CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

Huawei, 5G and China as a Security Threat

Kadri Kaska, Henrik Beckvard and Tomáš Minárik

Tallinn 2019

About the authors

The authors are researchers at the CCDCOE Law and Strategy branches.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 21 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. The heart of the Centre is a diverse group of international experts from military, government, academia and industry backgrounds.

The CCDCOE is home to the *Tallinn Manual 2.0*, the most comprehensive guide on how international law applies to cyber operations. The Centre organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring the Centre hosts the International Conference on Cyber Conflict (CyCon), a unique event joining key experts and decision-makers of the global cyber defence community. Since January 2018, CCDCOE has been responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations; to date Austria, Belgium, the Czech Republic, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Portugal, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

Table of Contents

Executive summary

This paper, *Huawei, 5G, and China as a Security Threat,* examines the cybersecurity debate around Huawei as the potential supplier of 5G technology for next generation wireless networks. Looking at cybersecurity considerations and beyond, the paper discusses factors that have brought Huawei to its current contested status: the Chinese national policy of technological superiority, the legal (both domestic and international) context of its operations, and the political environment, including its track record of cyber activity. Informed by this context, the paper makes a comparative analysis of existing national positions regarding 5G solutions originating from China. The paper does not, however, venture into discussions over other potential interests such as trade or industry. Granted, these areas might also influence the choice of 5G provider but they lie outside the NATO CCDCOE remit and therefore the scope of this paper.

The authors argue that the issue of Huawei 5G deployment must be assessed in the broader geopolitical context. First, China approaches it as such. Its legal and political environment, along with its known practice of 'public-private partnership' in cyber espionage, remain a concern. Secondly, the role of fundamental digital infrastructure for modern societies is not a mere technocratic platform issue. Neither can the 5G discussion be isolated to the civilian or the defence domain. It has critical implications for both simultaneously, and choices must therefore be informed by both perspectives.

The growth of Chinese technology companies have made them a global market power. This is largely a product of focused government industrial policy and funding instruments. Chinese companies are not only subsidised by the Chinese government but also legally compelled to work with its intelligence services. Whether the risk of such collaboration is real or perceived, the fear remains that adopting 5G technology from Huawei would introduce a reliance on equipment which can be controlled by the Chinese intelligence services and the military in both peacetime and crisis. In addition, infrastructure decisions are not easily reversed: once a 5G provider has been chosen it will be very costly and time consuming to roll back that decision – and, from a security perspective potentially, too late.

The authors maintain that 5G rollout needs to be recognised as a strategic rather than merely a technological choice. It is rational to demand the highest possible security assurance from 5G technology used for critical communication. Possible loss or interruption of availability, integrity or confidentiality in such systems could have a significant adverse effect on society. Eliminating the risk of control over such systems by an adversary state may include the elimination of Chinese products from the supply chain. Solid accountability, transparency, and risk mitigation mechanisms are the essential minimum in order to benefit from the socioeconomic benefit of 5G without jeopardising national security.

Viable alternatives to Huawei technology are necessary to preserve flexibility of choice and to prevent being trapped with one supplier without a way out. To this end, R&D investment and strengthening regional industry are not purely issues of global competitiveness, but should also be considered – and more importantly, pursued – for their security dimension.

The Chinese general, military strategist, writer and philosopher Sun Tzu is often quoted for stating that 'the supreme art of war is to subdue the enemy without fighting'. Even though the reference was made with regard to breaking the opponents' will to fight, it rings equally true in this context. The decisions we make today will have an impact on our tomorrow.

Introduction

The escalation of the national security debate around Huawei has caught a number of 5G enthusiasts off guard. The United States, Australia, New Zealand, Japan and the Czech Republic, among others, have imposed restrictions on the use of Huawei 5G solutions over national security concerns; much of Europe is pondering whether to follow suit. Summed up, the nations' worries are rooted in the ties between Chinese communications technology companies and its intelligence services, reinforced by China's political and legal environment requiring cooperation with intelligence agencies. Perceived or real, fears persist that adopting Huawei 5G technology will introduce a critical reliance on equipment that can potentially be controlled by the Chinese intelligence services and the military in peacetime and in crisis.

Chinese technology companies have become significant players in the global market because of their embrace of innovation and the notably improved quality and affordable cost of their products. However, the legal and political influence of the Chinese state over its technology industry and ties between the government and the companies leave the Western countries uneasy. China has made no secret of its adversarial perception of the West, and has been actively seeking a stronger global influence. It has for long also sustained a remarkable track record of cyber espionage.

On the other side of the coin is the nature and the potential of 5G. More than simply a new cool technology that offers improved quality and innovative possibilities, 5G networks have the potential of becoming the digital nervous system of the contemporary societies. However, no technology can be assured to be fully secure, and the risk of unexpected vulnerabilities that can be exploited by a malicious actor will have to be factored into the calculation. China's known capability and inclination to take advantage of this feature make the issue of 5G deployment more than a mere technocratic matter – it needs to be considered comprehensively, recognising that the choice of technology has both economic and national security implications.

Neither is it a discussion where the civilian and the defence perspective can be separated. The national security and defence organisations are to a significant extent users of civilian infrastructure, and have a mandate to protect it during crisis. As more digital or 'smart' technologies find their way into military operations, the establishment and maintenance of a parallel digital infrastructure for defence will be even less realistic. As 5G will have critical civilian and defence implications, decisions must be informed by both perspectives.

The authors hold that it is rational to demand high security assurance from 5G technology used for mission-critical communication and, to the farthest degree possible, to eliminate the risk of control over network resources by foreign services. However, the fundamental question is one of trust: states need assurances that their critical systems and data – and those of their partners and allies – are safe from foreign meddling, both now and in the foreseeable future, thus cost and speed cannot be the sole or decisive factors in the rollout of innovative infrastructure. Viewing 5G security as merely a matter of network security, and failing to consider a potential national security dimension may ultimately prove more expensive and harm the long-term wellbeing of the society.

This paper addresses these considerations from both a cybersecurity point of view and that of a broader national security context. It will consider the strategic and legal issues raised by potential reliance on Chinese technology in the rollout of 5G, the emerging national responses, and offer recommendations for a common approach.

Finally, the paper does not aspire to identify – much less delineate – all areas of opportunity, categories of risk, and potential remedies to contain the risks posed by the adoption of Chinese technology. Modern liberal democracies are increasingly dependent on digital infrastructure and technology for operating their societies and sustaining their way of life. The need to consider the risks arising from linking such dependencies to technology potentially controlled by non-democratic or adversarial states becomes more pressing.

More broadly, Western democracies need a better understanding of the way China integrates its technological and geopolitical ambitions in accessing Western markets. The implications of this endeavour for liberal democracies go far beyond the issue of 5G.

WHAT IS 5G AND WHAT ARE THE SECURITY IMPLICATIONS?

5G is the next generation of wireless mobile technology, providing greater data speeds, lower latency (better responsiveness), and the possibility to simultaneously connect to more devices.[1] These qualities will expedite the advance of robotics and automation, virtual and augmented reality, and artificial intelligence and machine learning[2] – transforming the scene of smart devices and applications, and the entire operation of digital societies, very likely in ways unimagined today.

A higher use of virtualisation in 5G will, at the same time, arguably lead to further evolution of security threats and a broader, multifaceted attack surface. Linking increasing billions of intercommunicating devices, 5G will entail an exponential rise in the number of both potential targets and means for espionage, not to mention its potential for emerging signals intelligence platforms to enable massive collecting and parsing of telemetry data. In grim but not unrealistic prognoses, these developments will lead to the emergence of a potential '"surveillance web" over much of the planet'.[3]

5G technology reduces the separation between edge and core communications networks, meaning that it is no longer possible to limit vendor impact to the edge: a potential threat anywhere in the network will be a threat to the whole network.[4]

Any hope of the possibility to roll back implementation of a particular vendor's technology might remain an illusion: it would mean having to change architecture, which is complicated, time-consuming, and therefore costly.[5]

[1] Christian de Looper, 'What is 5G? Here's everything you need to know'. Digital Trends, 25 January 2019. https://www.digitaltrends.com/mobile/what-is-5g/; Sascha Segan, 'What Is 5G?' PC Magazine, 28 January 2019. https://www.pcmag.com/article/345387/what-is-5g; David Goldman, 'What is 5G?' 25 February 2019. https://edition.cnn.com/2019/02/25/tech/what-is-5g/index.html

[2] Fredric Paul, 'Six IoT predictions for 2019'. Network World, 2 January 2019. https://www.networkworld.com/article/3330738/six-iot-predictions-for-2019.html

[3] Heather Woods, 'Do I want an always-on digital assistant listening in all the time?' The Conversation, 16 July 2018. https://theconversation.com/do-i-want-an-always-on-digital-assistant-listening-in-all-the-time-92571

[4] Corinne Reichert, 'Huawei denies foreign network hack reports'. ZDNet, 5 November 2018. https://www.zdnet.com/article/huawei-denies-foreign-network-hack-reports/

[5] Daphne Zhang, 'U.S. Push on Huawei Ripples Through Markets'. Wall Street Journal, 23 November 2018. https://www.wsj.com/articles/u-s-push-on-huawei-ripples-through-markets-1542981918

1. Why Huawei?

Huawei technological and price advantage

The rise of Huawei is exemplary of the Chinese national policy of technological superiority: the past few years have seen the company grow into the largest telecoms equipment manufacturer in the world. In 2018, it passed Apple as the second largest producer of smartphones after Samsung.[6] It is currently the only company that can produce 'at scale and cost' all the elements of a 5G network, with its closest competitors Nokia and Ericsson not yet able to offer a viable alternative.[7] Huawei's ambition is to dominate the market for 5G wireless communications,[8] and it has established cooperation with telecommunications companies in a number of countries in Europe and worldwide.

Huawei and other Chinese telecommunications companies have obtained a visible and active role in the development of global 5G standards and have acquired a significant proportion of core patents for 5G. China currently holds an estimated 10% of the '5G-essential' industrial property rights in radio access solutions; of these, Huawei has the most patents, followed by ZTE. Chinese influence in the global standards organisations (ITU, 3G Partnership Project) has also grown in terms of the key positions held by Chinese representatives.[9]

The growth of the global market power of Chinese technology companies is largely a product of focused government industrial policy and accompanying funding instruments.[10] Like its technological advantage, Huawei's affordable pricing is more likely an outcome of China's domestic policy (further discussed in Chapter 2 of this paper) than its fundamental technological superiority over competitors.[11] Preferential treatment of domestic providers means that the latter 'control 75 percent of the [Chinese] market, giving them unbeatable economies of scale'.[12]

Huawei past activities and product security

To date, there has been no evidence, at least publicly, of significant vulnerabilities in Huawei technology. However, the company has repeatedly been blamed for industrial espionage (the 2003 Cisco case[13]

---

[6] Can Huawei survive an onslaught of bans and restrictions abroad? The Guardian, 13 December 2018. https://www.economist.com/business/2018/12/15/can-huawei-survive-an-onslaught-of-bans-and-restrictions-abroad; Global Smartphone Market Share: By Quarter. Counterpoint, 16 November 2018. https://www.counterpointresearch.com/global-smartphone-share/

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

[8] Frank J. Cilluffo, Sharon L. Cardash, 'What's wrong with Huawei, and why are countries banning the Chinese telecommunications firm?' The Conversation, 19 December 2018. https://theconversation.com/whats-wrong-with-huawei-and-why-are-countries-banning-the-chinese-telecommunications-firm-109036

[9] Parv Sharma, '5G Ecosystem: Huawei's Growing Role in 5G Technology Standardization'. Counterpoint Research, 20 August 2018. https://www.counterpointresearch.com/huaweis-role-5g-standardization/

[10] John Lee, ' The rise of China's tech sector: The making of an internet empire'. The Interpreter, Lowy Institute, https://www.lowyinstitute.org/the-interpreter/rise-china-s-tech-sector-making-internet-empire; Adam Segal, 'When China Rules the Web: Technology in Service of the State''. Foreign Affairs, September/October 2018.

[11] See, e.g., China - Market Challenges. Export.gov, 4 May 2018. https://www.export.gov/article?id=China-Market-Challenges

[12] Thorsten Benner, 'Germany Is Soft on Chinese Spying'. Foreign Policy, 9 December 2018. https://foreignpolicy.com/2018/12/09/germany-is-soft-on-chinese-spying/. See also Erick Fang, 'Barriers To Entry Into The Chinese Mobile Market'. Forbes, 21 December 2018. https://www.forbes.com/sites/forbestechcouncil/2018/12/21/barriers-to-entry-into-the-chinese-mobile-market/#6df45bff673b

[13] The Huawei Way. Newsweek, 15 January 2006. https://www.newsweek.com/huawei-way-108201

and the 2014 T-Mobile lawsuit[14]) and of continued violation of international economic sanctions against Iran and North Korea,[15] which has particular significance because Huawei products use components produced in the United States.[16] The company is currently at the centre of fraud and intellectual property theft investigations in the US.[17]

Huawei staff members have recently been linked to espionage allegations, with Australian intelligence reports in 2018 indicating that Huawei personnel were used 'to get access codes to infiltrate a foreign network' in an operation that took place within the last two years.[18] Canada and Poland have in recent months detained two Huawei officials, one related to the US investigations alluded to above (involving Huawei's chief financial officer, daughter of the founder and president of Huawei) and the other on grounds of espionage. Huawei has denied that the latter case had any relation to the company's business.[19] The Czech national cybersecurity authority (NCISA) relied on accessible findings of the cybersecurity community regarding Huawei and ZTE activities 'in the Czech Republic and around the world' in issuing a warning for the use of the companies' technologies.[20]

Huawei, for its part, rejects the accusations. It insists that its shares are owned by employees, it is not beholden to any government, and it has never used its equipment to spy on or sabotage other countries.[21] It also 'categorically denies that it has ever provided, or been asked to provide, customer information for any government or organisation'.[22] Huawei has set up Security Assessment Centres in the United Kingdom, Germany, and recently in Brussels to provide partners with the opportunity to assess their products, including the source code,[23] and generally refers to itself as the 'most audited technology company in the world'.[24]

IT IS NOT JUST ABOUT HUAWEI

While Huawei stands in the limelight due to its advanced 5G capacity, the issue is not just about Huawei: many states are likewise concerned about other Chinese communications and video surveillance technology manufacturers – primarily ZTE, but also Hytera Communications Corporation, Hangzhou Hikvision, and Dahua Technology, all of whose technology has been banned from use in government networks under US law.[25]

---

[14] Hiroko Tabuchi, 'T-Mobile Accuses Huawei of Theft from Laboratory'. The New York Times, 5 September 2014. https://www.nytimes.com/2014/09/06/business/t-mobile-accuses-huawei-of-theft-from-laboratory.html; Andrew Orlowski, 'Huawei spied, US federal jury finds'. The Register, 19 May 2017. https://www.theregister.co.uk/2017/05/19/huawei_spied_us_jury_finds/

[15] Kate Fazzini, 'Why the US government is so suspicious of Huawei'. CNBC, 6 December 2018. https://www.cnbc.com/2018/12/06/huaweis-difficult-history-with-us-government.html

[16] Tim Culpan, 'Don't Worry About a U.S. Component Ban on Huawei' Bloomberg, 13 December 2018. https://www.bloomberg.com/opinion/articles/2018-12-12/huawei-components-ban-is-unlikely-with-trump-ready-to-deal

[17] Harry Cockburn, 'Germany 'planning to exclude Huawei from new 5G network' as US reportedly investigates theft claims', Independent, 17 January 2019. https://www.independent.co.uk/news/world/europe/huawei-germany-5g-network-security-china-us-canada-trade-secrets-stolen-meng-wanzhou-a8732661.html

[18] *Supra* note 4.

[19] James Pomfret, Anna Koper, 'Huawei sacks employee arrested in Poland on spying charges'. Reuters, 12 January 2019. https://www.reuters.com/article/us-huawei-poland-security/huawei-sacks-employee-arrested-in-poland-on-spying-charges-idUSKCN1P60E8

[20] National Cyber and Information Security Agency Warning (reference 3012/2018-NÚKIB-E/110) of 17 December 2018, https://www.govcert.cz/download/kii-vis/Warning.pdf.

[21] *Supra* note 5.

[22] *Supra* note 4.

[23] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2018. A report to the National Security Adviser of the United Kingdom, July 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf; 'Huawei opens Security Innovation Lab in Bonn'. Huawei, 16 November 2018. https://huawei.eu/media-centre/press-releases/huawei-opens-security-innovation-lab-bonn

[24] Richard Chirgwin, 'Huawei: 'trust us, we are being transparent''. The Register, 28 May 2013. https://www.theregister.co.uk/2013/05/28/huawei_trust_us_we_are_being_transparent/

[25] John S. McCain National Defense Authorization Act for Fiscal Year 2019. https://www.congress.gov/bill/115th-congress/house-bill/5515/text

ZTE

ZTE is one of China's leading telecom equipment manufacturers and one of the world's leading network gear providers. Its main products are core and transport network, wireless and fixed access, cloud computing and energy solutions. ZTE is partially owned and controlled by the Chinese state.[26]

Sanctions violations and cybersecurity. In 2017, ZTE was fined for illegally exporting US technology to Iran and North Korea in violation of economic sanctions.[27] In April 2018, the US Department of Commerce issued a 7-year export ban of ZTE products to US, which was lifted in July after ZTE replaced its senior management and agreed to pay additional fines and establish an internal compliance team.[28] Its recently issued Cybersecurity Statement emphasises ZTE's dedication to cybersecurity, cooperation and transparency.[29]

HYTERA, HANGZHOU HIKVISION, DAHUA TECHNOLOGY

Hytera is the second largest global radio terminal manufacturer with 13% of global market share.[30] It produces DMR, TETRA, LTE and MPT-1327 systems,[31] of which TETRA is specifically designed for use by government agencies, emergency services and public safety networks, transport services (rail in particular) and the military.

Hikvision and Dahua Technology are both Chinese providers of video surveillance products, holding the first and second position in global market share.

[26] Steve Stecklow and Karen Freifeld, 'UPDATE 7-U.S. bans American companies from selling to Chinese phone maker ZTE'. Reuters, 16 April 2018. https://www.reuters.com/article/usa-china-zte/update-7-u-s-bans-american-companies-from-selling-to-chinese-phone-maker-zte-idUSL1N1RT0IX; 'Factbox: U.S. bans sales to major Chinese telco equipment vendor ZTE'. Reuters, 17 April 2018. https://www.reuters.com/article/us-usa-china-zte-factbox/factbox-u-s-bans-sales-to-major-chinese-telco-equipment-vendor-zte-idUSKBN1HO125

[27] Paul Mozur, Cecilia Kang, 'U.S. Fines ZTE of China $1.19 Billion for Breaching Sanctions'. The New York Times, 7 March 2017. https://www.nytimes.com/2017/03/07/technology/zte-china-fine.html

[28] David Shepardson, Karen Freifeld, 'U.S. reaches deal to keep China's ZTE in business: congressional aide'. Reutersm 25 May 2018. https://www.reuters.com/article/us-usa-trade-china-zte/u-s-reaches-deal-to-keep-chinas-zte-in-business-congressional-aide-idUSKCN1IQ2JY

[29] ZTE Cybersecurity Statement, ZTE Corporation, 11 January 2019. https://www.zte.com.cn/global/404?path=/global/about/press-center/news/201901/201901111654

[30] 'Hytera'. DMR Association. https://www.dmrassociation.org/hytera.html

[31] 'Hytera'. http://www.hytera.com/navigation.htm?newsId=6478&columnType=news&pageType=solutionNews

2. Security environment: China's strategic reinforcement of its interests

National technological superiority agenda

The determination of the People's Republic of China to become a digital technology superpower dates back well over a decade, with China's 2006 long-term national innovation strategy setting goals of technological indigenous innovation and untying itself from the West. The effort has been backed by firm government guidance and control, with focused government investment into technology research and development. By restricting Western companies' access to the Chinese market, Chinese industry has been able to benefit from the economies of scale in its home market, largely unchallenged by foreign competitors.[32]

Government subsidy and direct financing has boosted Chinese companies' competitive position on the global market, both in terms of technological advance and affordable prices. Over recent years, Chinese capital has acquired numerous Western technology and infrastructure companies,[33] which is leaving European and US regulators increasingly concerned.[34]

Practice of espionage and influence operations

Security concerns around the use of Chinese technology are as old as their rising position on global markets. Western government officials and the security community have been uneasy about the possibility that technology produced by Chinese companies could be used by the Chinese government and military to spy on users.

China has a notorious reputation for persistent industrial espionage, and in particular for the close collaboration between government and Chinese industry in 'targeting academia, industry and government facilities for the purpose of amassing technological secrets'.[35] There is a long trail of examples of using governmental and military cyber capabilities for the purposes of economic espionage and influence operations.[36] In 2013, Mandiant released their renowned report exposing a multi-year Advanced Persistent Threat (APT) campaign, publishing evidence linking the APT1 group to the Chinese People's Liberation Army and detailing the group's systematic theft of confidential data from over 140 organisations across multiple industries.[37] Numerous accounts by various other actors have been reported since.[38] As recently as December 2018, the UK and its allies announced that a group known as APT 10 'acted on behalf of the Chinese Ministry of State Security to carry out a malicious cyber campaign targeting intellectual property and sensitive commercial data in Europe, Asia and the

---

[32] See Mikk Raud, 'China and Cyber: Attitudes, Strategies, Organisation'. NATO CCDCOE, 2016. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf

[33] For a good investigative report over Chinese acquisitions, see Andre Tartar, Mira Rojanasakul and Jeremy Scott Diamond, 'How China Is Buying Its Way Into Europe'. Bloomberg, 23 April 2018. https://www.bloomberg.com/graphics/2018-china-business-in-europe/;

[34] Jerker Hellström, 'China's Acquisitions in Europe: European Perceptions of Chinese Investments and their Strategic Implications'. FOI, December 2016. https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4384--SE; Janne Suokas, 'Chinese investment in US, Europe plummets in 2018'. GBTimes, 14 January 2019. https://gbtimes.com/chinese-investment-in-us-europe-plummets-in-2018

[35] Mikk Raud, *supra* note 32, 5.

[36] The influence operations aspect is emphasised by e.g. the Czech Republic's Annual Report of the Security Information Service for 2017, https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/en/ar2017en.pdf.

[37] 'Mandiant Releases Report Exposing One of China's Cyber Espionage Groups', https://www.fireeye.com/company/press-releases/2013/mandiant-releases-report-exposing-one-of-chinas-cyber-espionage-groups.html

[38] See, e.g., FireEye's catalogue of Advanced Persistent Threat groups, with accompanying reports https://www.fireeye.com/current-threats/apt-groups.html.

US'.[39] Of all economic espionage cases handled by the US Department of Justice between 2011-2018, 90% involved China.[40] Chinese cyber espionage is a concern also frequently raised by European national intelligence and cybersecurity agencies in their public assessments.[41]

Legal and political environment in China

The Chinese National Intelligence Law of 2016 requires all companies 'to support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of. The state shall protect individuals and organisations that support, cooperate with, and collaborate in national intelligence work'.[42] In the same manner, the 2014 Counterintelligence Law with its implementing acts lays down obligations for 'relevant organisations and individuals' to provide information, facilities, or other assistance, and states the relevant organisations and individuals 'must not refuse' cooperation.[43] These acts leave little assurance regarding proper judicial or public oversight to constrain the introduction of backdoors should the state deem this necessary for its broad notion of maintaining state security.

Most countries lack specific transparency and accountability mechanisms over Huawei operations. The UK Huawei Cyber Security Evaluation Centre (HCSEC), with its dedicated oversight board controlled by the UK cybersecurity authority NCSC and reporting to GCHQ, the UK intelligence and security agency, is so far unique in its model of operation. (The recent entities set up in Germany and Belgium lack a similar oversight arrangement.)[44] Even in the absence of an official relationship between a technology company and the Chinese government, the legal environment is conducive to using private companies and their technology as vehicles for espionage.[45] The Czech NCISA assessment notes that companies 'usually' do not refrain from such cooperation.[46]

Chinese and Western approaches to individual rights also differ fundamentally. The EU takes a strict stand on protecting individual privacy and restricts mass surveillance (as evident through the implementation of the General Data Protection Regulation (GDPR) and in recent landmark judgments by the European Court of Justice),[47] and both the EU and United States have solid intellectual property protection regimes, Chinese national policy – and the consequent legal environment – clearly favours state interests over private ones. Although customer relations in countries where Huawei operates are subject to local law, a vertically integrated company cannot ignore obligations stemming from overlapping jurisdictions.

---

[39] 'UK and allies reveal global scale of Chinese cyber campaign'. Foreign & Commonwealth Office, National Cyber Security Centre, and The Rt Hon Jeremy Hunt MP, 20 December 2018. https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign

[40] Cristina Maza, 'China Involved In 90 Percent Of Espionage And Industrial Secrets Theft, Department Of Justice Reveals'. Newsweek, 12 December 2018. https://www.newsweek.com/china-involved-90-percent-economic-espionage-and-industrial-secrets-theft-1255908

[41] *Supra* note 36; Estonian Information System Authority Annual Cyber Security Assessment 2017, https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_csa_2017.pdf; 'Intelligence Risk Assessment 2018', Estonian Foreign Intelligence Service, https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

[42] Samantha Hoffman and Elsa Kania, 'Huawei and the ambiguity of China's intelligence and counter-espionage laws'. The Strategist, Australian Strategic Policy Institute, 13 September 2018. https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/

[43] Ibid.

[44] Huawei cyber security evaluation centre: oversight board annual report 2017. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2017.
https://www.theregister.co.uk/2018/12/18/german_cybersecurity_chief_show_me_the_huawei_evidence/

[45] 'Germany' BSI chief says 'No Evidence' of Huawei spying'. The Local, 16 December 2018. https://www.thelocal.de/20181216/german-it-watchdog-says-no-evidence-of-huawei-spying

[46] *Supra* note 20.

[47] Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB and Watson; Joined Cases C-293/12 and C-594/12 Digital Rights Ireland

In a legal and political environment that compels companies to collaborate with intelligence agencies, opaque organisational and personal links between the companies and the state aggravate concerns. In 2012, a US House Intelligence Committee investigative report noted Huawei's failure 'to disclose details of its dealings with the Chinese military or intelligence services' and refusal to 'provide clear answers on the firm's decision-making processes'.[48] The Committee also received almost no information on the role of the Chinese Communist Party Committee within Huawei or its interaction with the Chinese government.[49]

[48] 'Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE'. U.S. House of Representatives, 112th Congress, 8 October 2012. https://fas.org/irp/congress/2012_rpt/huawei.pdf.
[49] Ibid.

3. International law constraints

Since the primary risk of using Chinese technology arises from the influence exerted over Chinese companies by their government and military, the report will next consider applicable international law and treaty regimes to constrain China's behaviour, thereby potentially offering security assurances to Western governments.

Although acts of espionage within the country of operation are normally punishable under that country's domestic law,[50] espionage as such is not directly addressed in international law. Therefore, there is little legal restraint for state-to-state espionage in general, apart from specific acts that might be unlawful in their nature – such as a particular cyber operation breaching sovereignty or constituting prohibited intervention.

It is broadly accepted that state sovereignty, that is the right of a state to exclusively exercise the functions of state within its territory, also involves its authority over 'the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations'.[51] Conversely, a state's actions that disregard or obstruct another state from exercising its sovereignty constitute a violation of international law. For a particular cyber operation to qualify as violation of sovereignty (or a prohibited intervention, for that matter), the degree of infringement on the territorial integrity of the target state is to be considered, as well as the presence of interference with inherently governmental functions.[52] Furthermore, the nature and degree of state involvement in the operation is decisive in determining whether the activity constituted a breach of international law.[53] The mere identification of an exploitable vulnerability (such as a backdoor) in, for example, Huawei network gear would therefore have little significance from an international law perspective; each cyber operation would have to be qualified on its own based on evidence for specific facts. Again, this implies that international law, for all its merit, should not be regarded as a cyber risk management tool of choice.

China's sovereign authority over its domestic affairs means it is free to impose obligations on its industry, including for the purpose of intelligence collaboration. On the other side of the coin, sovereignty also means that Western states are in principle free to ban Chinese products, while respecting their obligations under international trade arrangements – in particular, the WTO General Agreement on Tariffs and Trade (GATT) which covers international trade in goods.

Article XXI of the WTO GATT contains a security exception which allows a party to take action or measures 'which it considers necessary for the protection of its essential security interests'.[54] The provision's broad scope (it was intended to exclude purely commercial measures under the guise of security[55]) means that even in the context of US-China GATT disputes, it would be difficult to dismiss restrictions introduced towards Huawei products despite commercial interests evidently being part of the disagreement.[56]

---

[50] However, an exclusion of Huawei from domestic markets due to conviction of company personnel could be challenged on the grounds of disproportionality.

[51] See Rule 2 of the Tallinn Manual 2.0, with accompanying commentary. Michael N Schmitt (Ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press, 2017. For a dissenting perspective, see UK Attorney General Jeremy Wright, 'Cyber and International Law in the 21st Century' (May 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

[52] Michael Schmitt, 'In defense of Sovereignty in Cyberspace', Just Security, 8 May 2018. https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

[53] See commentary accompanying Rule 4 (Sovereignty) in the Tallinn Manual, *supra* note 51. See also Rules 66 (prohibited intervention) and 68 (threat or use of force), with accompanying commentary, ibid.

[54] The General Agreement on Tariffs and Trade (GATT 1947), Article XXI. World Trade Organisation. https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXXI.

[55] Brandon J. Murrill, 'The 'National Security Exception' and the World Trade Organization'. Congressional Research Service, 28 November 2018. https://fas.org/sgp/crs/row/LSB10223.pdf

[56] Noah Feldman, 'Huawei and 5G: A Case Study in the Future of Free Trade'. Bloomberg, 13 February 2019. https:// www.bloomberg.com/opinion/articles/2019-02-13/huawei-and-5g-a-case-study-in-the-future-of-free-trade

At the national and regional level, which for the majority of this report's constituency means the EU, competition law and public procurement rules may also need to be considered. While these do not differentiate between EU and non-EU companies, both the EU public procurement Directive 2014/24/EU[57] in general and the electronic communications Directive 2002/21/EC,[58] which addresses the operation of communications networks and the awarding of radio spectrum licences, including 5G, in particular contain exceptions allowing each member state 'to take the necessary measures to ensure the protection of its essential security interests, to safeguard public policy and public security'.

[57] Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC. OJ L 94, 28.3.2014, p. 65–242. http://data.europa.eu/eli/dir/2014/24/oj

[58] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2002:108:TOC.

4. Emerging national responses

The discussion around accepting or restricting Huawei technologies for 5G is characteristic of the adage of 'not seeing the wood for the trees'. Despite growing attention to cybersecurity, the matter is often viewed purely through the lens of risk to a particular communications operator and to their service continuity, missing the dimension of the core communications network constituting the digital backbone of a nation, with cascading cross-sector and often transboundary dependencies for other essential services, and thereby for the society in general. While proper implementation of security baselines by the communications operator will minimise risks, a level of residual risk cannot be eliminated completely, and dependency risks are typically beyond the operator's visibility and control.

Core communications networks constitute fundamental infrastructure and therefore are an essential national interest, bearing national security implications. The fact that Huawei (and ZTE) technology is to be deployed for backbone communications networks means that it would become part of the core national communications infrastructure that a range of essential services and socioeconomic functions rely upon. This implies that Huawei would provide critical components in systems of strategic importance for society, including security services and the military, both due to the latter's partial reliance on these systems and a mandate to protect them during crisis.

The significance of fundamental infrastructure to the functioning of society makes the deployment of communications infrastructure a strategic decision not merely for the telecommunications operator, but for the nation, particularly as 5G is expected to lead to a massive growth of IoT-enabled services, 'upgrading' not merely the degree but the very character of contemporary societies' digital dependency. Therefore, a potential cyber incident – loss of availability, integrity, or confidentiality of data or systems – may have various degrees of impact on national security and vital national interests, potentially up to crisis situations.[59] As such risks cannot fundamentally be precluded with any supplier, the supplier's reliability as a partner to prevent, detect and disclose possible vulnerabilities and to cooperate in risk mitigation bears an even greater significance. Given the cost and difficulty of replacing or duplicating core infrastructure due to the architectural changes required and limited spectrum availability, supplier-side risks must be weighed in a comprehensive manner and beforehand.

Furthermore, due to its relative permanence, infrastructure deployment decisions could have long-term effects on cooperation with international partners and allies by potentially creating risks to sharing sensitive information – something that the United States, for example, has recently cautioned NATO allies about.[60]

Given these concerns, several nations have opted to impose restrictions on the use of Chinese technology in their domestic infrastructure. It bears noting that national positions regarding Huawei *et al.* are still evolving, especially as new facts come to light and other actors express their positions. This also means that a country's earlier restraint in introducing restrictions should not necessarily be considered as set in stone, and existing positions are likely to become more nuanced both in terms of the depth of limitations and the sectors or services to which they apply. Due to different security cultures, degrees of digital dependency, existing capabilities and different priorities, even Western democracies vary in how they perceive the increasing foothold of Chinese technology. This also impacts the choice of means to address the security concerns.

---

[59] See the reasoning in the Czech NCISA warning, *supra* note 20.
[60] Lesley Wroughton, Gergely Szakacs, 'Pompeo warns allies Huawei presence complicates partnership with U.S'. Reuters, 11 February 2019. https://www.reuters.com/article/us-usa-pompeo-hungary/pompeo-warns-allies-huawei-presence-complicates-partnership-with-u-s-idUSKCN1Q0007; Nick Wadhams and Zoltan Simon, 'Pompeo Hints at Huawei Ultimatum to Countries Buying Equipment'. Bloomberg, 11 February 2019. https://www.bloomberg.com/news/articles/2019-02-11/pompeo-hints-at-huawei-ultimatum-to-countries-buying-equipment

National practice towards restricting or accepting Chinese technology varies from binding legislative or administrative means by the state to restrict specific manufacturers (such as in the case of the United States and the Czech Republic), issuing non-binding guidance (Estonia), or voicing abstention from introducing restrictions. For example, Australia,[61] the Czech Republic[62] and Japan[63] have issued mandatory security guidance that excludes providers potentially controlled by foreign governments. Alternatively, New Zealand has blocked an operator's plan to deploy Huawei 5G technology on the basis of the 2013 Telecommunications (Interception Capability and Security) Act[64] due to 'significant national security risks'.[65]

The United States adopted a law in 2018 prohibiting the purchase and use of telecommunications and surveillance products by specific Chinese companies.[66] Huawei recently challenged this move as 'unconstitutional', restrictive of fair competition, and harmful of US consumers,[67] but its prospects of success may be thin since national security interests are standard grounds for limiting open competition as long as they follow fair process and are not arbitrary.[68]

Non-binding measures by the state have involved competent national authorities issuing security guidance, whether this is voluntary (Estonia) or *de facto* followed as binding.[69]

There are also countries which have chosen to abstain from restrictions. The head of Germany's Federal Office for Information Security (BSI) noted in October 2018 that evidence would be needed in order to introduce a ban on Huawei equipment. The position was, however, revised, and in February 2019, reports hinted at Germany requiring a possible 'no-spy deal' similar to the US-China 2015 agreement (which, the US claims, China has since abandoned).[70] The Slovakian Prime Minister has said that the country does not consider Huawei a security threat and would need evidence of risk before imposing any restrictions.[71]

National measures follow a risk-based approach. The restrictions that countries have introduced to date have not been universal, but instead appear to consider the degree of risk to a specific sector, service, or system. Legal measures have typically been limited to government agencies and essential service operators, including communications operators bidding for 5G licences, while non-binding guidance may be issued to the wider public[72] or there may be none at all. Furthermore, the extent of restrictions is occasionally subject to a service risk assessment, such as in the Czech case, requiring that threats to the system be evaluated on a case-by-case basis.[73]

---

[61] Ministers for Communications and the Arts, 'Government Provides 5G Security Guidance To Australian Carriers'. 23 August 2018. https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers
[62] *Supra* note 20.
[63] 'Japan bans Huawei and its Chinese peers from government contracts'. Nikkei Asian Review, 10 December 2019. https://asia.nikkei.com/Economy/Trade-war/Japan-bans-Huawei-and-its-Chinese-peers-from-government-contracts
[64] Telecommunications (Interception Capability and Security) Act 2013. http://www.legislation.govt.nz/act/public/2013/0091/latest/whole.html#DLM5177923
[65] 'GCSB declines Spark's proposal to use Huawei 5G equipment'. Spark New Zealand, 28 Nov 2018. https://www.sparknz.co.nz/news/GCSB_declines_Spark_proposal_Huawei/
[66] Sec. 889 of the John S. McCain National Defense Authorization Act, *supra* note 66.
[67] Sijia Jiang, Jan Wolfe, 'Huawei fights back against U.S. blackout with Texas lawsuit'. 7 March 2019, https://www.reuters.com/article/us-usa-china-huawei-tech-filing/huawei-sues-us-government-seeks-ndaa-ban-lift-idUSKCN1QO061
[68] See a similar reference to domestic competition law in the Czech warning, *supra* note 20.
[69] Toomas Pott, 'Eesti riigivõrkudes Huawei seadmeid turvakaalutlustel ei kasuta'. ERR, 6 December 2018. https://www.err.ee/882737/eesti-riigivorkudes-huawei-seadmeid-turvakaalutlustel-ei-kasuta
[70] Guy Chazan, 'German cyber security chief backs 5G 'no spy' deal over Huawei'. Financial Times, 28 February 2019. https://www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663
[71] Tatiana Jancarikova, 'Slovakia has no evidence of Huawei security threat - prime minister' Reuters, 30 January 2019. https://www.reuters.com/article/us-usa-china-huawei-slovakia/slovakia-has-no-evidence-of-huawei-security-threat-prime-minister-idUSKCN1PO1TO
[72] *Supra* note 8.
[73] *Supra* note 20.

Specific or customised means can be used to mitigate risks, but they require national capacity and Huawei's willingness to cooperate. Huawei cybersecurity centres in the UK and Germany are examples of this. The UK Huawei Cyber Security Evaluation Centre (HCSEC), set up in 2010 to evaluate Huawei hardware and software, is controlled by the UK cybersecurity authority NCSC (part of the UK intelligence and security agency GCHQ). Its Oversight Board produces regular reports of its findings, most recently in July 2018.[74] The head of NCSC recently recognised that this detailed, formal oversight, building on a decade of formally agreed mitigation strategy and detailed provision of information, means that the UK regime is arguably the toughest and most rigorous oversight regime in the world for Huawei, and that it is proving its worth.[75] Huawei set up an assessment centre in Germany in November 2018 'to work with German customers, partners and research institutions as well as government and supervisory authorities'[76] and an EU Cyber Security Transparency Centre in Brussels in March 2019.[77] It has offered to establish a similar one in Poland.[78] It is still too early to tell whether these will prove effective or even credible as transparency and assurance mechanisms, as there does not appear to be a similar oversight arrangement to that of the UK.[79]

In any case, assessment by such bodies encompasses standard cybersecurity practices; it does not extend to assessing intelligence activity by China. The UK NCSC notes that it still has strict controls for how Huawei is deployed – its technology is not accepted into sensitive networks, including those of the government.[80]

Such an assessment and oversight approach may not be affordable for a small country or may be too onerous to justify investment for Huawei, which means that smaller countries will inevitably depend on partner institutions information-sharing or may be aligned towards using legally less precise instruments such as outright limitations.

Speeding up the maturing of alternative providers is an option. In mid-January 2018, Canada signalled its interest in Nokia technology by granting the company $40 million in 5G-related R&D funding.[81] Such means of stimulating supply diversity also help prevent undesirable market dominance by any one company, regardless of origin.

And finally, in the absence of – or next to – practice by states, it is service providers who are taking the initiative. For example, BT Group, the UK's leading telecommunications operator, announced a decision in December 2018 to abandon Huawei devices (both existing 3G and 4G, and new 5G);[82] Deutsche Telekom reported it was reviewing its vendor strategy; and Orange (formerly France Telecom) announced that it would not use Huawei devices.[83] Denmark's largest

---

[74] *Supra* note 44; Andrew Orlowski, 'German cybersecurity chief: Anyone have any evidence of Huawei naughtiness?' The Register, 18 December 2018. https://www.theregister.co.uk/2018/12/18/german_cybersecurity_chief_show_me_the_huawei_evidence/

[75] Ciaran Martin's CyberSec speech in Brussels. NCSC, 20 February 2019. https://www.ncsc.gov.uk/news/ciaran-martins-cybersec-speech-brussels

[76] 'Huawei opens Security Innovation Lab in Bonn'. Huawei, 16 November 2018. https://huawei.eu/media-centre/press-releases/huawei-opens-security-innovation-lab-bonn

[77] 'Huawei Cyber Security Transparency Centre Opens in Brussels'. Huawei, 5 March 2019. https://www.huawei.com/en/press-events/news/2019/3/huawei-cyber-security-transparency-centre-brussels

[78] Huawei offers to build cyber security center in Poland. https://in.reuters.com/article/us-poland-security/huawei-offers-to-build-cyber-security-center-in-poland-idINKCN1PV10P

[79] *Supra* note 77; Alex Ralph, 'Huawei opens without oversight board'. The Times, 6 March 2019. https://www.thetimes.co.uk/article/huawei-reassures-eu-with-security-lab-w9vzc2033

[80] *Supra* note 75.

[81] David Olive, 'What's at stake for Trudeau, Canada and Huawei'. The Star, 28 January 2019. https://www.thestar.com/business/opinion/2019/01/28/whats-at-stake-for-trudeau-canada-and-huawei.html

[82] 'BT bars Huawei's 5G kit from core of network'. BBC, 5 December 2018. https://www.bbc.com/news/technology-46453425;

[83] Douglas Busvine, Gwénaëlle Barzic, 'Deutsche Telekom reviews Huawei ties; Orange says no on 5G'. Reuters, 14 December 2018. https://www.reuters.com/article/us-huawei-europe-germany/deutsche-telekom-reviews-huawei-ties-orange-says-no-on-5g-idUSKBN1OD0G7

telecommunications operator TCD recently announced that it has chosen Ericsson for its 5G supplier due to considerations of quality.[84]

Is it mere protectionism? Given the frequent claim by Huawei and China[85] of restrictions upon Huawei technology being motivated by protectionist interests, this bears brief consideration. The current US-China trade dispute is something that cannot be overlooked. Yet it should not be overplayed as the sole driving reason. The restriction of Huawei technology has a long history and did not begin with the current US administration. Moreover, neither the US nor Australia, New Zealand, the Czech Republic *et al.* currently produce 5G technology themselves, so there are no domestic companies to benefit from these decisions.[86] To the contrary – many countries are eager to launch 5G networks due to the expected quality and innovative services, and a decision to rely on competitors would at the current stage certainly delay deployment.

[84] Sandra Meersohn Meinecke, 'Tech-analytiker om fravalget af Huawei: Sikkerhed og tryghed koster mere'. DR, 19 March 2019. https://www.dr.dk/nyheder/indland/tech-analytiker-om-fravalget-af-huawei-sikkerhed-og-tryghed-koster-mere

[85] 'Australia bans Huawei from 5G network over security concerns'. AP News, 23 August 2018. https://www.apnews.com/1419a86b429248a08ac6aece6d7684f0

[86] *Supra* note 12.

5. Conclusions and recommendations

The core of the Huawei *et al.* debate is not a narrow technology issue. There is, to date, no public evidence of serious technological vulnerabilities in specific Huawei or ZTE equipment. That said, it is fundamentally impossible to rule out potential technology flaws that can be exploited in the future. It does not matter that Chinese technology is, in this regard, no different from technology produced elsewhere. Whether vulnerabilities occur due to wilful action or become exploitable due to failure (to patch software or poor configuration, etc.) on the part of the user is of secondary significance. The potential is there. It remains a concern because procurement of a particular vendor's technology creates a degree of dependence: procuring digital technology is not merely about procuring 'an object', it involves long-term commitment to a relationship with a supplier. Given these prerequisites, the core of the Huawei dilemma is rather about determining which supplier one can trust and what mechanisms does such trust rely on: is it partner credibility, verifiability and accountability, or something else?

China's legal and political environment, along with its known practice of 'public-private partnership' in cyber espionage remain a concern. Chinese government and military cyber entities are among the most capable actors in the world. There are numerous examples of using private actors for the purposes of economic espionage and influence operations in state interests. Chinese companies are required by law to cooperate with their government in support of Chinese national interests, including participation in intelligence activities. Scarcity of accountability mechanisms and opaque organisational and personal links between the companies and the state mean there is little constraint for such 'cooperation'. The ties and interaction between the government and industry are based on a fundamentally different approaches from that which Western practice finds acceptable. China has made no secret of its ambition to reshape a Western-dominated global system.[87]

The security dilemma

The issue of Huawei technology and 5G represents classic dilemmas inherent to cybersecurity: the impact of stimulating the economy to national security and vice versa, and of modernising infrastructure to critical infrastructure protection (and vice versa).[88] Given the significance of backbone national infrastructure, defining a position on these dilemmas is a far more complex challenge than simply finding an acceptable balance on a linear scale: it entails comprehensive understanding of all risks, socioeconomic and security, and mitigating those that are critical by means that are available, i.e. that the society can afford. A level of burden sharing is inevitable: it is not just operator risks that apply, and therefore it should not be just up to the operator to mitigate them.

Given that the issue is more complex than merely the current state of Huawei *et al.'s* technology, it is rational and responsible to consider means of deterring potential future exploitation and to mitigate apparent risks. The concern voiced by the Czech NCISA is not unique – the degree of potential risk to any state is not negligible. Possible loss or interruption of availability, integrity or confidentiality in such systems may have a significant effect which could lead to the emergence of a crisis.

The question is whether we can afford the promise of a 'cheaper' solution put forward by Huawei technology. The current wake-up to the Chinese cyber threat occurs at a time of growing political awareness of digital dependency in societies. Compared to barely half a decade ago, there is greater acknowledgement of the need to take lifecycle costs into account when procuring digital technology, rather than just deployment cost. However, the long-term strategic cost – to the operator, to dependent services and to society, not to mention to international partnerships – is notoriously difficult to measure

[87] See, e.g. Chinese President and Communist Party leader Xi Jinping's 'Xi Jinping And His Era'. China Daily, 18 November 2017. http://www.chinadaily.com.cn/kindle/2017-11/18/content_34683261.htm.

[88] See Alexander Klimburg (Ed.), National Cyber Security Framework Manual. NATO CCDCOE, 2012. https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/. 34-39.

and therefore often ignored. The complexity of estimating their impact does not make these categories less relevant, however.

The authors therefore maintain that viable alternatives to Huawei technology are necessary to preserve flexibility of choice and to prevent being trapped with one supplier without a way out. To this end, R&D investment and strengthening regional industry are not purely issues of global competitiveness, but should also be considered – and importantly, pursued – for their security dimension.

Recommendations

5G rollout needs to be recognised as a strategic rather than merely a technological choice. Solutions chosen today will steer and limit the choices available for years to come. Given the complexity of socioeconomic and security issues affected by the decision to deploy backbone digital infrastructure, the issue of welcoming or refusing Huawei or other Chinese providers cannot be left for technocrats alone to resolve. It requires the political will to step out of the comfort zone and tackle complex aspects of technology, economy and security, the effect of which will span well beyond parliamentary election terms.

A shared concern necessitates a coordinated response. There is growing appetite among EU member states and NATO allies on EU/NATO coordination in this matter. In January 2019, Poland's Minister of Internal Affairs called for the EU and NATO to take a 'joint stance' on Huawei after the arrest of a Huawei employee on spying charges.[89] A similar sentiment was also expressed by the Estonian IT minister.[90] EU Commissioner Julian King, in his speech at the Munich Security Conference in February, outlined a number of critical issues regarding European digital resilience towards foreign threats. These included the uncoordinated issuing of 5G spectrum licences, sales of European cutting edge technologies to foreign capital, and the need for coordinated investment in AI, quantum computing and cryptography so that the action of individual countries will constitute more than merely 'the sum of its parts'.[91] He also highlighted the need for acknowledging critical elements in the European digital ecosystem. None of these issues are easy to resolve and are likely to require going beyond existing safeguards to address the risk. Next to political will to act, this indicates a need for radically improved understanding of the intertwined nature of contemporary digital ecosystems – which is even more true of EU member states due to their political and market independencies going beyond mere technology.

The dilemma at hand primarily concerns civilian networks, so it is not overly likely that NATO will take a lead in coordinating action. However, the NATO Alliance is, and will remain, an important venue for allies and partners for sharing information on threats, and that capacity should not be viewed as separate from defining a common approach among liberal (and European in particular) democracies. The issue of Huawei technology is, however, not without relevance to the Alliance. NATO depends of national critical infrastructure to execute national operations and missions. Infrastructure security issues may affect NATO networks or deployed networks such as the Federated Mission Network. Such networks can also be exposed to risk because their extensions may use host nation civilian infrastructure.

One size does not fit all: there is a need for nuanced risk awareness and risk management tools. Pending a common position – or possibly complementing one – national positions regarding accepting or restricting Huawei technology will likely remain conditioned by the degree of criticality of a risk to a particular service or sector. To deal with these in an adequate and proportionate manner, nations need to re-evaluate their societies' essential functions in the digital era, the nature and degree of dependence of these on digital infrastructure, and continuity mechanisms, including alternative solutions.

---

[89] 'EU, NATO should agree on joint position towards Huawei: Poland.' Reuters, 12 January 2019. https://www.reuters.com/article/us-poland-security/eu-nato-should-agree-on-joint-position-towards-huawei-poland-idUSKCN1P60FV

[90] *Supra* note 69.

[91] Commissioner King's keynote speech at the Munich Cyber Security Conference. 14 February 2019. https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-keynote-speech-munich-cyber-security-conference_en

There is room for nuanced approaches regarding the potential risk of Huawei solutions, too, instead of a blanket ban: the model of inclusive, competent, and transparent oversight embodied in the UK Huawei supervisory board is a good example. Such 'confidence building' and risk mitigation measures may, however, be accessible only to countries with extensive resources and expertise. Realistically this approach would be viable for approximately one third of EU and NATO member states, leaving the rest with the dilemma of choosing their dependencies: trust Chinese technology or trust their partners' insight. The need to share insight and expertise through regional competence centres becomes all the more compelling, given nations' universal shortage of highly specialised experts and the rapidly evolving 5G technology and the market.

Certainly, there are no easy responses to this dilemma. Shutting the door to cooperation with Huawei and China may backfire, as it deprives European and other regional industries of a chance to develop 5G services. This leaves development to be driven by Chinese companies, which can well afford it given the scope and growing purchasing power of their home market and their active engagement with developing countries as growing future markets for new technology.

Finally, risks associated with investments and takeovers by foreign capital are structural and are not specific to digital infrastructure. From a holistic point of view, 5G is but an example among many of China using economic power to acquire a more dominant position in global affairs. Its numerous acquisitions of Western technology and infrastructure companies have left European and US regulators increasingly concerned. As part of the Belt and Road initiative,[92] China is further seeking wide-spectrum plans of cooperation in the development of roads, railways, bridges, civil aviation, ports, energy and telecommunications with many Western countries.

The reluctance of Western countries to deploy critical network solutions – 5G or otherwise – originating from non-democratic states is likely to grow as the latter are becoming more assertive and methodical in their practice of enforcing 'sovereignty' over their 'information space' and markets. Meanwhile, nations with better awareness of risks and a stronger commitment to tackle them could become less inclined to work closely with states that do not share their concerns. Diverging acknowledgement of and inclination to address security risk from using technology from companies such as Huawei has the potential to sow division among both NATO and EU member and partner states. The question is: how will Western democracies tackle this?

With a binary choice of 'take it or leave it' not among the options – there are as of yet no equivalent alternatives to Huawei 5G technology; the West is neither able nor willing to afford a technological stagnation, and with the expected socioeconomic benefits in the promise of 5G, states will likely remain pragmatic in their approaches. Whether by issuing security guidance to reinforce the security of critical government and commercial functions, strengthening risk assessment and management processes, or agreeing on transparency and accountability mechanisms, national responses will likely seek to improve risk mitigation.

[92] 'Belt and Road Initiative'. The World Bank, 29 March 2018. https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative

References

Advanced Persistent Threat Groups. FireEye, https://www.fireeye.com/current-threats/apt-groups.html.

Annual Report of the Security Information Service for 2017, https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/en/ar2017en.pdf.

'Australia bans Huawei from 5G network over security concerns'. AP News, 23 August 2018. https://www.apnews.com/1419a86b429248a08ac6aece6d7684f0

'Belt and Road Initiative'. The World Bank, 29 March 2018. https://www.worldbank.org/en/topic/regional-integration/brief/belt-and-road-initiative

Benner, Thorsten, 'Germany Is Soft on Chinese Spying'. Foreign Policy, 9 December 2018. https://foreignpolicy.com/2018/12/09/germany-is-soft-on-chinese-spying/

Busvine, Douglas and Gwénaëlle Barzic, 'Deutsche Telekom reviews Huawei ties; Orange says no on 5G'. Reuters, 14 December 2018. https://www.reuters.com/article/us-huawei-europe-germany/deutsche-telekom-reviews-huawei-ties-orange-says-no-on-5g-idUSKBN1OD0G7

'BT bars Huawei's 5G kit from core of network'. BBC, 5 December 2018. https://www.bbc.com/news/technology-46453425

'Can Huawei survive an onslaught of bans and restrictions abroad?' The Guardian, 13 December 2018. https://www.economist.com/business/2018/12/15/can-huawei-survive-an-onslaught-of-bans-and-restrictions-abroad

Chazan, Guy, 'German cyber security chief backs 5G 'no spy' deal over Huawei'. Financial Times, 28 February 2019. https://www.ft.com/content/5a0fe826-3b34-11e9-b856-5404d3811663

China - Market Challenges. Export.gov, 4 May 2018. https://www.export.gov/article?id=China-Market-Challenges

Chirgwin, Richard, 'Huawei: 'trust us, we are being transparent''. The Register, 28 May 2013. https://www.theregister.co.uk/2013/05/28/huawei_trust_us_we_are_being_transparent/

Ciaran Martin's CyberSec speech in Brussels. NCSC, 20 February 2019. https://www.ncsc.gov.uk/news/ciaran-martins-cybersec-speech-brussels

Cilluffo, Frank J. and Sharon L. Cardash, 'What's wrong with Huawei, and why are countries banning the Chinese telecommunications firm?' The Conversation, 19 December 2018. https://theconversation.com/whats-wrong-with-huawei-and-why-are-countries-banning-the-chinese-telecommunications-firm-109036

Commissioner King's keynote speech at the Munich Cyber Security Conference. 14 February 2019. https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-keynote-speech-munich-cyber-security-conference_en

Culpan, Tim, 'Don't Worry About a U.S. Component Ban on Huawei' Bloomberg, 13 December 2018. https://www.bloomberg.com/opinion/articles/2018-12-12/huawei-components-ban-is-unlikely-with-trump-ready-to-deal

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) (OJ L 108, 24.4.2002, p. 33), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2002:108:TOC.

Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC. OJ L 94, 28.3.2014, p. 65–242. http://data.europa.eu/eli/dir/2014/24/oj

Estonian Information System Authority Annual Cyber Security Assessment 2017, https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria_csa_2017.pdf

EU, NATO should agree on joint position towards Huawei: Poland.' Reuters, 12 January 2019. https://www.reuters.com/article/us-poland-security/eu-nato-should-agree-on-joint-position-towards-huawei-poland-idUSKCN1P60FV

‘Factbox: U.S. bans sales to major Chinese telco equipment vendor ZTE’. Reuters, 17 April 2018. https://www.reuters.com/article/us-usa-china-zte-factbox/factbox-u-s-bans-sales-to-major-chinese-telco-equipment-vendor-zte-idUSKBN1HO125

Fang, Erick, ‘Barriers To Entry Into The Chinese Mobile Market’. Forbes, 21 December 2018. https://www.forbes.com/sites/forbestechcouncil/2018/12/21/barriers-to-entry-into-the-chinese-mobile-market/#6df45bff673b

Fazzini, Kate, ‘Why the US government is so suspicious of Huawei’. CNBC, 6 December 2018. https://www.cnbc.com/2018/12/06/huaweis-difficult-history-with-us-government.html

Feldman, Noah, ‘Huawei and 5G: A Case Study in the Future of Free Trade’. Bloomberg, 13 February 2019. https://www.bloomberg.com/opinion/articles/2019-02-13/huawei-and-5g-a-case-study-in-the-future-of-free-trade

‘GCSB declines Spark’s proposal to use Huawei 5G equipment’. Spark New Zealand, 28 Nov 2018. https://www.sparknz.co.nz/news/GCSB_declines_Spark_proposal_Huawei/

‘Germany’ BSI chief says ‘No Evidence’ of Huawei spying’. The Local, 16 December 2018. https://www.thelocal.de/20181216/german-it-watchdog-says-no-evidence-of-huawei-spying

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

Global Smartphone Market Share: By Quarter. Counterpoint, 16 November 2018. https://www.counterpointresearch.com/global-smartphone-share/

Goldman, David ‘What is 5G?’ 25 February 2019. https://edition.cnn.com/2019/02/25/tech/what-is-5g/index.html

‘Huawei Cyber Security Transparency Centre Opens in Brussels’. Huawei, 5 March 2019. https://www.huawei.com/en/press-events/news/2019/3/huawei-cyber-security-transparency-centre-brussels

Harry Cockburn, ‘Germany ‘planning to exclude Huawei from new 5G network’ as US reportedly investigates theft claims’, Independent, 17 January 2019. https://www.independent.co.uk/news/world/europe/huawei-germany-5g-network-security-china-us-canada-trade-secrets-stolen-meng-wanzhou-a8732661.html

Heather Woods, ‘Do I want an always-on digital assistant listening in all the time?’ The Conversation, 16 July 2018. https://theconversation.com/do-i-want-an-always-on-digital-assistant-listening-in-all-the-time-92571

Hellström, Jerker, ‘China’s Acquisitions in Europe: European Perceptions of Chinese Investments and their Strategic Implications’. FOI, December 2016. https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4384--SE

Hiroko Tabuchi, ’T-Mobile Accuses Huawei of Theft from Laboratory’. The New York Times, 5 September 2014. https://www.nytimes.com/2014/09/06/business/t-mobile-accuses-huawei-of-theft-from-laboratory.html

Hoffman, Samantha and Elsa Kania, ‘Huawei and the ambiguity of China’s intelligence and counter-espionage laws’. The Strategist, Australian Strategic Policy Institute, 13 September 2018. https://www.aspistrategist.org.au/huawei-and-the-ambiguity-of-chinas-intelligence-and-counter-espionage-laws/

Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2018. A report to the National Security Adviser of the United Kingdom, July 2018. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf

Huawei cyber security evaluation centre: oversight board annual report 2017. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2017

Huawei offers to build cyber security center in Poland. https://in.reuters.com/article/us-poland-security/huawei-offers-to-build-cyber-security-center-in-poland-idINKCN1PV10P

‘Huawei opens Security Innovation Lab in Bonn’. Huawei, 16 November 2018. https://huawei.eu/media-centre/press-releases/huawei-opens-security-innovation-lab-bonn

‘Hytera’. DMR Association. https://www.dmrassociation.org/hytera.html

‘Intelligence Risk Assessment 2018’, Estonian Foreign Intelligence Service, https://www.valisluureamet.ee/pdf/raport-2018-ENG-web.pdf

‘Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE’. U.S. House of Representatives, 112th Congress, 8 October 2012. https://fas.org/irp/congress/2012_rpt/huawei.pdf.

Jancarikova, Tatiana, ‘Slovakia has no evidence of Huawei security threat - prime minister’ Reuters, 30 January 2019. https://www.reuters.com/article/us-usa-china-huawei-slovakia/slovakia-has-no-evidence-of-huawei-security-threat-prime-minister-idUSKCN1PO1TO

‘Japan bans Huawei and its Chinese peers from government contracts’. Nikkei Asian Review, 10 December 2019. https://asia.nikkei.com/Economy/Trade-war/Japan-bans-Huawei-and-its-Chinese-peers-from-government-contracts

Jiang, Sijia and Jan Wolfe, ‘Huawei fights back against U.S. blackout with Texas lawsuit’. 7 March 2019, https://www.reuters.com/article/us-usa-china-huawei-tech-filing/huawei-sues-us-government-seeks-ndaa-ban-lift-idUSKCN1QO061

John S. McCain National Defense Authorization Act for Fiscal Year 2019. https://www.congress.gov/bill/115th-congress/house-bill/5515/text

Joined Cases C-203/15 and C-698/15 Tele2 Sverige AB and Watson

Joined Cases C-293/12 and C-594/12 Digital Rights Ireland

Klimburg, Alexander (Ed.), National Cyber Security Framework Manual. NATO CCDCOE, 2012. https://ccdcoe.org/library/publications/national-cyber-security-framework-manual/. 34-39.

Lee, John, ’ The rise of China’s tech sector: The making of an internet empire’. The Interpreter, Lowy Institute, https://www.lowyinstitute.org/the-interpreter/rise-china-s-tech-sector-making-internet-empire

de Looper, Christian, ‘What is 5G? Here’s everything you need to know’. Digital Trends, 25 January 2019. https://www.digitaltrends.com/mobile/what-is-5g/

Maza, Cristina, ’China Involved In 90 Percent Of Espionage And Industrial Secrets Theft, Department Of Justice Reveals’. Newsweek, 12 December 2018. https://www.newsweek.com/china-involved-90-percent-economic-espionage-and-industrial-secrets-theft-1255908

‘Mandiant Releases Report Exposing One of China’s Cyber Espionage Groups’, https://www.fireeye.com/company/press-releases/2013/mandiant-releases-report-exposing-one-of-chinas-cyber-espionage-groups.html

Meinecke, Sandra Meersohn, ‘Tech-analytiker om fravalget af Huawei: Sikkerhed og tryghed koster mere’. DR, 19 March 2019. https://www.dr.dk/nyheder/indland/tech-analytiker-om-fravalget-af-huawei-sikkerhed-og-tryghed-koster-mere

Ministers for Communications and the Arts, ‘Government Provides 5G Security Guidance To Australian Carriers’. 23 August 2018. https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers

Mozur, Paul and Cecilia Kang, ’U.S. Fines ZTE of China $1.19 Billion for Breaching Sanctions’. The New York Times, 7 March 2017. https://www.nytimes.com/2017/03/07/technology/zte-china-fine.html

Murrill, Brandon J., ‘The ‘National Security Exception’ and the World Trade Organization’. Congressional Research Service, 28 November 2018. https://fas.org/sgp/crs/row/LSB10223.pdf

National Cyber and Information Security Agency Warning (reference 3012/2018-NÚKIB-E/110) of 17 December 2018, https://www.govcert.cz/download/kii-vis/Warning.pdf.

Olive, David, ‘What’s at stake for Trudeau, Canada and Huawei’. The Star, 28 January 2019. https://www.thestar.com/business/opinion/2019/01/28/whats-at-stake-for-trudeau-canada-and-huawei.html

Orlowski, Andrew, ‘Huawei spied, US federal jury finds’. The Register, 19 May 2017. https://www.theregister.co.uk/2017/05/19/huawei_spied_us_jury_finds/

Orlowski, Andrew, ‘German cybersecurity chief: Anyone have any evidence of Huawei naughtiness?’ The Register, 18 December 2018. https://www.theregister.co.uk/2018/12/18/german_cybersecurity_chief_show_me_the_huawei_evidence/

Paul, Fredric, 'Six IoT predictions for 2019'. Network World, 2 January 2019. https://www.networkworld.com/article/3330738/six-iot-predictions-for-2019.html

Pomfret, James and Anna Koper, 'Huawei sacks employee arrested in Poland on spying charges'. Reuters, 12 January 2019. https://www.reuters.com/article/us-huawei-poland-security/huawei-sacks-employee-arrested-in-poland-on-spying-charges-idUSKCN1P60E8

Pott, Toomas, 'Eesti riigivõrkudes Huawei seadmeid turvakaalutlustel ei kasuta'. ERR, 6 December 2018. https://www.err.ee/882737/eesti-riigivorkudes-huawei-seadmeid-turvakaalutlustel-ei-kasuta

Ralph, Alex, 'Huawei opens without oversight board'. The Times, 6 March 2019. https://www.thetimes.co.uk/article/huawei-reassures-eu-with-security-lab-w9vzc2033

Raud, Mikk, 'China and Cyber: Attitudes, Strategies, Organisation'. NATO CCDCOE, 2016. https://ccdcoe.org/uploads/2018/10/CS_organisation_CHINA_092016_FINAL.pdf

Reichert, Corinne, 'Huawei denies foreign network hack reports, ZDNet, 5 November 2018. https://www.zdnet.com/article/huawei-denies-foreign-network-hack-reports/

Segal, Adam, 'When China Rules the Web: Technology in Service of the State''. Foreign Affairs, September/October 2018

Schmitt, Michael N (Ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press, 2017. Wright, Jeremy, 'Cyber and International Law in the 21st Century' (May 2018), https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

Schmitt, Michael, 'In defense of Sovereignty in Cyberspace', Just Security, 8 May 2018. https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/

Segan, Sascha, 'What Is 5G?' PC Magazine, 28 January 2019. https://www.pcmag.com/article/345387/what-is-5g

Sharma, Parv, '5G Ecosystem: Huawei's Growing Role in 5G Technology Standardization'. Counterpoint Research, 20 August 2018. https://www.counterpointresearch.com/huaweis-role-5g-standardization/

Shepardson, David and Karen Freifeld, 'U.S. reaches deal to keep China's ZTE in business: congressional aide'. Reutersm 25 May 2018. https://www.reuters.com/article/us-usa-trade-china-zte/u-s-reaches-deal-to-keep-chinas-zte-in-business-congressional-aide-idUSKCN1IQ2JY

Stecklow, Steve and Karen Freifeld, 'UPDATE 7-U.S. bans American companies from selling to Chinese phone maker ZTE'. Reuters, 16 April 2018. https://www.reuters.com/article/usa-china-zte/update-7-u-s-bans-american-companies-from-selling-to-chinese-phone-maker-zte-idUSL1N1RT0IX

Suokas, Janne, 'Chinese investment in US, Europe plummets in 2018'. GBTimes, 14 January 2019. https://gbtimes.com/chinese-investment-in-us-europe-plummets-in-2018

Tartar, Andre, Mira Rojanasakul and Jeremy Scott Diamond, 'How China Is Buying Its Way Into Europe'. Bloomberg, 23 April 2018. https://www.bloomberg.com/graphics/2018-china-business-in-europe/

Telecommunications (Interception Capability and Security) Act 2013. http://www.legislation.govt.nz/act/public/2013/0091/latest/whole.html#DLM5177923

The General Agreement on Tariffs and Trade (GATT 1947), Article XXI. World Trade Organisation. https://www.wto.org/english/docs_e/legal_e/gatt47_02_e.htm#articleXXI.

'The Huawei Way'. Newsweek, 15 January 2006. https://www.newsweek.com/huawei-way-108201

'UK and allies reveal global scale of Chinese cyber campaign'. Foreign & Commonwealth Office, National Cyber Security Centre, and The Rt Hon Jeremy Hunt MP, 20 December 2018. https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign

Wadhams, Nick and Zoltan Simon, 'Pompeo Hints at Huawei Ultimatum to Countries Buying Equipment'. Bloomberg, 11 February 2019. https://www.bloomberg.com/news/articles/2019-02-11/pompeo-hints-at-huawei-ultimatum-to-countries-buying-equipment

'What Are the Top 5G Security Challenges?' SDX Central, https://www.sdxcentral.com/5g/definitions/top-5g-security-challenges/

Wroughton, Lesley and Gergely Szakacs, 'Pompeo warns allies Huawei presence complicates partnership with U.S.'. Reuters, 11 February 2019. https://www.reuters.com/article/us-usa-pompeo-hungary/pompeo-warns-allies-huawei-presence-complicates-partnership-with-u-s-idUSKCN1Q0007

'Xi Jinping And His Era'. China Daily, 18 November 2017. http://www.chinadaily.com.cn/kindle/2017-11/18/content_34683261.htm

Zhang, Daphne, 'U.S. Push on Huawei Ripples Through Markets'. Wall Street Journal, 23 November 2018. https://www.wsj.com/articles/u-s-push-on-huawei-ripples-through-markets-1542981918

ZTE Cybersecurity Statement, ZTE Corporation, 11 January 2019. https://www.zte.com.cn/global/404?path=/global/about/press-center/news/201901/201901111654