stockholm, The Swedish Institute of International Affairs, 2020.

Rühlig, Tim Nicholas, et al., *5G and the US–China Tech Rivalry: a Test for Europe's Future in the Digital Age. SWP Comment 29*, Berlin, SWP, 2019.

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

Steveson, Reed, "How Huawei Became a Target for Governments," *Bloomberg*, accessed: 2020-03-28, at: https://www.washingtonpost.com/business/how-huawei-became-a-target-for-governments/2019/11/22/302af044-0d4f-11ea-8054-289aef6e38a3_story.html.

The Economist, "Britain Takes a Third Way on 5G with Huawei," *The Economist*, accessed: 2020-02-27, at: https://www.economist.com/britain/2020/01/28/britain-takes-a-third-way-on-5g-with-huawei.

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

Voland, Thomas, and Michel Petite, "Cybersecurity Measures and WTO Law," *Europäische Zeitschrift für Wirtschaftsrecht* 23: 8, 2020, pp. 218-229.

Wall, Matthew, "What is 5G and What WIll It Mean for You?," *BBC*, accessed: 2020-03-27, at: https://www.bbc.co.uk/news/business-44871448.

Wines, Michael, "China Fortifies State Businesses to Fuel Growth," *CNBC*, accessed: 2020-03-28, at: https://www.cnbc.com/id/38910346.

Yap, Chuin-wei, "State Support Helped Fuel Huawei's Global Rise," *Wall Street Journal*, accessed: 2020-02-09, at: https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736.

ZDF, "Operation Rubikon. Wie BND und CIA die Welt belauschten. Fontal 21 vom 11. February 2020," *ZDF*, accessed: 2020-03-28, at: https://www.zdf.de/politik/frontal-21/operation-rubikon-100.html.

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.

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