RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS WORKING PAPER

NO. 332

EU POLICIES ON HUAWEI AND 5G WIRELESS NETWORKS

ECONOMIC–TECHNOLOGICAL OPPORTUNITIES VS CYBERSECURITY RISKS

FRANK UMBACH

S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
SINGAPORE

23 DECEMBER 2020

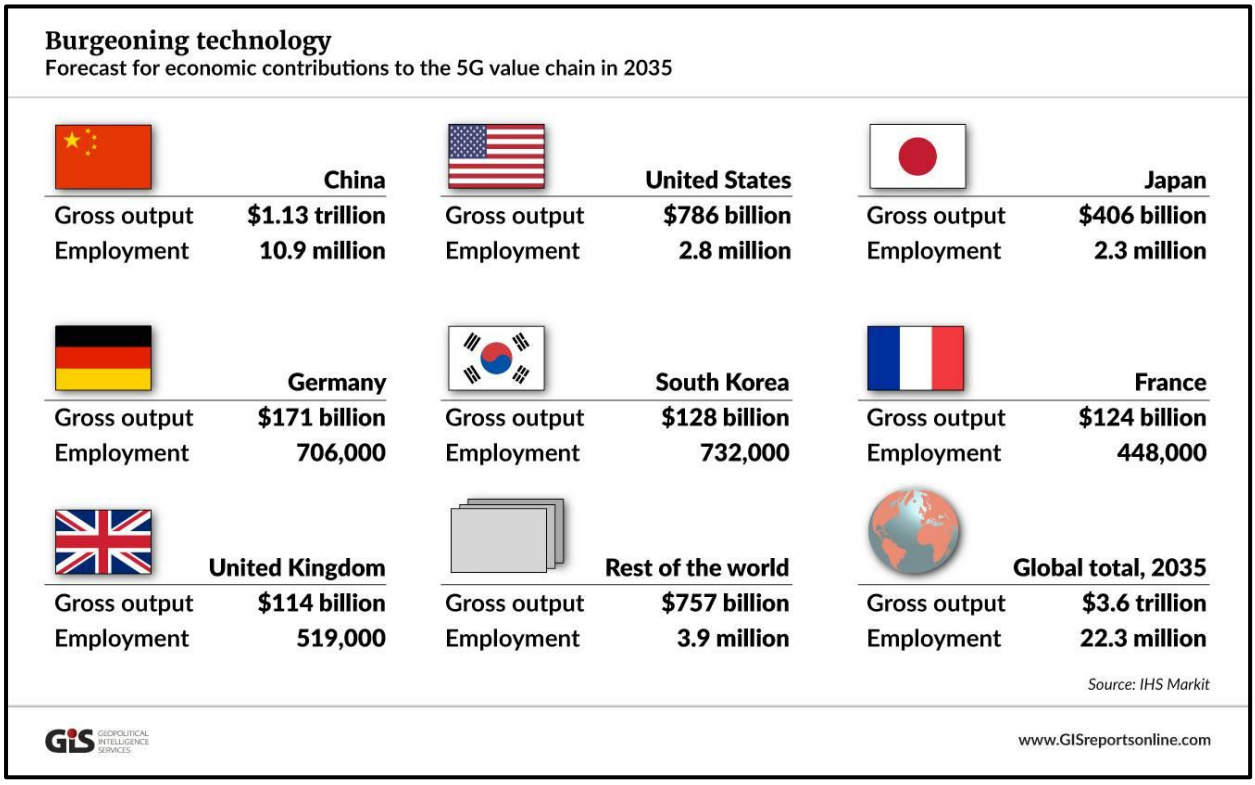
Abstract

Against the backdrop of the global US–China–EU technology competition, this working paper examines the security–economic nexus as European policymakers prepare for the rollout of the next-generation mobile technology network or 5G. Using a comparative approach, it will explore how various EU institutions and EU members approach the tradeoffs between their technological and economic–industrial policies and the inherent cybersecurity risks in 5G technology, notably, the risks in the prospective involvement of the Chinese company Huawei in their 5G rollout. It will particularly look at the approaches of the United Kingdom, Germany and France. The key question that will be addressed is whether the UK government's turnaround in July 2020 to ban Huawei from its 5G rollout and the increasingly assertive stance of several EU member states against Huawei and China are merely the result of American political pressure or the consequence of the changing EU–China relationship or both.

Introduction: A Digital Pax Sinica?

The next years will decide the speed with which the newly introduced 5G or fifth generation of mobile network technology will be deployed for Europe's industries and critical infrastructure (CI). More significantly, they will indicate the extent to which Europe will become economically and technologically dependent on Huawei, the world's leading manufacturer and financier of 5G networks. They will also indicate the extent to which EU member states will accept increasing future cybersecurity risks involving industrial and political espionage or even sabotage as a result of embracing Huawei and of Europe's wider economic–technological dependencies on China. Last summer, Huawei had a share of 36 per cent across the European continent (as opposed to 28 per cent worldwide).[1] Economically, 5G technology could create more than US$13 trillion in new value globally by 2035.[2] The decision of EU member states to involve or ban Huawei and other Chinese companies in the 5G rollout will also highlight the extent to which the European Union is able to agree on common industrial, technology and cybersecurity policies, such as determining and implementing common cybersecurity standards for 5G networks.

Figure 1: Global Economic Benefits of 5G Technology



Source: Klon Kitchen, "US–China 5G battle portends a divided internet", Geopolitical Intelligence Service (GIS), 15 June 2020.

[1] "Huawei/European Telecoms: Security Hang-up", *Financial Times (FT)*, 14 July 2020.
[2] IHS Markit, "The 5G Economy: How 5G will contribute to the Global Economy", November 2019.

The 5G-network technology will become the interconnecting backbone technology for a faster internet and much larger data transfer capacity, facilitating the operations of CI, artificial intelligence (AI), robotics, the internet of things (IoTs), "Industry 4.0" applications, and connecting autonomous cars, smart cities and intelligent factories.[3] With maximum speeds 100 times more than its predecessor 3G/4G technologies, the next generation of mobile technology will reshape economies, societies, the military and cultures through an unparalleled level of connectivity that will change every aspect of daily life.

However, the evolution of 5G technology will lead to rising national and collective cybersecurity risks and vulnerabilities.[4] The technology's overall strategic importance for a country's political and economic stability cannot be overestimated and cannot be compared with the predecessor 3G/4G networks. It will be one of the most disruptive technologies, with revolutionary impacts across economies, societies and armed forces worldwide.[5]

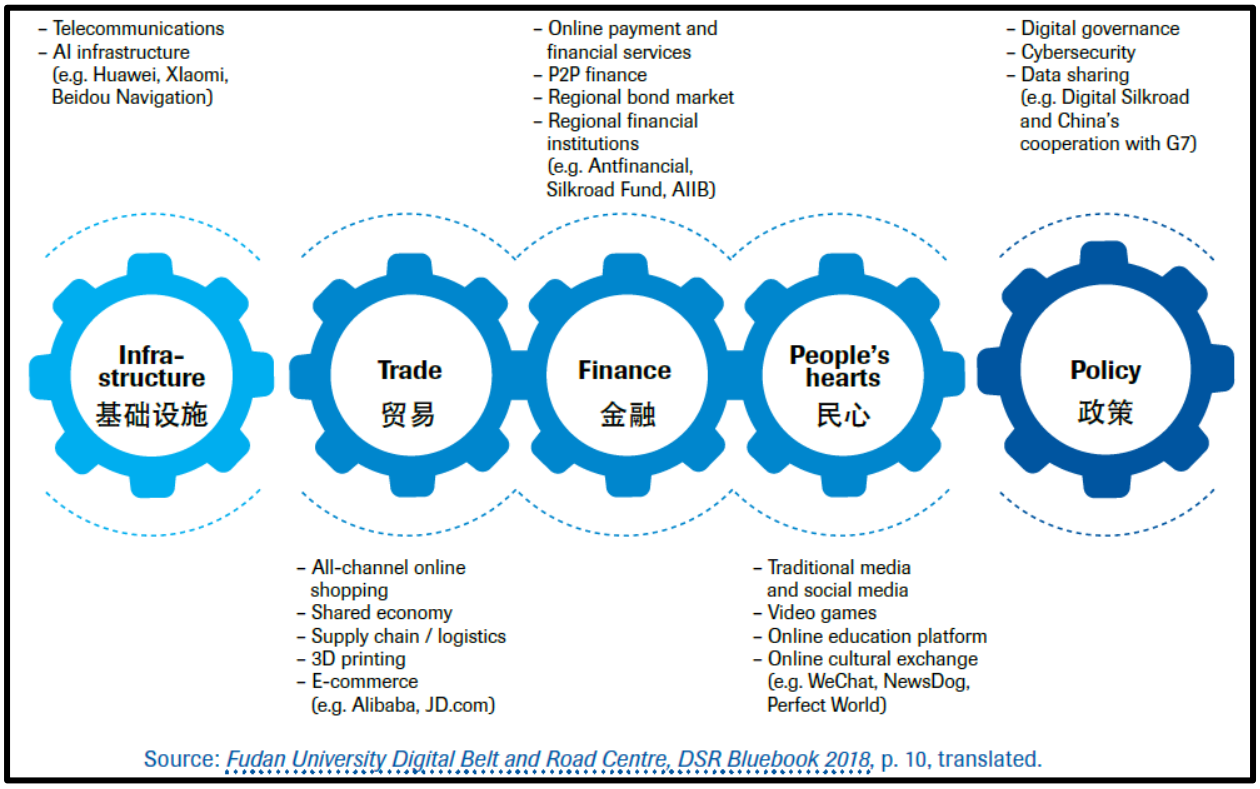
The conceptual framework of the economic–security nexus (based on non-traditional security challenges) suggests that in regard to new disruptive technologies (such as 5G), commercial interests and national (cyber) security risks are more than ever entangled and difficult to separate from one other.[6] Many new systemic cybersecurity risks are ultimately the result of globalisation, privatisation of the telecommunication sector and the accelerating digitalisation. They have often forced private telecommunication companies to prioritise costs and profits over security and national interests. As long as private companies consider cybersecurity investments a liability rather than a competitive advantage in the marketplace, cybersecurity of CI (based on the future 5G network) will hardly improve.[7] Governments and the public, for their part, have often overlooked cybersecurity threats as they often lack comparable independent technical expertise on 5G technology. Even in Europe, wider political and public debates began only after the US administration forced the EU member countries in 2018 to position themselves for Huawei's involvement in their 5G rollout.[8]

In the view of Western security experts, a worldwide Chinese 5G deployment could contribute to China's technology sector and its supply chains acquiring global dominance — and that too, at a time of an escalating technological arms race and rising geopolitical competition not just between the United

[3] See also "5G was going to unite the World — Instead it's tearing us apart", Wired.com, 2 July 2020.
[4] See also F. Umbach, "Europe and Huawei: Rising Cybersecurity Challenges", *Geopolitical Intelligence Service (GIS),* 2 April 2020.
[5] See also Xuewu Gu et al., "Geopolitics and the Global Race for 5G", CGS Global Focus, Centre for Global Studies (CGS), University of Bonn, May 2019.
[6] See also Muhammad Faizal Bin Abdul Rahman, "The Intersection of Emergent Technologies and Geopolitics: Implications for Singapore", RSIS Working Paper No. 327, 7 April 2020.
[7] F. Umbach, "Energy Security in a Digitalized World and its Geostrategic Implications", Konrad Adenauer Foundation study on Regional Project: Energy Security and Climate Change Asia-Pacific (RECAP), Hong Kong, September 2018.
[8] See also "America will Huawei-Technik aus Deutschland verbannen", *Frankfurter Allgemeine Zeitung (FAZ),* 24 November 2018, p. 19; James Kynge and David Bonge, "UK and Germany grow wary of Huawei as US turns up pressure", *FT*, 29 November 2019; Daniel Voelsen, "5G, Huawei und die Sicherheit unserer Kommunikationsnetze", *SWP-Aktuell* No. 5, Berlin, February 2019.

States and China, but also between the European Union and China.[9] Complementing Beijing's "Made in China 2025" concept, China's "Digital Silk Road" strategy, introduced in 2015, and its forthcoming "China Standards 2035" concept[10] (including for 5G) as well as its 2017 cybersecurity law and efforts for "digital sovereignty" could have wide-ranging global implications. They could influence international standards and global governance for future digital markets in UN institutions and networks, ultimately leading to conflict with core values, laws and constitutional rights in Western democracies.[11]

Figure 2: Key Aspects of China's "Digital Silk Road" Strategy of 2015



Source: Brigitte Dekker and Maaike Okano-Heijmans, "Unpacking China's Digital Silk Road", Clingendael Report, Netherlands, July 2020.

China has not only used its own cybersecurity laws and regulations to tighten its controls over its citizens and internet usage within the country; through the Cyberspace Administration of China, it also has initiated new, tighter cybersecurity review processes for any purchases for its own CI, and for the installation of new network equipment (servers, clouds, data software) and services in the country. While China demands unrestricted access to foreign markets for its companies and digital technologies,

[9] See also Mark Siemons, "Das Huawei-Paradox", *Frankfurter Allgemeine Sonntagszeitung (FAS)*, 17 February 2019, p. 35; F. Umbach, "Europe and Huawei: Rising Cybersecurity Challenges".

[10] "China Standards 2035" is a blueprint to define and set global standards for the next generation of technologies. See Alexander Chipman Koty, "What is the China standards 2035 Plan and how will it impact emerging industries?", *China Briefing*, 2 July 2020.

[11] See also James Kynge, "From AI to facial recognition: How China is setting the rules in new tech", *FT,* 7 October 2020; Brigitte Dekker and Maaike Okano-Heijmans, "Unpacking China's Digital Silk Road", Clingendael Report, Netherlands, July 2020; Andre Wheeler, "China's Digital Silk Road (DSR): The New Frontier in the Digital Arms Race?", Silkroadbriefing.com, 19 February 2020; and Anna Gross and Madhumita Murgia, "China and Huawei propose reinvention of the Internet", *FT*, 27 March 2020.

it has restricted the opportunities for foreign and multinational technology companies to penetrate its own market.[12] Both the United States and European Union have called for *reciprocal* market access as Huawei until recently had full access to all three markets (US, Europe and China), whereas foreign technology companies were denied comparable full access to the Chinese market. The Huawei case is just one example of many unfair trade competition conditions and the lack of reciprocal market access.[13] China's unified export-control law, including for AI and other disruptive technologies, which was adopted in October 2020, may further restrict the sale and export of technologies developed by US and European companies with extensive manufacturing and research and development (R&D) activities in China.[14]

Since 2018, the US government has demanded that its allies in Europe and Asia ban Huawei and its 5G technology because it would create huge cybersecurity risks involving industrial as well as political espionage.[15] The Trump administration has even threatened to restrict intelligence sharing with these allies as well as within the North Atlantic Treaty Organisation (NATO) alliance members. While many European allies generally share America's cybersecurity concerns in regard to Huawei, they have not been willing to impose outright bans on Huawei in their overall 5G deployment; instead, until the spring of 2020, they have merely sought to restrict its role.[16]

Washington's new sanctions on Huawei and new technology export controls in 2020 have not only opened a new US front against China;[17] they have also created new challenges for transatlantic relations and the European Union's China policies because the European Union can neither ignore US efforts nor refuse to engage with the US administration.[18] Despite its often counterproductive coercion diplomacies,[19] the Trump administration forced the European Union to rethink its 5G policies and its inadequate export controls for emerging technologies. It has also forced EU members to re-examine their ability to coordinate policies more effectively within their union as well as with transatlantic institutions.

[12] In March 2020, China's largest state-owned mobile telecommunication company, China Mobile, selected Huawei and ZTE almost exclusively to build its 5G mobile network domestically. See Ryan Mc Morrow and Nian Liu, "China Mobile picks Huawei and ZTE to build its 5G network", *FT*, 2 April 2020, and Simone McCarthy, "China's new cybersecurity rules could hit foreign service providers", *South China Morning Post (SMCP),* 28 April 2020.

[13] William H. Overholt, "Trump versus Huawei: Right Target, Disastrous Strategy", East Asia Forum, 21 June 2020.

[14] See also "China's New Export Control Law", *Merics-China Briefing*, Berlin, 22 October 2020.

[15] See also Kiran Stacey, "US accuses Huawei of stealing technology from six companies", *FT*, 14 February 2020; Guy Chazan, "Trump's ambassador to Germany hits out at Berlin over Huawei", *FT*, 25 November 2019.

[16] See also Demetri Sevastopuli and David Bond, "UK says Huawei is manageable risk to 5G", *FT*, 17 February 2019.

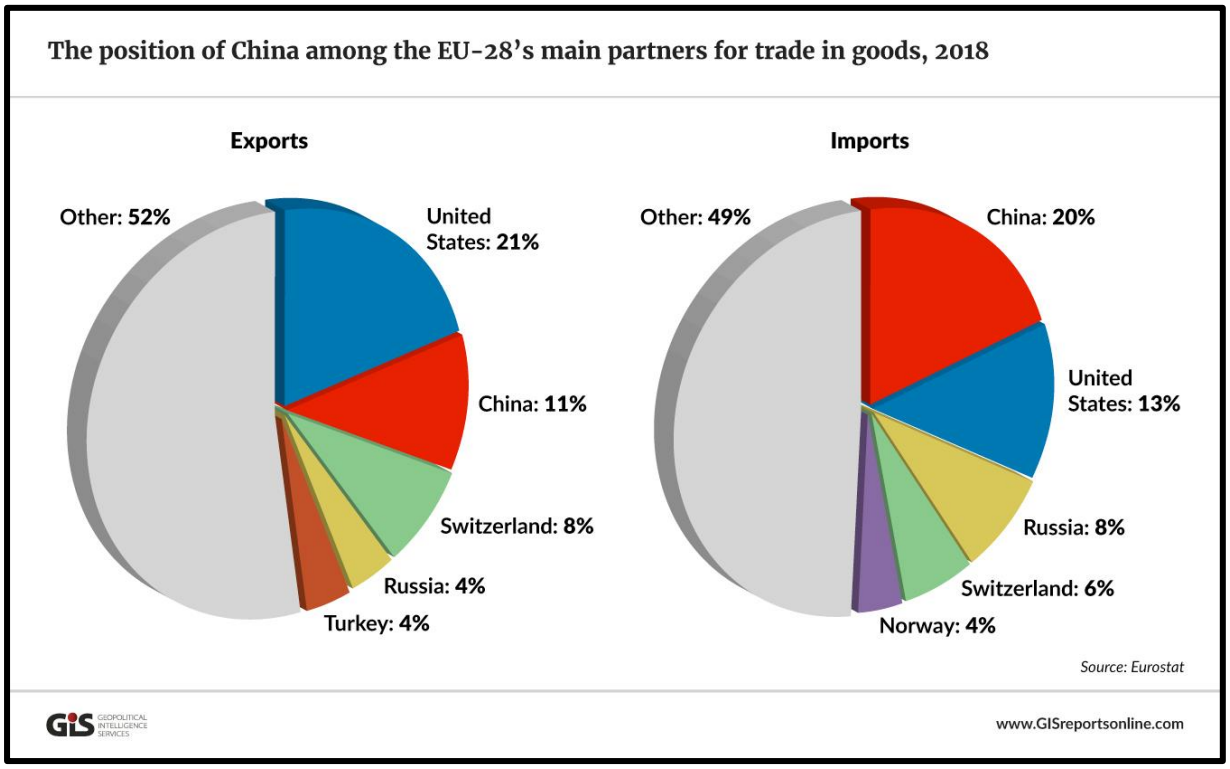
[17] See also "Inside the Fed's Battle against Huawei", www.wired.com, 16 January 2020.

[18] Noah Barkin, "Export Controls and the US–China-Tech War", *MERICS-China Monitor Perspective*, Berlin, 18 March 2020.

[19] See also Michael H. Fuchs, "How to lose friends and strain allies: Washington's partners aren't buying its China policy", *Foreign Affairs*, 12 March 2020.

Furthermore, the policies of the European Union and its member states towards Huawei's inclusion in their national 5G installation could be impacted by the wider EU–China relationship, which has been changing over the past two years and particularly in the last months. While China is the second largest trading partner of the European Union (after the United States), the European Union is China's largest trading partner. But the longstanding relationship is increasingly characterised by a growing asymmetric interdependency. By exploiting its "debt-trap diplomacy" and a "divide-and-rule" tactic towards the European countries, China has been increasingly perceived to weaken the political–economic unity of the European Union for maximising its own unilateral benefits, contrary to its often declared "win-win" cooperation. China's mercantilist trade and investment policies are perceived as challenging the European Union's economic interests in Europe and beyond. Consequently, the European Union is increasingly unwilling to support an "unequal partnership", which involves the sacrifice of its short-term interests in the long-term hope of integrating China into the Western-dominated global governance system.[20] Since 2019, the European Union officially views China not just as an economic partner, but simultaneously also as a "systemic rival".[21]

Figure 3: China's Place in EU Trade



Source: F. Umbach, "The Challenges of EU–China Decoupling", GIS, 6 October 2020.

Against this complex background, this working paper will examine the European Union's security, technological and economic–industrial policies as well as cybersecurity concerns and their strategic

[20] See also F. Umbach, "The Challenges of EU–China Decoupling", GIS, 6 October 2020.
[21] European Commission, "EU–China Strategic Outlook: European Commission and HR/VP Contribution to the European Council", 12 March 2019.

implications for 5G eco-systems in the context of the US–China–EU technology competition. It will analyse how the European Commission (and the European Network and Information Agency, ENISA) and the major EU member states (with a focus on the United Kingdom, Germany and France) balance the economic benefits of 5G and Huawei's inclusion with the inherent cybersecurity risks. The analysis will also consider whether the UK government's turnaround by banning Huawei from its 5G plans was just the result of US political pressure and/or also of the increasing assertive stance of the European Union in its relationship with China.

The paper will begin by reviewing US government policies, security discussions and pressure on its European allies to ban Huawei from the European Union's 5G rollout in the context of the geo-economic "technology arms race" and "digital decoupling" from China.[22] It will then undertake a comparative analysis of the 5G policies of the EC (and ENISA) and of the EU member states (with a focus on the United Kingdom, France and Germany). Particularly, it will look at their involvement of Huawei and the extent to which they have balanced the economic benefits of 5G with the potential cybersecurity risks. Finally, the paper will explore whether ASEAN can draw lessons from the European Union's collective cybersecurity policies that can be applied to its own 5G rollout. It will also examine the prospects for enhanced EU–ASEAN cooperation on the cybersecurity risks arising new disruptive technologies.

US Policies on China/Huawei and Pressure on Allies in an Era of "Weaponised Interdependence"[23]

The "technological cold war" on digitalisation, robotics and AI between the United States and China has intensified during the past year.[24] This new "cold war" has many more facets than the previous cold war between the West and the Soviet Union. Given its much larger population, economic and financial power as well as technology ambitions, China is, for both the United States and Europe, a far more formidable geo-economic and security challenge.[25] Coping with the new digital and cybersecurity challenges demands an ever closer collaboration between the civilian sector and the military industry as almost all AI technologies are developed by the former. This fact has also created unprecedented

[22] Despite the British exit from the European Union, the United Kingdom is still included in this analysis as its 5G policies since 2018, when it was still an EU member, have been a model for ENISA as well as for EU member states. The United Kingdom will also in the future closely collaborate with the European Union in all aspects of intelligence-sharing, cybersecurity cooperation as well as on China in general. The European Union, for its part, has a strategic interest in cooperating with the United Kingdom even after a hard Brexit as Britain's institutionalised cybersecurity expertise and engineering capabilities in data analysis software are considered the best in Europe.

[23] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion", *International Security* 44, No. 1 (Summer 2019), pp. 42–79.

[24] Adam Segal, "When China rules the web: Technology in service of the state", *Foreign Affairs*, September/October 2018, pp. 11-18; Ariel E. Levite and Lyu Jinghua, "Is there common ground in US–China cyber rivalry?", Thecipherbrief.com, 15 March 2020; F. Umbach, "Globaler Wettlauf bei Künstlicher Intelligenz und Digitalisierung. Geopolitische Dimensionen", *Europäische Sicherheit & Technik (ES&T)* 05/2020, pp. 39-43; F. Umbach, "The US–China AI Race: A 'Third Way' for Europe?", *GIS,* 25 April 2019; Cecilia Kang and Alan Rappeport, "The New US–China Rivalry: A Technology Race", *New York Times (NYT)*, 6 March 2018; "The Coming tech war with China", Stratfor.com, 6 February 2018; and Richard Staropoli, "America's New Digital Cold War with China", *FT*, 3 April 2018.

[25] See also John Thornhill, "China Is setting itself up to win Cold War 2.0", *FT*, 15 June 2020.

challenges for control of the emerging technologies since they are all dual-use in nature. China's unrivalled military–civil fusion strategy seeks to exploit systematically any new emerging technology for both civilian and military use.[26] In response to these challenges and China's efforts to steal foreign technologies as well as patents,[27] American and other Western universities as well as research centres have begun to cut their ties with Chinese telecommunication companies such as Huawei and ZTE.[28]

Huawei's 5G policies are a perfect example of China's long-term thinking, which involves defining future disruptive technologies as well as industry applications and seeking strategic control of global supply chains, ranging from R&D to critical raw materials up to semi-finalised products and finally global installation and application of these new technologies and related hardware.[29]

In this context, Europe has become a major battlefield of Chinese and US ambitions for technology prowess, while the European Union is trying to develop a "digital sovereignty" of its own. The United States, the European Union and China have moved in separate digital directions. This is occurring at a time when enhanced transatlantic cooperation is needed more than ever, given that the United States and European Union share interests in defining global standards and long-term strategies for the new digital and other disruptive technologies as well as global digital governance.[30] As a result, a bi- or tri-polar world is emerging, in which China as the biggest digital miner, could dominate the world, sharing private, political and commercial data that it controls with an increasing number of authoritarian countries. In the view of Western observers, a Chinese-dominated cyberspace will be less global and open, will restrict free speech, and limit worldwide digital exchanges owing to its overriding strategic interest in entrenching the political power of the Communist Party of China.[31]

Huawei became the world's largest 5G network provider because China's huge government subsidies allowed the company to market its technologies at prices 20–30 per cent lower than those of its

[26] See also Kathrin Hille, "Washington unnerved by China's 'military–civil fusion", *FT*, 8 November 2018.

[27] Both the United States and European Union as well as many independent cybersecurity experts have accused China of long-term cyber economic espionage involving the theft of technologies and patents as well as sensitive company and trade data. See Christopher Bing, "US cybersecurity experts see recent spike in Chinese digital espionage", Reuters, 25 March 2020; International Institute for Strategic Studies (IISS), "Asia-Pacific Regional Security Assessment 2019", Chapter 5 ("China's Cyber Power in a New Era"), IISS, 2019; National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace 2018", Washington, DC, 2018; Mike Giglio, "China's Spies are on the offensive", *The Atlantic*, 26 August 2019; *IPI Global Observatory*, "What are China's Cyber Capabilities and Intentions?", 22 March 2019; Jordan Robertson and Michael Riley, "The big hack: How China used a tiny chip to infiltrate U.S. Companies", *Bloomberg Businessweek,* 4 October 2018; FireEye Insight Intelligence, "Redline dawn: China recalculates its use of cyber espionage", Special Report, June 2016; Yuan Yang and Ben Bland, "Who is the Chinese group blamed for cyber attacks on the West?" *FT*, 21 December 2018; and Robert Potter, "Cybersecurity: The China problem", *Pacific Forum*, 28 June 2018.

[28] Louise Lucas, Nicole Liu and Henny Sender, "MIT cuts partnerships with China's Huawei and ZTE over risks", *FT*, 4 April 2019, and Madhumita Murgia and Christian Shepherd, "Western AI researchers partnered with Chinese surveillance firms", *FT*, 19 April 2019.

[29] F. Umbach, "Energy Security in a Digitalised World and its Geostrategic Implications", and F. Umbach, "The new 'rare metal age': New Challenges and Implications of Critical Raw Materials' Supply Security in the 21st Century", RSIS Working Paper No. 329, RSIS, 27 April 2020.

[30] Rana Foroohar, "Europe and the US can still compete with Chinese tech", *FT*, 19 July 2020, and Rosemary Foot, "Shaping from Within: a UN with Chinese Characteristics?", East Asia Forum, 3 August 2020.

[31] See also James Kynge, "China's tech juggernaut steams ahead", *FT*, 24 July 2020, and Ariel E. Levite and Lyu Jinghua, "Is there common ground in U.S.-China cyber rivalry?"

European competitors.[32] Chinese state-owned banks have made some US$100bn of credit available to Huawei customers, on terms ranging from interest-free loans, repayment holidays and loan periods running up to 30 years. Huawei had access to as much as US$75bn in state support over the past years. Without these massive government subsidies, Huawei's EU market share would have been significantly lower.[33]As Huawei's technologies are still intentionally very hardware-centric, making them incompatible with technologies produced by most of their rival vendors. This creates path dependencies over several technology generations. Although Western telecommunication and other technology companies are also trying to restrict the ability of their technologies to interface with third party technologies, they are obliged to comply with regulations favouring consumer choice and restricting path dependencies that create technology monocultures.

Amid a hardening China policy[34] and growing domestic consensus on China policy in the United States,[35] Huawei had already been blacklisted by the US Commerce Department in 2019: US companies were required to obtain a licence to sell electronics and software to Chinese telecommunication companies. Nevertheless, Huawei boosted its spending with US suppliers by 70 per cent last year.[36]

[32] Being able to define standards can give hardware producers numerous advantages against their competitors, who may find it difficult to develop products that are compatible with their hardware. Robert D. Atkinson, one of the most well-known experts on the telecommunication industry, 5G and Huawei, has criticised the past US and European lack of attention to Huawei's rise to global 5G leader through government subsidies and cyber-theft of competitors' intellectual property. The world was oblivious as China increasingly took control of international standards groups. Huawei and ZTE's rise in global market shares has only been possible with Chinese government support against their more innovative international competitors since 1979. Beijing's "innovation mercantilism" has also limited foreign access to China's own huge telecommunication markets and allowed its own companies to grow. Huawei has also benefitted by saving as much as US$25bn in taxes between 2008 and 2018 owing to state incentives to promote China's telecommunication industry. China has provided more funding each year to support its digital exports than the 36 member states of the Organisation for Economic Cooperation and Development (OECD) combined. Huawei's ability to spend significantly less on R&D than Nokia and Ericsson but achieve a higher patenting rate is attributed to Beijing's alleged orchestrated theft of intellectual property. Moreover, the trustworthiness of Chinese companies is in question, with the likes of Huawei and ZTE lacking transparency in financial reporting and other compliance rules that their Western counterparts are subjected to. While Huawei appears as the world leader in 5G patents by numerical counts, other studies have used global market shares as an index and adjusted the ranking accordingly. Consequently, Nokia and Ericsson rank ahead of Huawei. Furthermore, the quality of the 5G patents registered by Ericsson, Nokia and Samsung is on average still higher than that of Huawei and ZTE's. In Atkinson's view, arguments by Huawei and other Chinese companies that having more suppliers means greater competition needs to be questioned as having more Chinese suppliers effectively means less innovation. Limiting the market shares for Huawei and other Chinese companies is considered a precondition for making way for new 5G network suppliers (such as Samsung) with small but growing 5G market share. See the enlightening study by Robert D. Atkinson, "How China policies have undermined global innovation in the Telecom Equipment Industry". *Information Technology & Innovation Foundation (ITIF)*, June 2020.

[33] Robert D. Atkinson, "Comments on the European Commission's White Paper on Foreign Subsidies", ITIF-Comments, 2 September 2020.

[34] In June 2020, the Pentagon compiled a new list of 20 Chinese companies with ties to the PLA. This was a response to China's military–civil fusion strategy to blur the lines between the civilian and military sectors. See Demetri Sevastopulo and Katrina Manson, "Pentagon lists 20 companies aiding Chinese military", *FT*, 25 June 2020.

[35] On the wider US discussions on China and European perceptions of China, see Philip Stephens, "A cold war does not answer China's challenge", *FT,* 30 July 2020; and Michael Swaine, "Why the world needs a saner US approach to China", *SCMP*, 30 July 2020.

[36] Nic Fildes/James Kynge, "Huawei spending with US companies surges despite sanctions", *FT*, 31 March 2020.

In May 2020, the US Commerce Department adopted new export-control restrictions on semiconductors for closing loopholes in the previously adopted sanctions and export controls. The restrictions also cover manufacturing equipment, software and technology.[37] The new sanctions expand the scope of coverage to include foreign companies using US chip-making technologies. These companies (notably, Taiwan Semiconductor Manufacturing/TSMC, the world's largest contract chipmaker, which also controls half of the world's market for made-to-order chips) would now require an export licence from the United States before selling chips to Huawei.[38] For Huawei, as the world's third largest buyer of semiconductors in 2019 (behind Apple and Samsung), it has become almost impossible to find a fabrication plant anywhere in the world that could still work with it. Huawei, according to its CEO, has to fight now for "survival" following the US "death sentence".[39] The new US sanctions and export controls for key computer chips will also have wide-ranging impacts on global technology supply chains and what some analysts call the "new national security economy".[40]

The United States has also supported the European rivals of Huawei, the Swedish telecommunication company Ericsson and Finland's Nokia.[41] Despite its demands that its European and Asian allies exclude Huawei from their future 5G networks, Washington itself is facing a dilemma as no US company can currently offer any real 5G alternative to Huawei. Worldwide, only Nokia and Ericsson, and to a lesser extent Samsung of South Korea, can currently provide alternative 5G networks. New options may become available, particularly for the core networks, through Oracle from the United States and the Japanese group Rakuten as well as Samsung, which all have expanded their R&D activities and commercial businesses, supported by their respective governments.[42] Rakuten and others are developing an open-source-based 5G network at scale as an alternative to Huawei's and Ericsson's technologies.[43]

[37] See also Michael E. Leiter, "Commerce Department's new export-related restrictions inhibit semiconductor design by and manufacturing for Huawei", www.skadden.com, 18 May 2020; and "Huawei chip unit said to be switching orders from TSMC to SMIC as US restrictions loom", *SMCP*, 17 April 2020.

[38] About 40 per cent of the world's chipmakers are using US machines. See Kathrin Hille, "US 'surgical' attack on Huawei will reshape tech supply chain", *FT*, 19 May 2020; and Kathrin Hille and Kiran Stacey, "TSMC fails into line with US export controls on Huawei", *FT,* 9 June 2020.

[39] Kathrin Hille, "Huawei says new US sanctions put its survival at stake", *FT*, 18 May 2020.

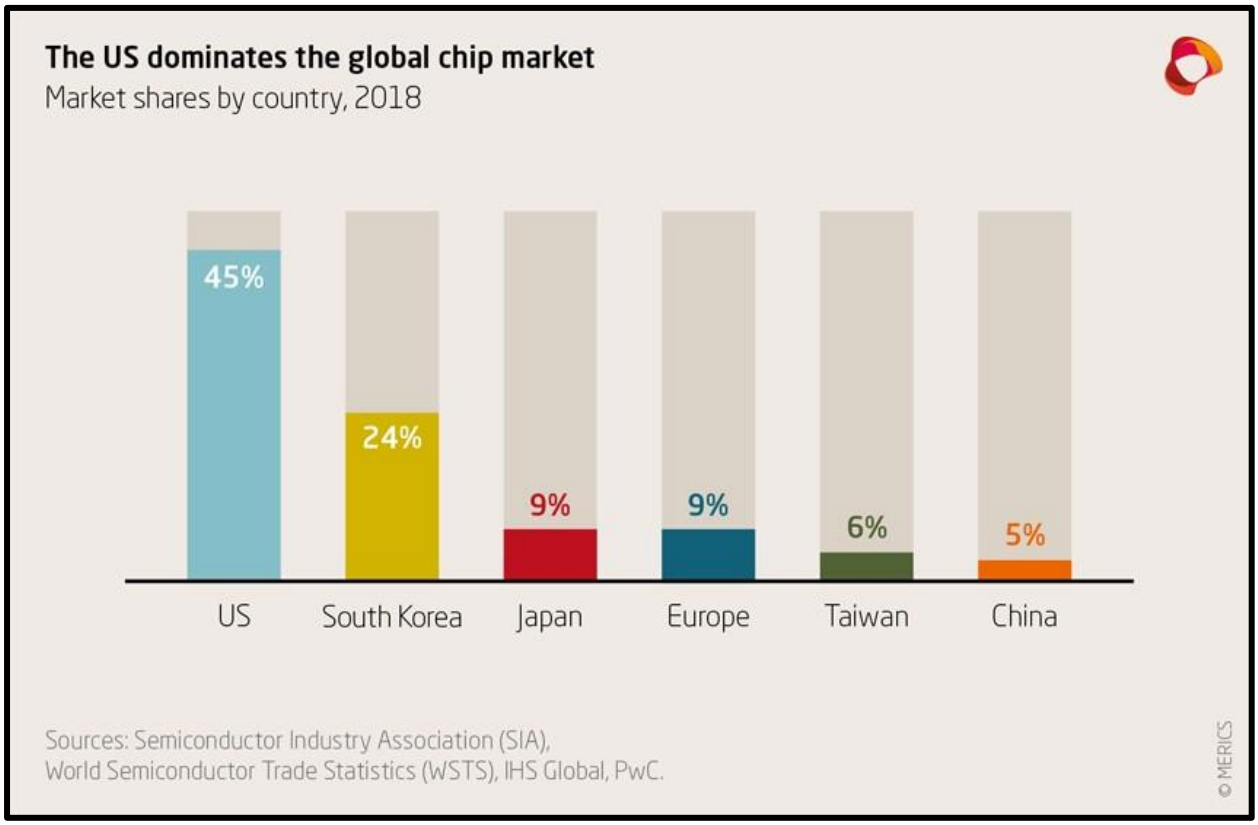
[40] See also Torsten Riecke, "Resilience and decoupling in the era of great power competition", MERICS, Berlin, 20 August 2020; Kathrin Hille, "Huawei says new US sanctions put its survival at stake", *FT*, 18 May 2020; and Brad Glosserman, "Business must brace for the new security economy", East Asia Forum, 12 February 2020.

[41] US Attorney-General William Barr even advocated that the US government acquire shares in the Swedish and Finnish telecommunication companies either directly or indirectly through US companies. See Richard Milne, "Nokia and Ericsson remain vulnerable in geopolitical 5G tussle", *FT*, 2 July 2020.

[42] "Ericsson/5G: Tough Call", *FT*, 17 July 2020.

[43] Nic Fildes, "Telecoms network look to fix Huawei problem with open-source software", *FT*, 27 June 2020.

Figure 4: The Global Chip Market



Source: Torsten Riecke, "Resilience and Decoupling in the Era of Great Power Competition", MERICS, Berlin, 20 August 2020, p. 3.

At the end of June 2020, the US Federal Communications Commission officially designated Huawei and ZTE as "national security threats" to the US national communications networks and 5G gear.[44] The Trump administration subsequently framed its anti-Chinese telecommunication policies as the "5G Clean Network" initiative. The initiative aims to build a "coalition of like-minded countries and companies" to secure CI against "malign actors such as the Chinese Communist Party".[45] A new requirement is that network traffic entering US diplomatic facilities should have an end-to-end "clean path" involving clean network carriers, clean app stores, clean apps, clean cloud services and clean undersea cables that do not include any equipment from Chinese companies.[46] Other projects under US leadership seek to promote "Open Radio Access Networks (O-RAN)" as a global 5G alternative to Huawei's technology. All these US initiatives seek to disconnect and remove Chinese telecommunication operators from the digital networks of the United States and its allies. But even if O-RAN networks are equipped entirely by US and European gear, they would still be based on Chinese patents.[47]

---

44 Demetri Sevastopulo, "Huawei and ZTE classified as security threat to US", *FT*, 1 July 2020; Eduard Kovacs, "Chinese companies Huawei and ZTE declared national security threats by FCC", www.securityweek.com, 1 July 2020.

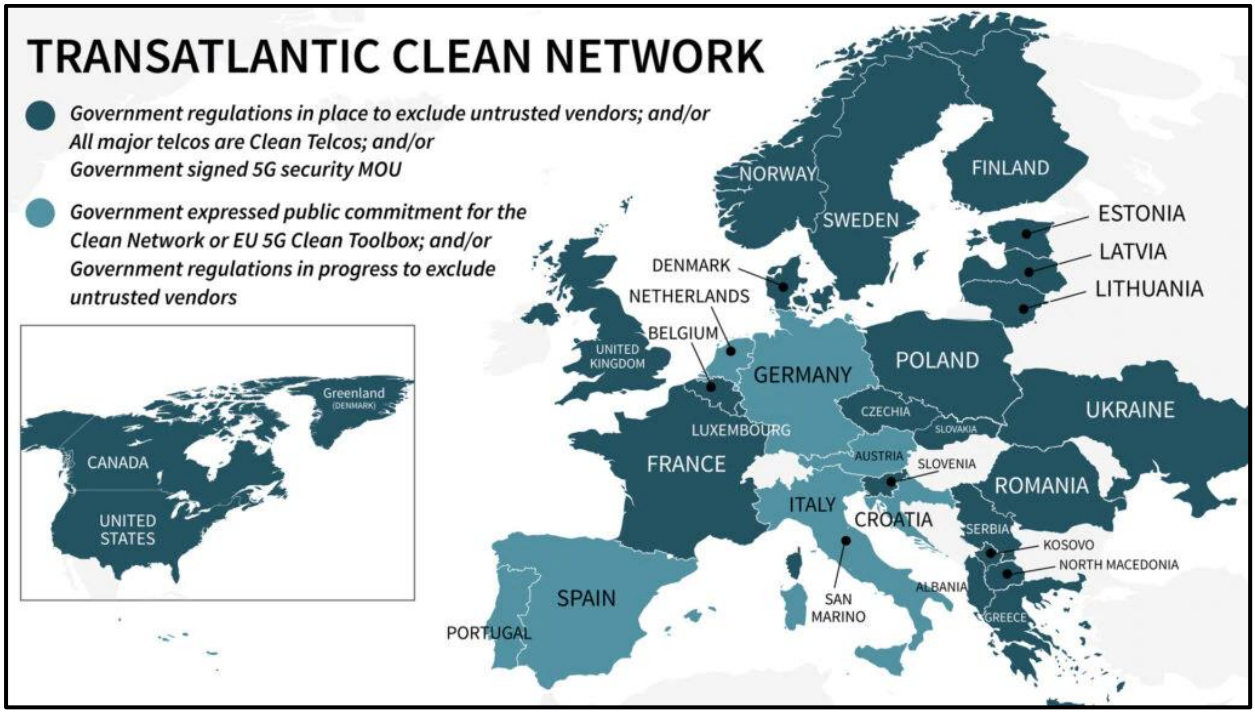
45 US Department of State, "The Clean Network", August 2020, https://www.state.gov/the-clean-network/.

46 Michael R. Pompeo, "Announcing the expansion of the clean network to safeguard America's Assets", US Department of State, 5 August 2020.

47 See also John Lee, "The Global war for 5G heats up", *The Diplomat*, 31 July 2020.

Decoupled from US technology companies, Huawei has turned to European suppliers and collaborative projects such as open-source projects in which hardware and software codes are made freely available for anyone to use, modify and redistribute as an alternative to licences sold by large companies. For China, this approach offers an alternative to US supplies, allowing for technological self-sufficiency as it reconciles itself to decoupling from the United States.[48] Meanwhile, Google, Microsoft and other leading US technology companies have already begun to relocate some production capacity from China back to the United States or other countries (e.g., Vietnam, India and Mexico).[49]

Figure 5: US "5G Clean Network"



Source: US State Department

Australia, New Zealand, Japan, Taiwan, Singapore and India have already banned Huawei and other Chinese telecommunication companies (like ZTE) from their networks,[50] while countries like Argentina, Brazil, Russia, the Philippines and Thailand have all welcomed China's 5G technology. For security reasons, Russia favours Huawei's 5G technologies over that of its Western rivals, considering the

[48] Raha Foroohar, "China wants to decouple from US tech, too", *FT*, 6 September 2020; Lauly Li and Cheng Ting-Fang, "Huawei builds up-2 year reserve of 'most essential' US chips", *FT*, 8 June 2020; Caroline Meinhardt, "Open Source of Trouble: China's Efforts to Decouple from Foreign IT Technologies", MERICS Blog, 18 March 2020.

[49] See also Eurasia Group, "Global sanctions present complex web of risks for multinationals", 18 August 2020.

[50] Jamie Smyth, "Australia bans China Huawei's 5G rollout over security fears", *FT*, 23 August 2018; "Australia, Huawei and 5G", IISS Strategic Comments 28, Vol. 25, October 2019; Amy Kazmin and Stephanie Findlay, "India moves to cut Huawei gear from telecoms network", *FT*, 24 August 2020; Archana Chaudhary et al., "China's Huawei, ZTE set to be shut out of India's 5G Trials", Bloomberg, 14 August 2020; Amalina Anuar, "5G in Singapore: Is the tide turning against Singapore?", East Asia Forum, 11 August 2020.

former a “lesser evil”.[51] Meanwhile, the United States is no longer putting pressure just on its European and Asian allies but also on numerous other countries.[52]

EU Policies: Balancing Competing Interests and Concerns and Maintaining Political Cohesion

The Huawei Challenge for EU Digital Sovereignty and Impact of Changing EU–China Policies

In deciding on the inclusion of Huawei’s technologies, EU member states need to consider complex as well as difficult conflicts of interests. They need to balance the shorter and longer-term strategic interests of industry, technology, and cybersecurity. Although the EC has been given more authority and sovereignty, officially, it can still only recommend cybersecurity guidelines and leave it to individual members to take responsibility for the technological sovereignty of the 5G network build-up and Huawei’s involvement in it. In reality, however, the cybersecurity recommendations and guidelines of the EC and ENISA have been increasingly implemented — albeit often slowly and with differing speeds across the EU owing to various national conditions.[53]

The situation is complicated for various reasons:

- Private Western telecommunication companies have already entered into technology cooperation with Huawei for the rollout of the 3G/4G wireless network since the 1990s. The deployment of 5G technology will be built upon the 3G/4G network and thus will create mixed or hybrid network infrastructures. Restricting Huawei’s technologies in both the core and periphery networks would require dismantling and replacing many Huawei technologies that have already been installed. In the industry view, this would be very costly.[54]
- Technology cooperation between European and Chinese companies as well as universities and research centres has significant commercial and academic benefits.[55] Technology supply chains are deeply intertwined.[56] A technology decoupling from China could be even more costly for Europe than for the United States.[57]

[51] Alexander Gabuev, “Huawei’s courtship of Moscow leaves West in the cold”, *FT*, 21 June 2020.
[52] “Brazil may face consequences if it gives Huawei 5G access, says US ambassador”, Reuters, 29 July 2020.
[53] For an overview of the European Union’s cybersecurity policies see the website of the EC, https://ec.europa.eu/digital-single-market/en/cyber-security. See also European Commission, “Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy”, 24 July 2020; and European Policy Centre, “Responding to Cyberattacks: Prospects For The EU Cyber Diplomacy Toolbox”, Brussels, 18 March 2019.
[54] Nic Fildes, “Ericsson chief warns Huawei fears will be add to Europe’s 5G delay”, *FT*, 19 February 2019.
[55] See also Caroline Meinhardt, “Open source of trouble: China’s efforts to decouple from foreign IT technologies”.
[56] See also Rana Foroohar, “One world, two systems in the 5G Race”, *FT*, 17 February 2020.
[57] F. Umbach, “The challenges of EU-China decoupling”.

- Ericsson and Nokia themselves have been relying on China's manufacturing capacity and its R&D facilities since the 1990s. As of 2018, 45 per cent of Ericsson's and 10 per cent of Nokia's manufacturing facilities was located in China.[58]
- Owing to their countries' rising economic dependence upon China, all European governments fear economic repercussions in their bilateral trade and economic relationships if they were to exclude Huawei.
- The new US sanctions on chips have raised uncertainty whether Huawei would still be able to contribute its components, equipment and software for the European 5G rollout, as highlighted in the section on the United Kingdom (see below).

In addition to US pressure, the European Union's Huawei and 5G policies are increasingly influenced by its own overall shifting policies towards China.[59] Both Huawei and the governments of the EU member states are also facing new challenges in regard to private data protection in Europe. The digitalisation policies of European government have enshrined data privacy as an important legal and constitutional right that needs to be respected. They can no longer ignore this aspect in their 5G rollout and the question of Huawei's inclusion. In July 2020, the European Court of Justice (ECJ) invalidated the "Privacy Shield" data agreement between the European Union, Switzerland and the United States by noting that government surveillance practices in the United States may override data privacy obligations. The trilateral agreement was designed to provide EU, Swiss and US companies with a mechanism to comply with data protection requirements for transferring personal data (e.g., for payroll or cloud services) in support of transatlantic commerce. The ECJ ruling called on the European Union to re-negotiate and revise the trilateral agreement with a higher level of data protection for its citizens (including with actionable rights in court against the US government).[60]

There is no majority in the outgoing US Congress for revising the trilateral agreement to accommodate the ECJ's objections, although the situation could change if a Biden administration supports such a revision and is able to influence the incoming Congress.[61] In the meantime, European data controllers could be required to switch to service providers in the European Union or in a country with an appropriate level of data protection until a new trilateral agreement is negotiated. The impasse may also force European governments to hasten their efforts to build European clouds to guarantee better data protection (compared with US clouds), in line with the EU's General Data Protection Regulation (GDPR).

[58] Yixiang Xu, "Has Merkel undermined European coherence on 5G network security?", AICGS, 24 October 2019, and Xuewu Gu et al., "Geopolitics and the Global Race for 5G", pp. 39 ff.

[59] Jim Brundsen, Sam Fleming and Alan Beattie, "EU ill-equipped to face China and US, Brussels trade chief warns", *FT*, 9 October 2019; F. Umbach, "EU–China Relations at the crossroads", *GIS*, 20 June 2019; F. Umbach, "Focus Germany: relations with China in perspective", *GIS*, 8 October 2019, and Zsuzsa Anna Ferenczy and Junjie Ma, "The EU and China: Partners or Rivals in an Emerging World Order?", *Pacific Forum*, 4 December 2019.

[60] Axel Spies, "No more data from Germany? European Court of Justice invalidates the EU–US. Privacy Shield", AICGS, 23 July 2020.

[61] Dominique Shelton Leipzig, "US should seize chance to end data-sharing stand-off", *FT*, 16 September 2020.

The even more interesting question deriving from the ECJ ruling is how private data protection can be achieved with countries with which the European Union does not even have such an agreement? In the case of the Chinese government and its obsessive governmental surveillance system, the prospect for any comparable bilateral agreement between the European Union and China is even more unrealistic. The installation of equipment from Huawei and other Chinese telecommunication companies in European 5G networks will make any legal transfer of personal data even more challenging as China's much more restrictive 2017 Cybersecurity of Law and its 2014 Espionage Law do not offer any protection for individual rights against the state. In contrast to the EU's GDPR, China's Cybersecurity Law does not envisage restrictive compliance requirements for data localisation or an independent entity to enforce its law; instead, China's law subordinates individual data rights to any governmental interpretation of national security.[62]

The EC's 5G Policies

The Commission's 5G Plans

The EC had already launched a "Public–Private–Partnership (PPP)" programme in 2013 for future 5G development. In 2016, it published an action plan for a timely deployment of 5G and called for a coordinated approach. The European Union set a target of covering all urban and all major terrestrial transport paths with uninterrupted 5G networks by 2025.[63]

But concrete strategies for large-scale 5G rollout are implemented by individual member states. National conditions vary widely for existing fibre infrastructure, public funding schemes and 5G auctions for network operators. Effectively, the network of operators and the market for mobile networks are highly fragmented.[64] In 2018, an EU Observatory was created to aid the EC in monitoring the progress in implementing the action plan of 2016. For expanding 5G coverage, the EC has developed new instruments for connecting schools, hospitals, cities and local administrations such as the "European Electronic Communications Code", which will be applied in December 2020 for creating an investment-friendly environment. It has also developed the "Connecting Facility Digital" regulation and set up European structural investment funds.[65]

The original plans for 5G rollout had been based almost exclusively on economic and industrial considerations in competition with rival Chinese and US 5G installations. Initially, 5G had been viewed

[62] See also Brigitte Dekker and Maaike Okano-Heijmans, "Unpacking China's Digital Silk Road", Clingendael Report, Netherlands, July 2020, p. 11 f.

[63] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*:* 5G for Europe: An Action Plan", COM (2016) 588 final, 14 September 2016.

[64] See also Peggy Hollinger and Nic Fildes, "Slow 5G rollout risk to Europe's supply chains, warn industrialists", *FT*, 18 September 2020.

[65] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Secure 5G deployment in the EU — Implementing the EU Toolbox", COM (2020) 50 final, 29 January 2020.

almost entirely through the prism of economic growth, digitalisation, and job creation. The cybersecurity challenges of next-generation 5G networks had been somewhat ignored until 2018. But during the past years, the EU's cybersecurity concerns have grown significantly in tandem with the accelerating pace of digitalisation, industry 4.0 and AI technologies and owing to rampant cyber espionage, theft of intellectual property and technologies or disinformation campaigns by foreign powers. Most of the advanced cyber threats have been linked with foreign powers and attributed to Russia and China.[66] The steady, but slow progress the European Union made in addressing cybersecurity challenges and developing as well as implementing mitigating security measures for the 5G eco-system has clashed with the speed of the 5G rollout in many member states.

In March 2019, representatives from 30 EU, NATO, and other countries (including the United States, Germany, Japan and Australia) attended a cybersecurity conference in Prague. They agreed on a set of non-binding security proposals for future 5G networks and on their impacts on policy, technology, economies and security, with general recommendations for how best to mitigate potential security risks.[67]

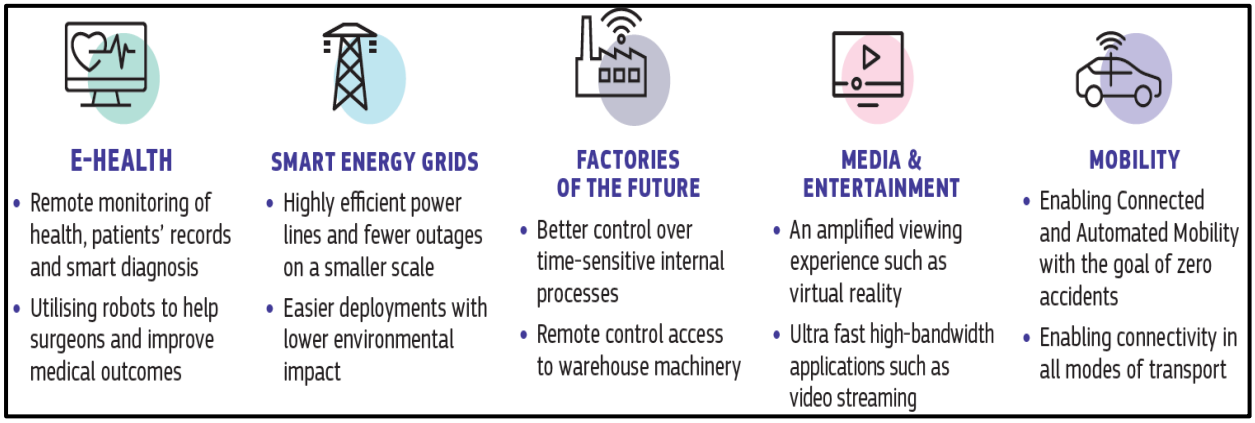
In July 2020, the European Union for the first time imposed sanctions against cyber attackers such as a unit of Russia's military intelligence agency or GRU and a Chinese technology company, Tianjin Huaying Haitai Science and Technology Development Company Ltd.[68] The EU's cyber sanctions regime includes a toolbox comprising travel bans and asset freezes to deter cyberattacks. But these sanctions are applied only to persons and entities; applying them to national governments is a political decision that requires unanimity among EU member states. However, consensus building within the European Union has improved in light of increasing cybersecurity challenges during the past years.
In January 2020, the EC published a report on the security challenges inherent in the forthcoming 5G networks. This was intended to avoid any widespread disruption, given the interconnected nature of digital eco-systems. The Commission, along with its member governments, had already called in 2019 for concerted action against the security risks of 5G.

[66] In contrast to the United States, the EU and other European governments (e.g., Germany) as well as European industries and companies had been reluctant until the spring of 2020 and the outbreak of the Covid-19 pandemic to explicitly accuse China of conducting cyberattacks and cyber espionage campaigns. However, based on my interviews with the German secret services and EU intelligence experts as well as larger technology companies (e.g., Siemens) during the past years, their conclusions have not been very different from the analysis of US intelligence agencies. See also Samuel Stolton, "Von der Leyen: Chinese cyberattacks on EU hospitals 'can't be tolerated'", Euractiv, 24 June 2020; Laurens Cerulus, "Von der Leyen calls out China for hitting hospitals with cyberattacks", Politico, 22 June 2020; Stuart Lau, "EU leaders talk tough to Beijing over long list of unmet promises", *SCMP*, 23 June 2020; Patricia Weiss and Ludwig Burger, "Bayer contains cyber-attack it says bore Chinese hallmarks", Reuters, 4 April 2019; Helen Warrell and Katrina Manson, "State-backed hackers using virus to increase spying, UK and US warns", *FT*, 8 April 2020; "BASF, Siemens, Henkel, Roche target of cyber-attacks", Reuters, 24 July 2019; "Chinesische Hacker greifen EADS and ThyssenKrupp an", Spiegel-Online, 24 February 2013 and "Maxim Worcester, "China's Growing Spy Threat", PMG-Denkwürdigkeiten, No. 88, February 2014.

[67] Government of the Czech Republic, "Prague 5G security conference announced series of recommendations: The Prague proposals", Press advisories, 3 May 2019, https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-propos.als-173422/.

[68] "EU Sanctions on Russian, Chinese 'Cyber *Attackers"*", www.securityweek.com, 30 July 2020.

Figure 6: 5G Networks for Critical Infrastructure and Industrial Applications



Source: European Commission 2020

Despite the deeply intertwined technology supply chains between the European Union and China, the former can neither ignore the manifold cybersecurity risks arising from involving Huawei and other Chinese telecommunication companies nor can it just capitalise on the US–Chinese rivalry and US sanctions policy to embrace these Chinese companies because wider transatlantic economic and security interests are at stake. Furthermore, the growing perception that China is pursuing mercantilist and nationalistic policies has changed the European Union's economic, industry and security interests with respect to China.

However, given the economic fallout of the Covid-19 global pandemic, the European Union does not want to decouple from China, as the United States is doing. The room to pursue political–diplomatic manoeuvres to balance the European Union's relationship between the United States and China has clearly been constrained. Europe has also overlooked the new challenges of export controls for emerging technologies. It is now being forced to take clearer positions but seeks to avoid the impression that it is merely giving in to US pressure.[69]

Some European representatives have spoken up in defence of Huawei, arguing that the US "Patriot Act" allows the US government to use national security grounds to make similar demands for private data from US companies (including those that store the private data of European citizens in their European clouds). But US secret services (and the secret services of the EU members) are supervised by parliamentary control committees and operate under the rule of law in contrast to China's secret services. Every major Chinese company has a party committee embedded at the highest levels of its management structure. Its employees worldwide can be forced to undertake espionage activities at any time and, in return, receive rewards or, in the event of non-compliance, face retaliation, including even against family members still living in China. Thus, any comparison

[69] Noah Barkin, "Export controls and the US-China tech war". MERICS China Monitor Perspectives, 18 March 2020.

between US and Chinese secret services, their political control and compliance with laws needs to take into account the very core and nature of the different political systems and conditions.[70]

However, the European Union's cybersecurity policy has also become more ambiguous as the security services of some member states have called on technology companies to allow them "exceptional access" to encrypted digital communications used by criminals and hostile governments that they themselves may be unable to crack. Domestic debates for developing stronger privacy protection have forced technology companies to develop more secure end-to-end encryption. But the flip side of this trend is that law enforcement agencies find it increasingly difficult to crack strongly encrypted messages.[71]

Systemic Cybersecurity Risks of 5G Networks

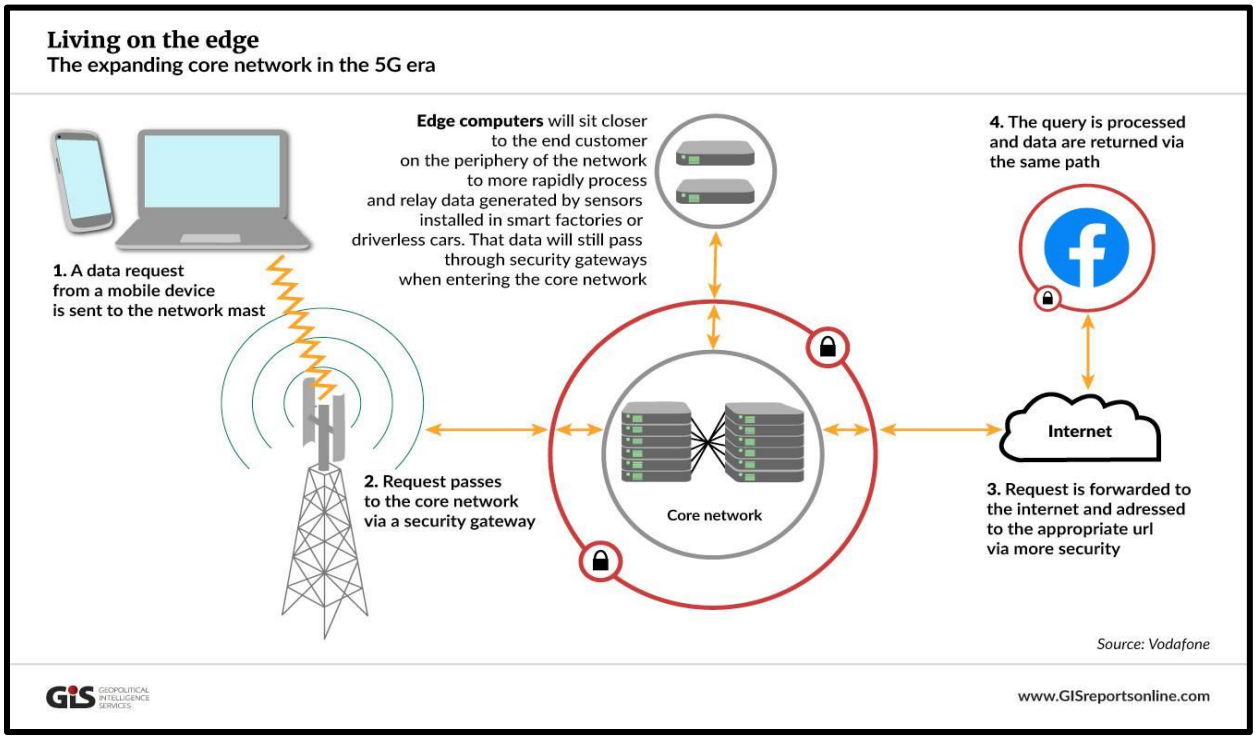
There are rising systemic cybersecurity challenges in 5G networks that all European deployments of the technology will have to cope with. And, these are by no means limited to the inclusion of Huawei. The following are some of the challenges:[72]

- The build-up of national 5G eco-systems will connect the future networks of a country's CI with millions of unsafe IoT appliances. These connections can open the doors to cascading cyberattacks on CI and Industry 4.0. With every additional connection, it becomes harder to figure out the vulnerabilities of the system despite enhanced encryption, authentication, privacy protocols, integrity protection and overall network resilience.[73]
- The various hardware, software applications and protocol and code layers of the conceptual framework, known as "Open Systems Interconnection model", include an inordinate amount of proprietary information (hardware protocols and codes) that it makes it impossible to reverse engineer every component and to verify all network messages over the hardware back to the end consumers such as Huawei (or China's secret services).[74]
- The cybersecurity risks and vulnerabilities of the future 5G network will be far greater than that of existing 3G/4G networks because its "core" (where customer information is stored and processed) can no longer be clearly separated from the periphery (Huawei's antennas and base stations). In the words of the editorial board of the *Financial Times*, "The core no longer sits in a central box but is virtual, composed of software spread across the network."[75] More computing power, clouds,

[70] See also Zachary Filingham, "We're asking the wrong questions about Huawei", *Geopolitical Monitor*, 24 April 2020.
[71] Dan Sabbagh, "MI5 Chief asks tech firms for "exceptional access" to encrypted messages", *The Guardian*, 25 February 2020.
[72] See also F. Umbach, "Europe and Huawei: Rising Cybersecurity Challenges".
[73] See also Kevin Townsend, "Huawei and Supply Chain Security — The Great Geopolitical Debate", www.securityweek.com, 27 January 2020; and Siddhart Venkataramakrishnan, "Cyber security 2050: hackers to tap smart cities and deep fakes", *FT*, 21 January 20.
[74] See also Ahana Datta, "UK Huawei decision highlights dilemmas of the surveillance age, *FT*, 29 January 2020, and Yuan Yang "What are the main security risks of using Huawei for 5G?", *FT*, 25 April 2019.
[75] Editorial Board, "Barring Huawei from Britain's 5G is too costly to justify", *FT*, 20 January 2020.

servers and processes will move from the core to the periphery as the numerous appliances of Industry 4.0 demand much more sliced and decentralised 5G networks.[76]

Figure 7: The Expanding Core Network in the 5G Era



Source: Frank. Umbach, "Europe and Huawei: Rising Cybersecurity Challenges", GIS, 2 April 2020.

- Future mobile networks will run on advanced software in increasingly virtualised networks. The traditional distinction between hardware and software will become increasingly blurred in those virtual networks. Their designs rely more than ever on software in dynamically configured hardware. If a hacker gains control of the software managing the network, he can also control the entire network.[77]
- As 5G network technologies will be entangled with the older 3/G4G network technology, safety and security cannot be enhanced sufficiently owing to existing 4G protocol vulnerabilities, which will be inherited with the 5G network deployments.[78]
- With hitherto rather lax security legislation, many Western network operators could choose between optional security features. Even mandatory security features, defined by international and national standards security committees, have often not been implemented owing to perceived costs. Even 5G standards committees have missed many opportunities to address systemic

[76] See also "Australia, Huawei and 5G", IISS Strategic Comments, p. 2; Nic Fildes, "Can the 5G network be secured against spying?", *FT*, 19 January 2020; "Reports Huawei to supply UK networks draw criticism", AFP, 25 April 2019; Daniel Voelsen, "5G, Huawei und die Sicherheit unserer Kommunikationsnetze".

[77] "5G and IoT security: Why cybersecurity experts are sounding an alarm", www.techrepublic.com, 2 March 2020; Bruce Schneier, "China isn't the only problem with 5G", *Foreign Policy*, 10 January 2020; Daniel Voelsen, "5G, Huawei und die Sicherheit unserer Kommunikationsnetze;and Nic Fildes, "Can the 5G Network be secured against spying?".

[78] See also Bruce Schneier, "China isn't the only problem with 5G".

cybersecurity challenges as security and government surveillance had never been prioritised over corporate profits. For some experts, it is already too late to secure 5G networks sufficiently.[79]

- Cybersecurity experts have demanded the disclosure of source and programme codes for 5G networks. But this call contradicts traditional business practice. Even if such demands are complied with, network operators (like Huawei) can change their programme codes subsequently via remote control and under the guise of maintenance.
- An even more challenging feature, a so-called "bugdoor", is control over automated software updates, which leaves almost no option for assessing those updates in time to uncover any security flaws.[80]
- The dynamic deployment of 5G networks will dramatically change the cybersecurity landscape by increasing the scale of surface attacks and restricting effective surveillance and control. Traditional monitoring methods will become increasingly ineffective and obsolete. The 5G network may become so complex that managing the risks associated with an "untrustworthy" vendor could overwhelm all the national resources of smaller countries[81] that have no institutional capacity or an established cyber risk security culture to analyse potential vulnerabilities as well as to survey and control unprecedented dynamic and complex 5G network operations.

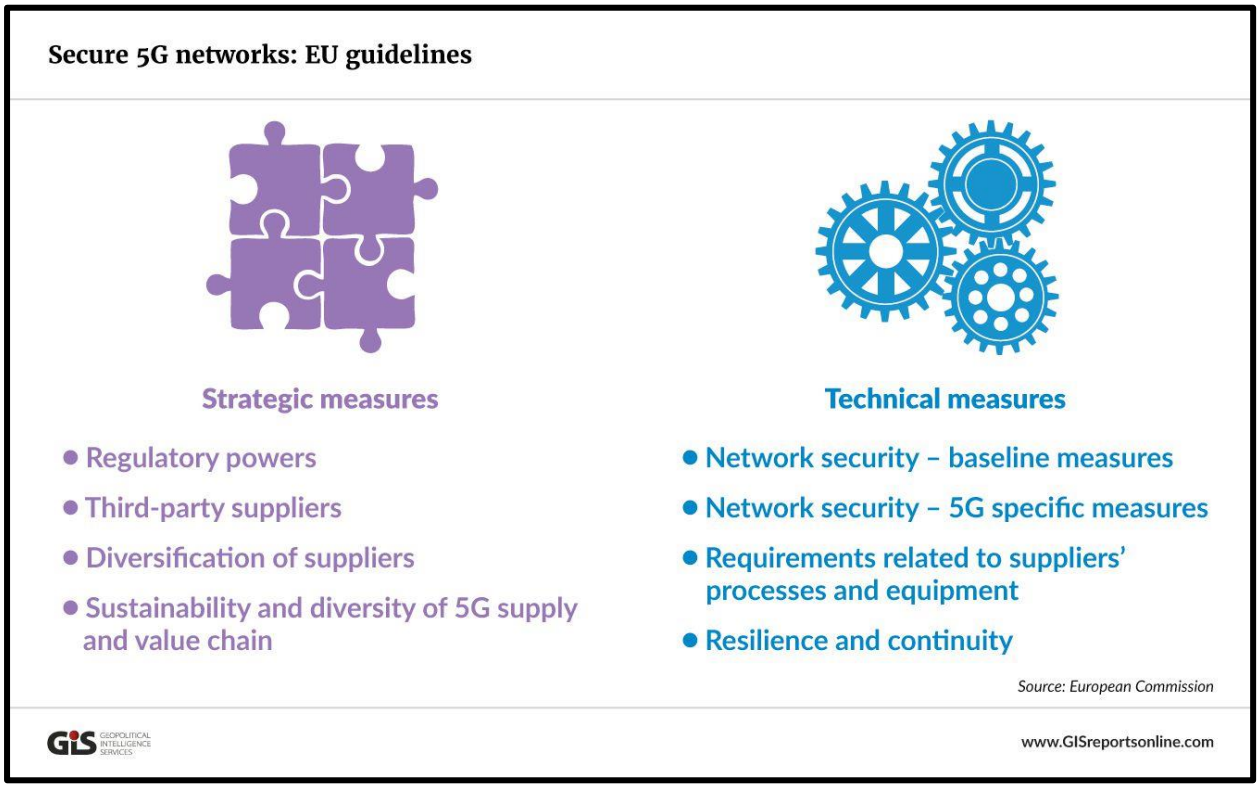
ENISA's Recommendations and Guidelines for 5G Rollout

All EU member states are now working collectively in the EU's security "Network and Information Systems (NIS-Directive)". At the beginning of 2019, each member state completed its own national risk assessment of the 5G network infrastructure and transmitted it to ENISA. In March 2019, the EC published cybersecurity recommendations for 5G networks.[82] In June 2019, the EU's "Cybersecurity Act" entered into force.[83] It creates a framework for European cybersecurity certification schemes for products, processes and services, which are to be supervised and certified by ENISA and EC. Once in place, these certification schemes will also enable producers to demonstrate that they have included specific security features in the early stages of their products' design. They guarantee users a certain level of security assurance on an EU-wide basis and are an essential supporting tool to promote consistent levels of cybersecurity, including for 5G equipment and software. While these certification schemes can only serve as recommendations and do not have legal force, EU members states are effectively forced to introduce them as they would not otherwise be able to cooperate with one other as well as with the EC and ENISA.

[79] Bruce Schneier, "China isn't the only problem with 5G".
[80] See also Kara Frederick, "The 5G Future is not just about Huawei", *Foreign Policy*, 3 May 2019.
[80] See also Yuan Yang, "What are the main security risks of using Huawei for 5G?", *FT*, 25 April 2019.
[81] See also Editorial Board, "Barring Huawei from Britain's 5G is too costly to justify", FT, 20 January.
[82] See European Commission, "Commission recommendation: Cybersecurity of 5G Networks", 2335 final 26 March 2019.
[83] "Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act)", https://eur-lex.europa.eu/eli/reg/2019/881/oj.

In January 2020, the NIS-Cooperation Group published a toolbox of risk mitigating measures. It describes a set of strategic and technical measures as well as supporting action to reinforce their effectiveness.[84] In order to avoid heavy dependence on a single supplier, the report recommends a multi-vendor strategy through the development of a diverse and sustainable 5G supply chain. In the area of key assets defined as critical and sensitive in the EU coordinated risk assessment, the report recommends applying relevant restrictions (including exclusions) for suppliers considered to be high risk. Other recommendations to make Europe's 5G networks more secure in future include standardisation, certification, screening of foreign direct investment (FDI), enhanced competition rules, incident response and crisis management as well as cyber exercises and joint EU diplomatic responses to cyberattacks.

Figure 8: The European Union's Key Strategic and Technical Measures



Source: F. Umbach, "Europe and Huawei: Rising Cybersecurity Challenges", GIS, 2 April 2020.

In July 2020, the EC and ENISA published a new review reporting on the progress made in implementing the joint toolbox of mitigating security measures. The review noted the progress each country has made in implementing all defined and recommended strategic and technical measures. It also highlighted that the progress made varied significantly between EU member states and between individual recommended measures, looking like a patchwork. It charged that many EU member states

[84] NIS Cooperation Group, "Cybersecurity of 5G networks — EU Toolbox of Risk Mitigation Measures", 29 January 2020.

had “not yet established or communicated clear plans to effectively address existing situations of dependency on high-risk suppliers, and [to] prevent future dependencies”.[85]

The area where most progress had been made, according to the review, was in enhancing the powers of regulatory authorities for 5G security, restricting the involvement of suppliers based on their risk profiles, and developing network security and resilience requirements for mobile operators. The report warned that more progress needs to be made in areas such as decreasing the risks of dependence on high-risk suppliers, designing and imposing appropriate multi-vendor strategies for individual mobile network operators and screening of FDIs. Further recommendations have been made for exchanging more information on the challenges, best practices, and solutions as well as monitoring and evaluating the implementation of the EU’s toolbox.

More recently, the European Union also addressed and highlighted the cybersecurity risks of 5G in its much more comprehensive and holistic July 2020 “EU Security Union Strategy”.[86] It warned that the protection and resilience of CI have not kept pace with the rising cybersecurity risks. Given the rollout of 5G infrastructure and increasing interdependencies of many critical services and CI on 5G networks, the consequences of systemic and widespread disruption could be much more severe than in the past. In addition to its 2019 recommendations on the cybersecurity of 5G networks and the key measures contained in the 5G toolbox, the Commission has proposed the creation of a “Joint Cyber Unit” for enhanced structured and coordinated operational collaboration, including a mutual assistance mechanism in times of crisis at EU level and the offer of key services to member states.[87] It is expected that these recommendations too will be implemented step by step by EU member states, just as they have implemented the recommendations calling for the screening of FDI, which was prompted by concerns about China’s investments and take-overs of high-tech companies.[88]

[85] NIS Cooperation Group, “Report on member states’ progress in implementing the EU Toolbox on 5G Cybersecurity”, July 2020; and Samuel Stolton, “Commission presses member states to take action on high-risk 5G vendors”, *EURACTIV*, 24 July 2020.
[86] European Commission, “EU Security Union Strategy”.
[87] European Commission, “EU Security Union Strategy”, p. 6 ff.
[88] The EU’s screening framework has been in place as of October 2020, one and a half years since the EU member states approved it.

Key EU Member States: Balancing Economic–Industrial Interests vs Security Interests

United Kingdom

The British government decided on 28 January 2020 that Huawei will be excluded from the core 5G network and restricted to its periphery. The government also imposed a cap on future market share for Huawei in the United Kingdom's non-core 5G network, reducing it from the current 44 per cent to 35 per cent by 2023. If such a cap had not been imposed, Huawei would have acquired a future market share up to 70 per cent within the next three years.[89]

The British National Cyber Security Centre (NCSC), a division of the British signals intelligence agency known as Government Communications Headquarters (GCHQ), admitted in January 2020 that the risks of using Huawei's technologies in its 5G network can never be completely removed, but are "manageable" and can be decreased to "acceptable levels".[90] But it has evaluated Huawei as Britain's only high-risk vendor in the national 5G rollout. The assessment is not only based on China's National Intelligence Law of 2017, which allows the Chinese government to "compel anyone in China to do anything". The NCSC has also warned that China's state and associated actors "have carried out and will continue to carry out cyberattacks against the UK and our interests". It has also repeatedly charged that "Huawei's cybersecurity and engineering quality is low and its processes opaque"[91] despite Huawei's own claims to offer "total transparency" through its "Huawei Cyber Security Evaluation Centre" (HCSEC), a unique partnership with the NCSC, which involves officials from the GCHQ.[92]

In its 2019 report, the NCSC confirmed that Huawei had made "no material progress" in addressing "major defects" and significant security concerns already raised the previous year. It added that it could provide only limited assurance against the cyber risks posed by Huawei to UK national security and sufficient risk mitigation in the long-term perspective.[93] Also in its annual 2020 report of September 2020, HCSEC highlighted "nationally significant" "systemic [security] defects" such as "poor software engineering and cybersecurity processes" with "the increasing number and severity of vulnerabilities discovered", although it added that the identified vulnerabilities had neither been exploited nor were the defects the "result of Chinese state interference". Nevertheless, it said an attacker with knowledge of

[89] Nic Fildes, "Huawei executives greet UK 5G approval with relief", *FT*, 29 January 2020.
[90] See also Demetri Sevastopuli and David Bond, "UK says Huawei Is manageable risk to 5G", *FT*, 17 February 2019; George Parker, Helen Warrell and Kiran Stacey, "Huawei decision jolts UK–US 'special relationship' at sensitive time", *FT*, 28 January 2020.
[91] Shona Ghosh, "The UK's top cyber officials have warned that Huawei has poor cybersecurity", Source?, Date?; Stuart Lau, "British cybersecurity officials publicise distrust of Huawei as Boris Johnson gives 5G green light", *SCMP*, 29 January 2019..
[92] Victor Zhang (vice president, Huawei, London), "Letter: Huawei offers total transparency over its kit", *FT*, 22 July 2020.
[93] Kevin Townsend, "Huawei and Supply Chain Security — The Great Geopolitical Debate", www.securityweek.com, 27 January 2020; and "Britain 'approves' Huawei role in 5G network", AFP, 24 April 2019.

the many vulnerabilities would be able to sabotage UK networks. The agency warned that it had "no confidence that Huawei will effectively maintain components within its products."[94]

Adding to these concerns, the new head of M15, the British domestic security service, recently stated that China was the biggest long-term state-based threat to Britain even as he identified Russia as the biggest threat currently. While Russia, in his words, was delivering "bursts of bad weather", Beijing was "changing the climate".[95]

The British telecommunication industry warned that a ban on Huawei could cause a two-year delay in the full rollout of networks and a significant service disruption.[96] In May 2020, Huawei unveiled plans to invest £1bn in a new chip research centre and manufacturing facility in Cambridgeshire and create 400 jobs over the next five years. But the US government warned its British counterpart against the building of the facility, citing the security risks of such collaboration and joint research, notably, theft of technology and intellectual property.[97]

Despite the government decision, 38 members of the ruling Conservative Party voted against the compromise and formed an internal opposition group against Huawei's involvement (the so-called "China Research Group").[98] In June 2020, the British media revealed that the UK government planned to reduce Huawei's involvement to zero in the 5G rollout by 2023 owing to the prime minister's efforts to boost trade negotiations with the United States. In response, Huawei started a public relations campaign warning the British not to "overestimate the risk of security and forget the economic impact". It insisted that it would be a private company "100 per cent owned by its employees" and claimed to have "the best possible technology" for UK networks.[99]

China's enactment of a new security law for Hong Kong on June 30 2020 has further hardened the British government's position towards China as the law has given Britain's domestic critics even more political ammunition.[100] A controversial dossier, compiled with the support of former British intelligence officer Christopher Steele, concluded that high-profile Britons had been targeted to act as lobbyists and "useful idiots" for Beijing.[101]

[94] HSCEC Oversight Board, "Annual Report 2020: A report to the National Security Adviser of the United Kingdom", London, September 2020.
[95] Cited in Helen Warrell, "UK will do more to counter Chinese spying threat, says MI5 chief", *FT*, 14 October 2020.
[96] Nic Fildes 'Vodafone warns ripping out Huawei would cost UK lead in 5G", *FT*, 9 June 2020
[97] Nic Fildes, George Parker and Katrina Manson, "US warns over Huawei plan to spend £1bn on chip facility", *FT*, 25 June 2020.
[98] also Sebastian Payne and Hellen Warrell, "Huawei 5G vote prompts 'warning shot' from UK government rebels", *FT*, 10 March 2020.
[99] George Parker and Nic Fildes, "Huawei fights back against the attacks over Britain's 5G", *FT*, 7 June 2020.
[100] Sebastian Payne and George Parker, "Boris Johnson set to curb Huawei role in UK's 5G networks", *FT*, 12 July 2020; and George Parker et al., "UK faces calls to target China with new sanctions", *FT*, 7 July 2020.
[101] "Boris Johnson urged not to break ties with China amid pressure over Huawei role", *The National Scot,* 7 July 2020.

Following the May 2020 US sanctions, the NCSC conducted an emergency review of Huawei's potential as a supplier to UK networks amid new uncertainties about Huawei's ability to find an alternative chip supplier. The NCSC concluded that Huawei would be forced into a "major reconfiguration" of its supply chain and it questioned the future supply security and reliability of Huawei's equipment. Huawei in response declared that it would take months before it could fully reassure its customers (such as the BT Group and Vodafone) over the impact of the US sanctions.[102] But this response merely confirmed the British government's and industry's fears.

Finally, on 14 July 2020, the UK government rescinded its January compromise and banned Huawei completely from its 5G installation and demanded that network operators remove existing Huawei gear completely by the end of 2027 although this will be extremely expensive and time consuming for them.[103] Whether Huawei's equipment should be removed from the older 3G/4G networks still seems to be a matter of contention between Prime Minister Boris Johnson and some of his fellow Conservative parliamentary colleagues.[104]

The Johnson government has adopted the 2027 deadline as a compromise with BT as the latter has warned that an earlier ban would be even more costly and disruptive.[105] The government has largely defended its decision on "technical grounds" as Huawei can no longer buy key US chips for its 5G instalment.[106] However, the UK Parliament defence committee stated in October 2020 that it had found evidence of Huawei's collusion with the Chinese Communist Party apparatus and urged the removal of all Huawei equipment sooner than the 2027 deadline.[107]

The government's shifting position on Huawei is in line with recent British public opinion polls showing distrust of China being as high as 83 per cent. For many China observers among the British, the supposedly "golden era" in relations with China had proved to be a "golden error" and a complete misunderstanding, based on wishful thinking, of China's policy direction in the era of President Xi Jinping.[108]

The UK government has agreed with the United States to work with the "Five Eyes" partner countries — the United States, Canada, Australia and New Zealand — to develop alternatives to Huawei. It has also proposed a "D10" club of democratic partners that groups the G7 countries (Canada, France, Germany, Italy, Japan, the United Kingdom and the United States) with Australia, South Korea and

[102] Nic Fildes and Helen Warrell, "Huawei calls for UK to grant stay of execution", *FT*, 8 July 2020.
[103] George Parker et al., "UK orders ban of new Huawei equipment from end of year", *FT*, 15 July 2020; and Editorial Board, "Britain takes long view with Huawei 5G ban", *FT*, 14 July 2020.
[104] George Parker et al., "Boris Johnson tries to find path through US-China cold war", *FT*, 14 July 2020; and George Parker et al., "UK orders ban of new Huawei equipment from end of year".
[105] See also Chris Nuttall, "The Seven-Year Switch from Huawei", *FT*, 15 July 2020.
[106] See also Nic Fildes and Helen Warrell, "Why the UK has decided to ban use of Huawei's 5G kit", *FT*, 14 July 2020; John Sawers (former chief of M16), "The UK should ban Huawei from its 5G Network, *FT*, 5 July, 2020.
[107] "UK parliament committee says Huawei colludes with the Chinese state", Reuters, 8 October 2020.
[108] Jonathan Ford and Laura Hughes, "UK–China relations: From 'golden era' to the deep freeze", *FT*, 14 July 2020.

India to channel investments into their telecommunication companies and collaborate on 5G as well as other disruptive technologies and their global supply chains.[109]

France

France's 5G policies and the Huawei question have been influenced by the overall state of France–China bilateral relations, but also wider concerns about the "digital sovereignty" of the EU.[110] With France increasingly perceiving China as a major problem and not a solution for the future international order, French President Emmanuel Macron proclaimed in March 2019 that the "period of European naiveté is over".[111]

Like Germany, France wanted to avoid officially discriminating against any vendor and China. Its 5G installation process has been strongly controlled by the government. Following the government's introduction of new cybersecurity rules for network equipment suppliers in 2018, all suppliers were required to get the approval of the French cybersecurity agency. In February 2019, new reinforcing measures for mobile networks were announced by the government.[112] But the French president lamented in December 2019 that Europe had simply failed to have any degree of thinking or coordination on the issue, effectively delegating sovereign choices and decisions to telecommunication operators.[113]

The French government has held close cybersecurity consultations with the United States.[114] At the end of January 2020, the biggest French telecommunication company, Orange, had already chosen Nokia and Ericsson instead of Huawei for the deployment of its 5G network in France.[115] As it did in other European countries when government decisions loomed on Huawei's inclusion in their 5G rollout, the Chinese company declared in February 2020 that it would build a European manufacturing plant in France, investing €200million.[116]

France's 5G policy has most recently also been influenced by China's pandemic policies and Europe's dependence on China for the supply of medical equipment. During the past several months, bilateral

[109] Helen Warrell, Alan Beattie and Demetri Sevastopulo, "UK turns to 'Five Eyes' to help find alternatives to Huawei", *FT*, 13 July 2020; Erik Brattber and /Ben Judah, "Forget the G-7, build the D-10", *Foreign Policy*, 10 June 2020; and Laura Zhou, "Does the US-led Five Eyes have wider sights on China?", *SCMP*, 8 August 2020.

[110] "As Europe readies to recalibrate its relationship with China, should it look to Paris instead of Berlin?", AICGS, 30 July 2020.

[111] Michael Peel, Victor Mallet and Miles Johnson, "Macron hails 'end of Europe naïveté' towards China", *FT*, 22 March 2019.

[112] "France to tighten 5G security: Minister", AFP, 7 February 2020; and Laurens Cerulus and Klaus Geiger, "Deutschlands Kotau bei Huawei", *Die Welt, 27 May 2020*, p. 6.

[113] Ben Hall, "EU needs common telecoms rules to thwart Huawei's 5G threat", *FT*, 18 December 2020.

[114] "US presses France for 'strong security measures' against Huawei", AFP, 23 January 2020.

[115] Mathieu Rosemain and Sudip Kar-Gupta, "France's Orange chooses Nokia and Ericsson to deploy its 5G network at home", Reuters, 31 January 2020.

[116] "Huawei to build first European 5G factory in France to soothe Western nerves, says chairman", *The Straits Times*, 27 February 2020; and Laurens Cerulus, "Huaweis unmoralisches Angebot", *Die Welt*, 10 March 2020, p. 12.

relations further deteriorated following China's introduction of the Hong Kong national security law, China's disinformation campaigns and its treatment of the Uighur Muslim minority.[117] Huawei even filed three unprecedented defamation lawsuits against a well-respected French researcher on Asia, Valerie Niquet, after her comment in November 2020 that "no one would have given a Soviet company the means to monitor all the communication in the Western world and this is what we're doing with Huawei."[118]

At the beginning of July 2020, the French cybersecurity agency told its operators to avoid switching to Huawei. The French government has restricted Huawei's 5G technology from major CI to protect military bases, nuclear installations and other sensitive sites. Those already using Huawei equipment would be granted a three to eight year licence to operate 5G technology.[119] At the end of the month, the French government effectively banned Huawei from participating in its national 5G rollout by 2028.[120]

Germany

The German government has been extremely concerned about the escalation in US–China relations. It has criticised both the United States and China for the escalation as it undermines global trade as well as global security and stability. Berlin fears that the US–China "technology cold war" and its impact on the global supply chains for semiconductors could also increasingly affect German companies. Germany's bilateral trade with China had risen to €199bn by 2019, constituting a 6 per cent increase since 2017. Furthermore, German investments in China rose from €30bn in 2010 to €81bn in 2017.[121]

The German government and industry have been interested in an early 5G rollout, which would give them a competitive advantage over their economic rivals. When US President Trump demanded a ban on Huawei, the German government declared that it would not exclude any Chinese company. But in January 2019, Germany's foreign intelligence service, known by its abbreviated form, BND, had already warned the government against including Huawei in the 5G rollout. In fact, it had already sounded out warnings on Huawei and China's cyber industrial espionage as far back as 2008 at least.[122] At the end of 2019, the US government shared with the German and UK foreign ministries "smoking gun" evidence proving Huawei's collaboration with Chinese security agencies. This evidence allowed the conclusion that Chinese companies lack trustworthiness and that Huawei can access by the back door networks

[117] Sudip Kar-Gupta and Leigh Thomas, "Huawei will not be prevented from investing in France: Le Maire", Reuters, 21 July 2020; and Togo Shiraishi, "France places de facto ban on Huawei gear by 2028", *Asia Nikkei*, 24 July 2028.
[118] American Foreign Policy Council, "Huawei sues French researcher for highlighting its government ties", China Reform Monitor No. 1396, 11 December 2019.
[119] "China urges 'fair' treatment after France restricts Huawei", AFP, 7 July 2020; and "Huawei not totally banned from France, says watchdog: Report", AFP, 6 July 2020.
[120] Togo Shiraishi, "France places de facto 5G ban on Huawei gear by 2028"; Yixiang Xu, "As Europe readies to recalibrate its relationship with China, should It look to Paris instead of Berlin?", AICGS, 30 July 2020.
[121] Guz Chazan, "Merkel faces party revolt over Huawei's role in German 5G rollout", *FT*, 20 November 2019.
[122] Joachim Müller-Soares, "Trojaner aus Peking", *Capital* 12/2008, pp. 48-52.

that it helped to build. Subsequently, the German foreign ministry declared that the trustworthiness of Chinese companies for secure 5G networks cannot be guaranteed.[123]

Meanwhile, China Mobile, the world's largest mobile phone company in regard to customers and the biggest one in China, has turned entirely to Huawei and ZTE to build and expand 5G mobile networks in China, restricting market access to foreign players. Although the European Union and Germany have argued for adopting the guiding principle of reciprocity in their relationship with China, they still have to live up to this declared principle as a matter of political credibility by denying market access to Huawei.[124]

The previous UK government's compromise approach of differentiating between the core and periphery network offers a model for the German government. However, for now, the German government, owing to its wider economic interests, has yet to adopt a complete official exclusion of Huawei. Minister for Economic Affairs Peter Altmaier declared as recently as in July 2020 that "it would be wrong to exclude a company on political grounds, even though there is no evidence that the legal system, privacy or data protection of an EU country is threatened."[125] In 2019, the Chinese ambassador in Berlin threatened retaliation against German companies if the German government were to exclude Huawei from its 5G rollout.[126] The German government fears the impact of such retaliation on its automobile industry and other important sectors.[127]

Critics, focusing almost exclusively on the technical risks of the future 5G networks, said the German government's policy was tantamount to a kowtow to China, a policy they derisively labelled as "automobile foreign policy". They felt the Berlin government did not respond initially to the rising cybersecurity challenges, growing high dependency on Huawei, the wider industrial challenges and the country's failing compliance with the European Union's and ENISA's 5G cybersecurity policies.[128]

Since 2019, the debates within the German government have become more heated, as the discussion surrounding a new information technology (IT) security law has highlighted.[129] In November 2019, critics within Chancellor Angela Merkel's own CDU/CSU alliance insisted that the German Bundestag should

[123] Michael Peel, Javier Espinoza and Nic Fildes, "EU draws up 5G plan to screen security risks amid Huawei fears", *FT*, 29 January 2020; Rana Foroohar, "One World, Two Systems in the 5G Race", *FT*, 17 February 2020; "China: US officials accuse Huawei of retaining clandestine network access", Stratfor.com, 12 February 2020; Florian Flade and Georg Mascolo, "US–Geheimdienste warnen Bundesregierung vor Huawei", *Sueddeutsche Zeitung*, 29 January 2020; Moritz Koch, "'Smoking Gun': Streit um Beweise gegen Huawei", *Handelsblatt,* 29 January 2020.

[124] See also Thomas Sigmund and Moritz Koch, "Industrie rückt von Huawei ab", *Handelsblatt*, 26 January 2020.

[125] Cited in Philipp Grüll, "Germany's Altmaier encourages MEPs to be more realistic", EURACTIV, 16 July 2020.

[126] "America's war on Huawei nears its endgame", *The Economist*, 16 July 2020.

[127] Laurens Cerulus "How US restrictions drove Deutsche Telekom and Huawei closer together", *Politico,* 6 July 2020.

[128] Jan-Peter Kleinhans, "Eindimensionale Huawei-Politik der Bundesregierung", *FAZ*, 19 October 2019; Simon Schuetz, "Uprising against German Chancellor in the Case of Huawei", AICGS, 21 November 2019; Janka Oertel, "Germany chooses China over the West", *Foreign Policy*, 21 October 2019; Yixiang Xu, "5G Decision Time in Germany", AICGS, 23 January 2020; and Laurens Cerulus and Klaus Geiger, "Deutschlands Kotau bei Huawei", *Die Welt*, 27 May 2020.

[129] See also Justus Bender, "Misstrauen ist gut", *FAS*, No. 50, 15 December 2019, p. 4.

have the final say on Huawei and the issue of 5G.[130] This insistence forced the chancellery to compromise with its critics and the parliamentary opposition against Huawei's inclusion in Germany's 5G rollout.

The government's coalition partner, the Social Democratic Party (SPD), had already taken a much more hostile position against Huawei. It took the unanimous stand in December 2019 not to involve any foreign supplier and telecommunication company of an "authoritarian government" that is not a democracy, does not respect the rule of law and human rights, and therefore is not "trustworthy". Interestingly, even the Federation of the German Industry (BDI) is against Huawei's participation if sufficient security guaranties cannot be provided.[131] But Germany's second largest mobile phone company, Telefonica Deutschland, declared in December 2019 that it would include Huawei in its German 5G rollout, although it has not selected a supplier for its sensitive 5G core network owing to the controversy the matter has raised in Germany.[132]

In February 2020, the CDU/CSU developed a political compromise in response to its internal critics on the Huawei issue (mostly foreign policy experts such as Norbert Röttgen).[133] According to this compromise, no foreign telecommunication company will be officially excluded from the German 5G rollout. But the use of specific components from a supplier can be excluded if they are deemed to be against public interest, for instance, if they fail to comply with Germany's cybersecurity requirements. Any 5G equipment would need to meet clearly defined security criteria. The CDU/CSU position called on Germany to avoid a "monoculture" to prevent any foreign country having harmful influence on the network. The compromise paper conceded that even with a comprehensive technical review and checks, potential security risks related to technical components and equipment "cannot be completely eliminated — they can at best be minimised".[134]

Minister Altmaier has since vowed that the 5G rollout would fulfil the "highest security standards", standards "which no other country will surpass".[135] But he did not want to exclude in advance any

[130] Guz Chazan, "Merkel faces party revolt over Huawei's role in German 5G rollout"; and Matthew Karnitschnig, "Germany's CDU seeks to block Huawei from 5G rollout", *Politico*, 23 November 2019.

[131] Philipp Grüll, "Huawei shouldn't be getting its hopes up for German 5G expansion just yet", EURACTIV*,* 12 February 2020; Ansgar Graw, "Beteiligung von Huawei ist nicht zu akzeptieren", *Die Welt,* 26 November 2019; Matin Hakverdi, "Huawei ist der verlängerte Arm Pekings", *Die Welt*, 29 October 2019, p. 2.

[132] Nic Fildes, "Telefonica chooses Huawei to help German 5G network", *FT*, 11 December 2019; Wesley Rahn, "Mobile provider Q2 chooses Huawei to build its German 5G network", Deutsche Welle (DW*)*, 11 December 2019, "Huawei wins deal to help build Telefonica's 5G network in Germany", *SCMP*, 12 December 2019, and Thomas Heuzeroth, "Telefonica baut sein 5G-Netz auf", *Die Welt*, 12 December 2019, p. 10.

[133] Norbert Röttgen is the chairman of the Parliament's foreign affairs committee and one of the four CDU/CSU candidates for Mrs Merkel successor as chancellor. See "Röttgen gegen Huawei-Beteiligung bei deutschem 5G-Ausbau", *Handelsblatt*, 17 May 2020.

[134] CDUS/CSU Fraktion im Deutschen Bundestag, "Deutschlands digitale Souveränität sichern – Maßstäbe für sichere 5G-Netze setzen. Positionspapier", Berlin, Beschluss vom, 10 February 2020. See also Guy Chazan, "Germany's CDU stops short of Huawei ban in 5G Rollout", *FT*, 11 February 2020; and Andreas Rinke, "Merkel's conservatives stop short of Huawei 5G ban in Germany", *Reuters,* 11 February 2020.

[135] the interview with Economic Affairs Minister Peter Altmaier (CDU) in Jacques Schuster and Pilipp Vetter, "Politik wird im Parlament gemacht und nicht auf der Straße", *Welt am Sonntag*, No. 6, 9 February 2020, p. 34.

specific producer of network components such as Huawei.[136] This policy consensus follows the recommendations of ENISA and the EC, which avoided mentioning Huawei by name. But the new position has enhanced the restrictions so much that it may lead to a de facto ban of Huawei from at least the "core" of the 5G network.

Nevertheless, the question of "controllability" has still not been resolved.[137] As a technical review cannot completely guarantee cybersecurity, an additional political review for telecommunication companies of non-democratic countries is considered needed by the majority of the German Bundestag, including Ms Merkel's own CDU/CSU. According to the draft version of the IT security law 2.0, the German ministries for the interior and economic affairs would be responsible for determining the "trustworthiness" of a foreign supplier. However, because these ministries are filled by the CDU/CSU, the proposal was unacceptable to the foreign ministry, which is held by the SPD and to the SPD faction in the Bundestag.[138] One compromise being discussed is that the Federal Security Council[139] could make the final decision. Based on my interviews in September and October 2020 and press reporting, Germany, like France, will effectively exclude Huawei through its IT security law although stopping short of an official outright ban.[140]

Other EU Countries

In Italy, Huawei has been able to steadily expand its business ties and market share through various projects with university research centres, such as "smart cities". Italy has become Huawei's second largest market for smartphones in Europe after Germany. In July 2019, Huawei announced that it would invest more than US$3.1 billion over the next three years in Italy. But the new Italian government is much more pro-European Union than the previous one. The Parliamentary Committee for the Security of Italy conducted a study in December 2019, in which it recommended excluding state-owned companies, including Huawei, in Italy's 5G plans.[141] Italy had already passed a new "cyber security law" in November 2019, giving its government more powers in picking 5G suppliers between domestic companies and non-EU suppliers such as Huawei. But it did not ban the Chinese vendor. Nevertheless,

[136] Philipp Grüll, "Huawei shouldn't be getting its hopes up for German 5G expansion just yet".
[137] Moritz Koch, "Bundesregierung: Ausschluss von 5G Komponenten bestimmter Hersteller ist möglich", *Handelsblatt*, 4 May 2020.
[138] Moritz Koch, "Seehofer stärkt Cyberabwehr", *Handelsblatt,* 13 May 2020; Philipp Grüll, "Huawei shouldn't be getting its hopes up for German 5G expansion just yet"; and Philipp Grüll, "In Germany's new 5G security criteria, SPD sees a 'blunt sword'", EURACTIV, 14 May 2020.
[139] The German Federal Security Council is still an ad-hoc body rather than the kind of permanent, institutionalised decision-making body that other countries have. It brings together the main ministries, involving the expertise of Germany's secret services when needed in crisis situations or on high-security issues.
[140] See also Guy Chazan and Nic Fildes, "Germany crackdown set to exclude Huawei from 5G rollout", *FT*, 30 September 2020; and Manuel Bewarder and Christina Brause, "Kein Anschluss für Huawei?", *Welt am Sonntag*, 20 September 2020.
[141] Giovanna de Maio, "Playing with Fire: Italy, China, and Europe", Brookings Institution, Washington, DC, May 2020, p. 9f.

in August 2019, Telekom Italia (TIM) had already decided to exclude Huawei from its new 5G services for core network infrastructure, defending its decision as a commercial one.[142]

Belgium, being the headquarters of NATO and the European Union, will exclude any non-trustworthy supplier, at least from its 5G core network. The Netherlands as well as Estonia, Ireland, Norway and Portugal may do the same. But Iceland, Finland, Luxembourg, Austria, Switzerland, Turkey and Slovenia have not discussed any ban or restrictions on Huawei for their core networks.[143] In June 2020, Spain became the first EU member state to grant Huawei security clearance for a 5G product.[144]

In its approach to the Huawei issue, the most pressure Beijing has used in Europe was directed against one of its weakest members. In December 2019, an audio recording revealed that the Chinese ambassador to Denmark had threatened give up a free trade agreement with the Faroe Islands, part of Danish territory, if Huawei was not awarded a 5G contract on the island. The local government, a long-time Huawei customer, sought to keep the recording secret as it also revealed that the government had reassured Huawei that it would not interfere in the selection process for the 5G contract. This marked the first time that China had explicitly linked access to the vast Chinese market with Huawei's contracts.[145] In response, the Danish government announced a new law that would define its entire 5G network as CI, which effectively excludes Huawei.[146]

Sweden has recently banned the use of Huawei and ZTE telecommunication equipment from its 5G network following recommendations by the Swedish armed forces and its security service.[147] The latter also accused China of aiding its economic development and military capabilities through "extensive intelligence gathering and theft of technology, research and development". Sweden's bilateral relations with China have deteriorated over the detention and sentencing of the Swedish citizen and Hong Kong–based publisher of gossipy books about Chinese leaders, Gui Minhai, on charges of endangering China's national security.[148]

Among the East European countries, the Polish government has fostered the closest ties in Europe to the Trump administration, given its security concerns regarding Russia and its ambivalent views towards the European Union. Hence, Poland has blocked Huawei and other Chinese

[142] James MacKenzie and Elvira Pollina, "Huawei says it's working with Telecom Italia despite 5G exclusion: paper", Reuters, 20 July 2020.
[143] "America's war on Huawei nears its endgame", *The Economist*, 16 July 2020, and Moritz Koch and Stephan Scheuer, "'Armageddon' Scenario: Telekom spielt Huawei-Bann durch", *Handelsblatt*, 16 June 2020.
[144] "First security certification granted to Huawei in Spain", www.business-review.eu, 23 June 2020.
[145] Simon Kruse and Lene Winther, "Banned recording reveals China ambassador threatened Faroese Leader at secret meeting", *Berlingske*, 10 December 2019; and Charlie Duxbury, "How Huawei conquered the Faroe Islands", *Politico*, 7 October 2019.
[146] Laurens Cerulus and Klaus Geiger, "Deutschlands Kotau bei Huawei".
[147] Richard Milne, "Swedish bans Huawei and ZTE from 5G telecom networks", *FT*, 20 October 2020; Nic Fildes, "Ericsson shines against backdrop of Sino-Swedish tension", *FT*, 21 October 2020; and Dipanjan Roy Chaudhury, "Backed by bloc, Italy, Sweden pushback against China gaining a foothold in Europe", *The Economic Times*, 22 October 2020.
[148] Cited in Richard Milne, "Sweden bans Huawei and ZTE from 5G telecoms networks".

telecommunication companies from its 5G rollout. In January 2020, a Huawei employee was arrested in Poland on suspicion of spying.

The Czech Republic, for its part, shut out Huawei from public tenders following a warning from its cybersecurity agency. But Czech President Milos Zeman, known for his non-critical stance towards China and Russia, has warned the government against hurting Huawei's economic interests.[149]

Another close ally of the United States, Romania has just recently defined criteria for choosing partners to implement the 5G rollout, which would effectively exclude Huawei.[150]

But the situation in many other East European countries is different as they have become increasingly dependent on Chinese investments under the European arm of China's Belt and Road Initiative (BRI), or the so-called "17+1 BRI". Given concerns that the propensity for corruption in the region is high, the United States expended greater diplomatic energies in the spring of 2020 to persuade these countries to block Huawei, with US Secretary of State Mike Pompeo travelling to Hungary, Slovakia, and Poland. Slovakia's prime minister, Peter Pellegrini, maintained that Huawei should not be considered a security threat and argued that politicians should not intervene in competition among commercial entities.[151] Eventually, however, in October 2020, Poland signed the US "Clean Network" security initiative, which excludes Chinese hardware providers.[152] Most recently, Bulgaria, North Macedonia and Kosovo also signed on to the US "Clean Network" initiative.[153]

Another key partner of China in the "17+1" framework, Hungary and its prime minister, Victor Orban, have played down the security risks involved in dealing with Huawei,[154] even though Hungarian officials found their names on a leaked surveillance database compiled by a Chinese company.[155] Serbia, China's closest partner in Europe, has announced that it would work closely with Huawei for its 5G development and that it would maintain "technology neutrality". Huawei has also provided surveillance equipment for traffic and crime control in Serbia.[156]

[149] Filip Brokes, "Huawei Hoopla: 'Business as Usual' after Czech 5G Warning", Balkansinsight.com, 1 November 2019.
[150] Marcel Gascon Barbera, "Romanian conditions for 5G race would rule out Huawei", Balkaninsight.com, 5 August 2020.
[151] Aime Williams et al., "US warns of Huawei's growing influence over Eastern Europe", *FT*, 10 February 2020.
[152] Chris Duckett, "Four more European nations sign onto US 5G security agreements", ZDNet, 25 October 2020.
[153] "Bulgaria signs 5G deal with US excluding Chinese firms", AFP, 24 October 2020.
[154] Michael Peel and Nic Fildes, "EU draws up 5G Plans to screen security risks and Huawei fears", *FT*, 29 January 2020.
[155] CEPA, "Mapping the CCP's Westward Footprint", China Influence Monitor, 22 October 2020.
[156] Aleksandar Vasovic, "Serbia chooses links with China to develop economy, telecoms despite US warning campaign", Reuters, 13 August 2020.

Lessons for ASEAN?

Like the European Union, ASEAN and its 12 member states also need to determine the right balance between their economic and security interests. ASEAN considers the next-generation 5G as a game changer in its e-commerce, financial technology, and smart city development.[157] Like the European Union, it too feels sandwiched between US and Chinese pressure. It does not want to choose sides between the two major powers, the United States and China, in the light of the decoupling of their bilateral technology supply chains and the "balkanisation" of the global internet or what some refer to as "splinternet". Instead, like the European Union, it tries to uphold the principle of technology neutrality, which means the freedom to choose whatever technology is available for a country's specific needs.[158]

Also, similar to many smaller EU countries, ASEAN (with the notable exception of Singapore) appears to have overlooked many of the cybersecurity challenges of 5G and other disruptive technologies. Smaller and economically weaker countries do not have a deeply ingrained cybersecurity risk culture that allows them the ability to screen newly emerging technologies for inherent cybersecurity risks and vulnerabilities. Singapore already has in place a specialised team to prepare for its 5G rollout. Malaysia wants to build a centre for 5G cybersecurity. Brunei had already announced in 2019 that it intends to create a national cybersecurity agency. At the regional level, an ASEAN Framework for Digital Data Governance and concomitant forums and a formal ASEAN Cybersecurity Coordination mechanism have been initiated since 2019. The ASEAN–Singapore Cybersecurity Centre for Excellence and cybersecurity capacity building will also be enhanced.[159] With the exception of Vietnam and Singapore, hardly any other ASEAN country seeks to ban Huawei or any Chinese vendor. Singapore has already chosen Ericsson and Nokia, instead of Huawei, to install its national 5G network.[160]

But, on the whole, compared with the European Union, ENISA and the EC's cybersecurity policies, defined strategies, the toolbox of risk mitigating measures and compliance progress reports, ASEAN's collective cybersecurity policies appear to be at a rather early stage of development and implementation. In this light, closer cooperation between ASEAN and the European Union could benefit both sides. Despite criticisms that the progress made in many individual EU member states is insufficient and slow, the common cybersecurity strategies and defined security standards that they have developed (such as for the 5G rollout) have moved ahead during the past few years. The European Union can share its experiences and best practices in the 5G rollout and implementation of common cybersecurity strategies, defined risks, vulnerabilities, security standards and regulatory requirements. The European Union's experience may be particularly relevant for ASEAN as the EC and ENISA can officially only recommend and not directly enforce those policies against the sovereignty and political

[157] See also Stuart Lau, "ASEAN nations will consider Huawei as 5G supplier despite security questions", *SCMP*, 3 March 2020; and Amalina Anuar, "ASEAN Smart Cities: Balancing 5G and Geopolitics", RSIS Commentary No. 079/2020, 29 April 2020.
[158] See also Amalina Anuar, "ASEAN, 5G and the Great Tech Game", East Asia Forum, 29 April 2020.
[159] Amalina Anuar, "ASEAN, 5G and the Great Tech Game".
[160] Amalina Anuar, "5G in Singapore: Is the tide turning against Singapore?"

will of EU member states (although they supervise and verify the implementation of their recommendations). In this regard, the European Union can assist in the development of a cybersecurity regime for ASEAN, which would also be in the European Union's own wider foreign policy and global security interests.

Conclusion

Under President Xi Jinping, Beijing has promoted the concept of "cyber sovereignty" and the right to exercise control over the internet within and beyond its borders by advancing domestic surveillance at the expense of any privacy rules, rights and norms. Exercising control over the internet includes controlling political, economic, cultural and technological activities. By also lobbying for such rights and cyber sovereignty norms through international organisations (such as the United Nations), Beijing has also seen its policies increasingly backfiring as other countries and regional groupings (such as the United States and the European Union) are forced to reciprocate by declaring their own "digital sovereignty".[161]

For the US government, the security of 5G networks is non-negotiable and cannot be balanced with any vested economic, industrial or wider foreign policy interests. Since 2018 the US government has pressured its European and Asian allies to ban all Huawei technologies and gear. But the concerted actions of the Five Eyes (which Japan is interested to join[162]) and D10 alliances in regard to the cybersecurity challenges of 5G are not just the result of US diplomatic pressure but also a reflection of the other countries' own growing security concerns and increasing distrust of Beijing's new assertive "wolf warrior" diplomacy and geo-economic policies.

While US export-control measures and sanctions have undermined Huawei's prospects for becoming the dominant 5G supplier in Western democracies in the short-term, their long-term efficiency to constrain China's development and export of 5G equipment remains uncertain. Any effective US policy towards China will only succeed with the cooperation of America's friends, allies and partners in Europe and Asia. Winning such cooperation requires empathy, trust, collaboration and understanding of their interests and positions rather than bullying tactics and other coercive policies. In principle, the European Union has recognised that it needs an increasing transatlantic cooperation of democratic countries on new disruptive technologies and AI, as well as their inherent systemic cybersecurity risks and on China's policies in general.[163]

---

[161] Elliott Zaagman, "Cyber sovereignty cuts both ways", www.lowyinstitute.org, 7 August 2020.

[162] Five Eyes, founded in 1941, is the world's oldest intelligence sharing alliance. See Laura Zhou, "Does the US-led Five Eyes have wider sights on China?", SCMP, 8 August 2020.

[163] See also Jared Cohen and Richard Fontaine, "Uniting the Techno-Democracies", *Foreign Affairs*, November/December 2020, pp. 112-122; Marijn Rasser et al., "Common Code: An alliance Framework For Democratic Technology Policy", Center for New American Security, October 2020; David Moschella and Robert D. Atkinson, "Competing with China: A Strategic Framework", ITIF, August 2020; Eline Chivot and Raquel Jorge-Ricart, "The EU's Approach to 5G and the Reshaping of Transatlantic Relations", European Leadership Network, 10 September 2020; and Andrea Gilli and Francesco Bechis, "NATO and the 5G Challenge", *NATO Review,* 30 September 2020.

The German government and the European Union consider the decoupling efforts of the United States and China as well as having to adapt to technological self-sufficiency strategies to be alarming for both economic and foreign policy reasons. A complete decoupling from China on the scale envisaged by the US administration would be too costly to European companies. But the Trump administration's policies have also forced Germany and Europe into a new continuous balancing exercise involving their economic imperatives and security interests. With the advent of disruptive technologies, the European Union has found it ever more difficult in pursuing its relationship with China to separate its economic and trade interests from its wider security concerns, as well as democratic values and constitutional rights.

In so far as 5G policies are concerned, the transatlantic disagreement revolves not so much around the assessed cybersecurity risks linked with Huawei but rather the question of how to manage them. Each EU member has to balance economic benefits against the cybersecurity risks of involving Huawei in its 5G rollout by taking into account both US pressure and sanctions as well as factors governing its own bilateral relations with China and common elements governing EU–China relations. ENISA's toolbox of security guidelines with strategic and technical measures for 5G networks stops short of calling for an official ban on Huawei. While it does not mention Huawei by name, its recommendations include blocking high-risk equipment from at least the "critical and sensitive" parts of the network, including the core. The differentiation between the core and periphery networks looks like a perfect political–diplomatic compromise as no government wants to risk its economic, trade and investments ties with China. However, from a purely cybersecurity point of view, the traditional distinctions between "core" and the "non-core" periphery and between hardware and software are no longer possible or adequate for virtualised networks.

Moreover, cybersecurity cultures and capacities vary within the European Union. The United Kingdom, Germany, France, and a few other EU member states have the capacity to define and maintain "acceptable levels" of cybersecurity risks. But 10 other EU member states have neither institutionalised cybersecurity expertise and capacities for implementing comparable rigorous security-risk mitigation strategies nor do they have an entrenched cybersecurity risk culture to evaluate the cybersecurity risks of new disruptive technologies such as 5G. Nonetheless, as they struggle to implement comparably rigorous risk mitigation strategies, they have received increasing direct support from EC, ENISA and the bigger EU member states.

While US pressure has no doubt forced EU member states to review and rethink their 5G policies and helped to address the systemic cybersecurity risks inherent in 5G technology, their final positions, whether including or banning Huawei, have been increasingly influenced by their often deteriorating bilateral relationships with China — as in the case of France and Germany — as well as the overall state of EU–China relations. Even the United Kingdom's shifting policies are not so much the result of direct US political pressure but rather of the impacts of US sanctions, which have thrown into question Huawei's reliability as a supplier of 5G equipment. Some smaller European countries may still use

selected Huawei equipment (at least in the non-core sectors), thereby accepting a higher level of industrial and political espionage as well as cybersecurity risks related to Chinese-supported cyber theft and espionage activities. But if the European Union and its member states want to uphold the credibility of their own policies, then the newly defined principle of reciprocity in EU–China relations would also call for banning Chinese companies in the European 5G rollout as long as Beijing does not grant the same market opportunities for European companies. For the time being, Ericsson, Nokia and Samsung are already benefitting commercially from banning Huawei in the future 5G networks of many European and other countries.

A growing fragmentation of the internet and cyberspace between like-minded democracies on one side and China as well as other authoritarian states on the other side is already under way. Against this backdrop, several other countries are trying to balance their security and economic interests in relation to China. But such balancing may only work for some time. The Western democracies (such as D10), including the European Union, will incentivise their own companies to race towards developing the next "6G network technology" in order to decrease their technology dependencies on China and maintain their digital sovereignty. This development would also allow the European Union as well as the security committees of its member states collectively to define new security standards and build them into the design of the 6G networks right at the outset rather than try to retrofit security standards after the development of 6G technologies, which would only provide second-best security solutions.

China and Huawei have proposed new standards for core network technology (called "IP") at the UN's International Telecommunication Union (ITU), claiming that current global networks are "unstable" and would be "vastly insufficient" for the future digital world by 2030. These proposals have been perceived not just in the United States but also in the European Union as threatening their strategic interests. The Chinese government does not seek just to strengthen its control over the use of the internet by its citizens and within in its own country but increasingly also globally by expanding its authoritarian controls via UN institutions (such as the ITU and the World Health Organisation). Its position is supported by Russia, Saudi Arabia and even some European countries. Both the EC and many EU governments have not articulated their final positions but are still seeking advice from experts and partners from outside while also looking to develop political consensus among EU member states. In this regard, EU–ASEAN collaboration on future digital and cybersecurity standards would benefit both sides.

About the Author

Dr Frank Umbach has been an Adjunct Senior Fellow of RSIS since September 2017. He graduated from the University of Bonn with an MA in Political Science and a PhD. He is currently Research Director at the European Cluster for Climate Energy and Resource Security (EUCERS)/Center for Advanced Security, Strategic and Integration Studies (CASSIS) at the University of Bonn; and a Senior Lecturer at the University of Bonn; a Visiting Professor at the College of Europe in Natolin (Warsaw) in Poland, where he teaches “EU energy (foreign) policies", and an Executive Advisor at ProventisPartners, Munich (an M&A company). He is also a consultant for NATO, giving regularly presentations at high-level NATO conferences and seminars, and the Gerson Lehrman Group (GLG) and Wikistrat.com. He is an internationally recognised expert on global energy security, geopolitics, critical (energy) infrastructure protection, and (maritime) security policies in Asia–Pacific as well as Russia/Central Asia.

From 2014 to 2017, Dr Umbach had been an independent subject matter expert on international energy security for NATO’s annual “Strategic Forecast Analysis”. Between 2012 and 2015, Dr Umbach was a non-resident Senior Fellow of the Atlantic Council in Washington, DC. From 2003 to 2007, he was Co-Chair of the European Committee of the Council for Security Co-operation in Asia–Pacific (CSCAP–Europe). From 1996 to 2007, he headed the “Security Policies in Asia–Pacific” and “International Energy Security” programmes at the German Council on Foreign Relations (DGAP) in Bonn and Berlin. Earlier, he was a Research Fellow at the Federal Institute for East European and International Studies (BIOst) from 1991 to 1994 and a Visiting Research Fellow at the Japan Institute for International Affairs in Tokyo from 1995 to 1996.

Dr Umbach has done consultancy work and testimonies for: the German Ministries of Foreign Affairs and Defence Policies; European Commission and European Parliament; US State and Energy Departments; the US–China Economic and Security Review Commission of the US Congress; the Lithuanian Government; the House of Lords of the British Parliament; the Polish Foreign and Economic Ministries; Hungarian Foreign Ministry; South Korean Foreign Ministry; NATO; United Nations; Organization for Security and Co-operation in Europe (OSCE); World Energy Council; and the Federation of German Industries (BDI). He has also consulted for several energy and consultancy companies (including APCO and Roland Berger) and has advised international investors through GLG.

Dr Umbach is the author of more than 500 publications in more than 30 countries. These publications include the papers he has written as a contract author for the Geopolitical Intelligence Service (GIS) in Liechtenstein since 2011.

About the S. Rajaratnam School of International Studies

The S. Rajaratnam School of International Studies (RSIS) is a think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education and networking, it produces research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.

For more details, please visit www.rsis.edu.sg. Join us at our social media channels at www.rsis.edu.sg/rsis-social-media-channels or scan the QR code.

RSIS Working Paper Series
(from 2018 onwards)

332	EU-Policies on Huawei and 5G Wireless Networks: Economic-Technological Opportunities vs Strategic Risks of Cybersecurity *Frank Umbach*	(2020)
331	The Route to Radicalisation for Malay-Muslim Women: Tracing the Nexus between Universals and Particulars in Malaysia *Piya Sukhani*	(2020)
330	The Asia Pacific's "Age of Uncertainty": Great Power Competition, Globalisation and the Economic-Security Nexus *Evelyn Goh*	(2020)
329	The New "Rare Metal Age": New Challenges and Implications of Critical Raw Materials Supply Security in the 21st Century *Frank Umbach*	(2020)
328	Australia as a Rising Middle Power *Malcolm Davis*	(2020)
327	The Intersection of Emergent Technologies and Geopolitics: Implications for Singapore *Muhammad Faizal Bin Abdul Rahman*	(2020)
326	The "Indo-Pacific" Concept: Geographical Adjustments and their Implications *Wada Haruko*	(2020)
325	China's Belt and Road Initiative – A Perception Survey of Asian Opinion Leaders *Pradumna B. Rana, Chia Wai-Mun and Ji Xianbai*	(2019)
324	Capturing Anti-Jokowi Sentiment and Islamic Conservative Masses: PKS 2019 Strategy *Adhi Priamarizki and Dedi Dinarto*	(2019)
323	Propositions on Sino-American Trade Dispute: Some Helpful Ideas from Social Science *Steve Chan*	(2019)
322	Examining the Growth of Islamic Conservatism in Indonesia: The Case of West Java *Irman G. Lanti, Akim Ebih, Windy Dermawan*	(2019)
321	Financial Development in Myanmar and the Role of Japan *Tomoo Kikuchi, Takehiro Masutomo*	(2019)
320	China's Belt and Road Initiative and its Energy-Security Dimensions *Frank Umbach*	(2019)

319	The Hindu Rights Action Force and the Malaysian Indian Minority after the 2018 General Election in Malaysia *Arunajeet Kaur*	(2018)
318	The Fourth Industrial Revolution's Impact on Smaller Militaries: Boon or Bane? *Nah Liang Tuang*	(2018)
317	Pakistan and its Militants: Who is Mainstreaming Whom? *James M. Dorsey*	(2018)
316	Securing Energy Supply and Maritime Interests: Seeking Convergence *Frank Umbach*	(2018)
315	Is Use of Cyber-based Technology in Humanitarian Operations Leading to the Reduction of Humanitarian Independence? *Martin Stanley Searle*	(2018)
314	Game of Institutional Balancing: China, the AIIB, and the Future of Global Governance *Kai He and Huiyun Feng*	(2018)
313	Xi Jinping and PLA Transformation through Reforms *You Ji*	(2018)
312	Comparing the Governance of Islam in Turkey and Indonesia: Diyanet and the Ministry of Religious Affairs *Martin Van Bruinessen*	(2018)
311	Indonesian Muslims in a Globalising World: Westernisation, Arabisation and Indigenising Responses *Martin Van Bruinessen*	(2018)
310	Theocracy vs Constitutionalism in Japan: Constitutional Amendment and the Return of Pre-war Shinto Nationalism *Naoko Kumada*	(2018)
309	Cyber Deterrence in Singapore: Frameworks and Recommendations *Eugene EG Tan*	(2018)
308	Trade Policy Options for ASEAN Countries and Their Regional Dialogue Partners: "Preference Ordering" Using CGE Analysis *Xianbai Ji, Pradumna B. Rana, Wai-Mun Chia, and Chang Tai Li*	(2018)

Visit the RSIS website at www.rsis.edu.sg/working_papers/

to access the full list of past RSIS Working Papers.