

Research paper

The governance of 5G infrastructure: between path dependency and risk-based approaches

Roxana Radu^{1,2,*} and Cedric Amon³

¹Global Governance Centre, Graduate Institute of International and Development Studies, Chemin Eugène-Rigot 2A, CH-1202 Geneva, Switzerland, ²Centre for Socio-Legal Studies, University of Oxford, Manor Road Building, Manor Road, Oxford OX1 3UQ, UK and ³Graduate Institute of International and Development Studies, Chemin Eugène-Rigot 2A, CH-1202 Geneva, Switzerland

*Correspondence address: Global Governance Centre, Graduate Institute of International and Development Studies, Chemin Eugène-Rigot 2A, CH-1202 Geneva, Switzerland. Tel: +44-1865-278700; E-mail: roxana.radu@graduateinstitute.ch

Received 5 May 2020; revised 13 July 2021; accepted 23 July 2021

Abstract

The fifth generation (5G) wireless technology promises a powerful, reliable and fast infrastructure to match artificial intelligence and Internet of Things developments. But its rollout has stirred strong political tensions around the prominent role that Chinese providers might be allowed to play in building the new networks. Between 2018 and 2020, a few countries have banned—partially or totally—the use of networking equipment produced by Huawei and ZTE, while others have mandated technical and security reviews to mitigate the risks associated with Chinese-origin components in the national 5G infrastructure. This article provides a thematic analysis of the security arguments and policy options emerging in the early days of the 5G debates. Based on key high-level statements, parliamentary debates and legislative acts published from mid-2018 to 2020, we examine perceived risks and threats surfacing in the public discourse, as well as the main regulatory directions emerging in seven countries. Our analysis shows policy alignment across multilateral commitments such as the European Union (EU) or the Five Eyes intelligence alliance. While selected EU member states lean towards risk-based governance and adaptive policies, Five Eyes nations opt for pre-emptive bans of 5G Chinese vendors, revealing path-dependent strategies for the sector. We conclude by discussing the policy reversal experienced by the UK in 2020 and the consolidation of new governance approaches for 5G infrastructure.

Key words: 5G, infrastructure, Huawei, cybersecurity, risk-based governance, path dependency

Introduction

As the search for universal cyber norms continues, new ways of dealing with uncertainty around basic infrastructure emerge at the national and regional levels, reflecting both hard and soft power strategies. The recent fifth generation (5G) network debates have focused on the role that China plays in furthering insecurity, triggering diverse policy responses. In what has come to be known as the ‘5G war’ [1], a few governments—such as Australia, the United Kingdom, the United States—have excluded Chinese supplies from 5G infrastructure bids at the national level and have limited government purchases of wireless communications equipment that included Chinese components. While some countries have made it explicit that the addressees of

5G bans were the high-risk Chinese vendors, others decided to adopt vendor-agnostic strategies that did not limit market competition. This analysis seeks to uncover how states design national governance approaches for emerging technologies by exploring the extent to which their approaches are influenced by path dependence or risk management.

The early days of the 5G debates provide an insightful starting point. Since the Snowden revelations of mass surveillance in 2013, the sources of uncertainty surrounding new technologies have generally been scrutinized more closely, but have rarely ever triggered as many public debates and inquiries as the involvement of Huawei in the 5G networks. The planned 5G rollout has been a source of

political tension for three main reasons. First, competition for leadership in 5G networks and for a privileged market position for future 5G-based technologies remains fierce. Second, risks associated with dependence on critical equipment controlled by a foreign government have started to be seriously investigated, in particular as the evidence of breaches and state-sponsored cyberattacks has increased over the years. Third, 5G has the potential to transform the digital economy, giving increased weight to software and cloud service providers and shifting focus away from individual users to business-to-business models [2]. This article explores two dominant modes of governance emerging in nascent 5G discussions, contributing theoretical and empirical depth to both academic and policy debates on the topic.

Numerous high-level statements and media reports released since 2018 underlined the multitude of risks associated with the use of 5G equipment manufactured by Huawei and ZTE, stressing fears of espionage and software vulnerability exploitation by the Chinese authorities, amid an ongoing trade war with the United States. Yet the geopolitical and diplomatic ramifications of these developments went much further. After declaring ‘a national emergency with respect to this threat’ [3], the United States urged European allies to ban Huawei’s 5G technologies and threatened to cut ties with the British intelligence services in case they rejected a ban on Chinese-built infrastructure. These concerns are reflective of a broader, contending perspective on digital and technological sovereignty. While national control and jurisdictional issues in cyberspace have been around for decades, the 5G rollout has elevated the strategic autonomy discourse to a new level.

Drawing on recent developments in 5G policymaking, we suggest that the sidelining of Chinese manufacturers in the 5G rollout can be understood by combining two strategies to defend sovereignty. The first is embedded in path dependency, with a strong tendency to follow previous regulation directions, while the second is derived from risk-based governance, emphasizing mitigation strategies for specific threats. Drawing on a systematic review of policy documents and thematic analysis of key high-level statements, parliamentary debates and legislative acts passed between mid-2018 and mid-2019, this article offers an in-depth comparative analysis of the governance approaches envisioned in the early stages of 5G deployment. It puts forward two theoretical approaches to understand the drivers behind the policy solutions adopted by selected European Union (EU) member states and Five Eyes (FVEY) alliance members. The UK—part of both groupings at the time—made a U-turn on its 5G approach in mid-2020, switching from partially allowing Huawei technology into its 5G edge network to excluding Huawei from its networks entirely. This policy stance is thus explored in a case study. The final part of this analysis provides future directions to be scrutinized in the ongoing 5G controversy.

Theoretical Lens: Path Dependency and Risk-Based Governance

While remaining a highly specialized debate, 5G deployment has reached an unprecedented level of public attention. But how are states deciding on their governance approach on the matter? To what extent are the policy options under discussion driven by path dependency or an in-depth risk evaluation? We put forward two theoretical models in order to distil the complex reality of governing 5G. Our contribution fills an important gap in the empirical analysis of the governance arrangements set up by states to deal with the uncertainties and threats posed by new technologies and their appeal

to particular strategies of risk mitigation. Transnational policy coordination thus provides an important geopolitical angle. This can be seen in the EU, where there are proposals for the adoption of supranational instruments such as the investment screening guidance and the creation of a toolkit of regulatory instruments for member states. This makes it clear that there is no one-size-fits-all answer.

Security has been a top priority in the 5G debates, ‘a primary purchasing point—something that was not done for previous networks’ [4]. Security has long structured adversarial and cooperative interactions in the digital era, as acknowledged by both scholars [5–8] and policymakers [9–11], but the deployment of 5G revealed a new range of concerns around cyber sovereignty, from emerging threats [6, 12] to technological independence. To date, there has been little literature dedicated to the policy arrangements in place to deal with this type of insecurity. In determining security-related policies, states have long defined critical threats to core infrastructure and proposed excluding providers from the market in what has become a path-dependent policy process applied to 5G. An alternative governance strategy has been to break away with past decisions and evaluate new risks and threats on their own merit in order to establish the best course of action. These two approaches are well documented in the literature and are discussed below in order to identify key explanations for the 5G policy options implemented by early adopters.

Path dependency

Path dependency is a well-established theoretical concept in political science [13–17] and institutional economics [18, 19]. Disciplines as diverse as anthropology and economics have embraced its tenets, providing many definitions for this concept. In broad terms, there is agreement that it refers to actions and decisions from the past that shape and affect current and future policies [20, 21], without fully determining the evolution of policies in a certain field. As such, a degree of rigidity remains embedded in national processes based on past legacies. Following Karl [22], the early stages in a process appear to be more decisive for the dependency pattern. Technology debates show that, to respond to uncertainty, countries might select linear trajectories, indirectly shaped by past events and their externalities [23]. Accordingly, the decisions on how to manage 5G concerns would be strongly influenced by previous practices and constraints, in particular a cyber defence mindset with a focus on ‘securing’ the infrastructure.

On a technical level, 5G networks build on existing 4G infrastructure and thus on legacy networks, giving competitive advantage to a small number of providers and exacerbating the problem of vendor diversity in the deployment of the latest generation [24]. Despite it being presented as more secure than its predecessors, 5G also inherits vulnerabilities and flaws from prior generation networks [25–27]. Although there have been no publicly proven cases of breaches or abuse of the equipment by Chinese companies during 5G trials (at the time of writing), suspicion about their growing influence in the global information and communications technology (ICT) infrastructure and their ties to the country’s intelligence services have long been present in the West.

In the last decade, a number of countries had specific policies in place to mitigate risks connected to Chinese providers. Australia imposed an early ban on Huawei in 2012, restricting its bidding on their national broadband network [28]. In 2013, for its 4G rollout, the United States effectively banned the governmental purchase of any technology from companies thought to be ‘owned, operated or subsidized’ by the People’s Republic [29]. Given the significant extent to which 5G relies on previous generation infrastructure, countries

like the UK have considered the significant market share of Huawei in their 4G networks and have historically listed the company as a ‘high-risk vendor’. It is thus expected that these countries might continue to impose restrictions on Chinese manufacturers of 5G technology in line with their previous actions. While there is consensus in the path dependency literature that history matters and the articulation of legacies limits the decisions and options available, less is known about the extent to which the trajectory chosen by one state depends on membership in a particular grouping. Our analysis of two country groupings goes in this direction, uncovering the key levers affecting decision-making, as they surface in public discussions.

Risk-based governance

An alternative governance strategy pursued in high-risk cases has been derived from the evaluation of new threats introduced by emerging technologies. Risk-based governance defined the level of protection as proportional to the level of risk and promised a better allocation of scarce resources and improved transparency of political decisions [30]. It has, in some sectors, also been legally mandated. Risk is generally understood as ‘a combination of probability and adverse impact’ [31]. This definition also incorporates ‘quantification and science-based assessments (‘objectively’ calculating risk); monetarisation of adverse consequences [...]; and the use of probability theory to reduce uncertainty as much as possible’ [30], acknowledging it is impossible to eradicate risk completely. Moreover, the promise of increased connectivity and the opportunity to connect billions of new Internet of Things (IoT) and artificial intelligence (AI)-powered devices via new technology augment existing risks, such as the high surveillance potential of 5G, which can be more fully exploited by both governments and industry.

The recognition that risks have to be continuously managed is at the core of this governance approach. Yet evaluating risk in the 5G deployment and in the digital sphere more broadly remains challenging due to the recognition that not all threats can be known, anticipated or avoided. This recognition is also an important element in industrial risk management, considering that companies have to navigate complex environments within a rapidly changing risk landscape [32]. The focus on ‘resilience’ allows for the shifting of strategic resources from exclusively defensive capacities to absorbing and quickly recovering from inflicted damage [33, 34]. Therefore, risk-based governance mandates the integration of resilience models and mitigation strategies, paying particular attention to the identification and protection of key assets. For 5G-related risks, a cyber resilience mentality might consider multi-vendor solutions in order to build strategic autonomy.

The literature points out that risk-based decisions offer ways to protect government officials from blame in case of policy failure [30, 35, 36]. When translated into policymaking, risk-based governance ‘involves complex choices between competing political priorities and policy alternatives within the limits of the available resources’ [37]. In the case of 5G, policymakers introducing risk-governance strategies have to find appropriate solutions to maintain the security of the infrastructures and to navigate their political repercussions. Experimental approaches might thus be preferred. Sanderson identifies trial-and-error strategies in localized areas as a promising alternative to evidence-based approaches that purely support the often defended position of ‘what matters is what works’, arguing that ‘policies are essentially ‘conjectures’ based upon the best available evidence’ [30].

This idea is also embedded in the concept of policy ‘sandboxes’, welcomed and implemented by a number of countries in relation to fintech and cryptocurrencies [38, 39]. Sandboxes, with their submis-

sion and selection criteria [38], offer the advantage of applying the burden of proof to the applicant while operating in a limited scope. In the case of 5G, this could mean that network suppliers apply for the delivery of their technology to a designated authority. Additionally, the applicants would have to provide guarantees to compensate consumers in case of adverse outcomes caused by their product. Moreover, in evaluating such experiments, policymakers would be able to focus on the processes as much as on the outcomes [36, 37, 40] and adjust the regulatory frameworks as needed. However, for the time being, sandbox approaches have not been prioritized in 5G discussions, since there is indeed little margin for error in mitigating large-scale security risks and there is urgency to adopt this ‘game-changer’ technology.

Importantly, the adoption of risk-based governance is sometimes at odds with the normative culture of states and the understanding they have of their own role with respect to the protection of their citizens [40]. The ability of governments to justify calculated risks and the (un-) foreseeable limits of governance therefore also depends on the respective national political systems [36]. A 2012 analysis of the patterned adoption of risk-based governance in the UK, France and Germany showed that the trust in and the understanding of the state played an important role in how this type of governance was implemented [36]. In France for example, the role of the state as the responsible entity for its own as well as the public’s safety clashed with the notion of ‘acceptable or unavoidable risk’. Moreover, in both France and Germany, the constitutionally determined right to equal treatment prevented the government from making distinctions in the allocation of resources to certain populations based on risk assessments.

Mapping 5G Developments

While many countries prepare to introduce 5G, this new technology remains a Gordian knot. Unlike previous wireless generations, 5G is more widely discussed in mainstream media and public forums, whether for health-related concerns [41–43] or geopolitical issues [4, 44, 45]. These public debates come at a critical juncture, as governments are assessing the impacts of 5G ahead of its rollout, showing increased awareness of the long-term effects of procurement choices. 5G networks, upping the volume, latency and speed of wireless networks, are crucial for large-scale IoT applications (e.g. smart cities) and real-time AI operations (e.g. autonomous vehicles), thus being of strategic importance to governments. At a time of AI national strategies mushrooming [46], 5G debates have been divided between the pursuit of market-based and national security approaches. The augmented security concerns in the 5G rollout reveal a combination of technical, political and economic considerations. Yet the boundaries between technical motivations and geopolitical rationales become blurred in the public discourse. The frequent media reports on the topic have reduced the 5G tensions to great power rivalries between the United States and China and economic competition and espionage potential, overshadowing the complexity of risks associated with rolling out a new wireless technology. We posit here that it is all the more important to explore the underlying logics structuring the public debate by presenting the arguments in full light and zooming in on the ways in which national actions interconnect.

The analysis starts by mapping the main issues under discussion in the early days of 5G introduction, providing an overview of the global developments, followed by a timeline of regulatory and legislative developments at the national level. The countries that have taken the lead on addressing Huawei’s presence in their 5G networks

were the first to put forward policy responses to the complex issues and concerns raised so far. This section sets the basis for investigating more closely the national and regional approaches to 5G risk governance.

Global landscape

Security concerns have always been central to the governance of new technologies [47–49] and 5G is no exception. Cybersecurity became a dominant matter of interest in the early 1990s [50] and continues to drive inter-state negotiations, in particular for managing global resources such as the domain name system [50, 51] and for building norms [52]. Critical infrastructure protection has developed into a field of its own, covering not only technical, but also diplomatic discussions, such as the ones conducted by the various United Nations Groups of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security¹. Previous global cybersecurity discussions have already included clear references to wireless equipment requiring special protection to ensure its availability and integrity. The ‘Call to protect the public core of the Internet’ issued by the Global Commission on the Stability of Cyberspace refers to transmission media as critical infrastructure, in particular (i) infrastructure, systems and installations for communications serving the public, whether fibre, copper or wireless; and (ii) cellular and other wireless voice and data communications. Private sector initiatives, like the Tech Accord² or the Digital Geneva Convention, also shed light on the crucial role of the private sector in managing core infrastructure. Against the pre-existing challenges of finding common ground regarding Internet security issues, the uncertainty surrounding the 5G safety levels adds another layer of complexity to debates that have not yet reached the level of multilateral negotiations in international venues.

The world’s largest producers of 5G antennas are Huawei, Nokia and Ericsson.³ A Chinese giant with a revenue of 107 billion dollars in 2018, Huawei’s profits are mostly derived from manufacturing consumer-oriented wireless equipment. Market dominance by the Chinese has been repeatedly acknowledged as a threat [54–56], given that the latest wireless technology is projected to enable new market leaders in a similar way in which 4G was key to companies such as Google and Apple in the mobile sphere [54]. The early adoption of this technology is therefore key to remaining competitive not only in the telecommunications market, but also in other areas that will benefit from faster information transmission. However, the number of vendors of 5G equipment is low and competition in the market is limited by patent submissions, in particular those coming from Chinese operators [57]. Huawei and China Mobile have made significant contributions to the elaboration of the 5G standards in the 3GPP framework⁴ [58] and own a non-negligible amount of patents

that will be necessary for the operationalization of the new network technology [59, 60].

Moreover, China increasingly projects ‘cyber power’ [61] through its Belt and Road Initiative (BRI), the largest infrastructure development project of the century, spanning >150 countries across four continents. As part of the BRI plan, the Digital Silk Road initiative provides support in building fibre optic and connectivity, accompanied by technical assistance and Chinese expertise. Huawei and ZTE, another Chinese infrastructure provider with a revenue of 12.7 billion dollars, stand to gain massively from the BRI. This, in turn, creates concerns that China might not only be exporting technology, but also some of its domestic regulations and practices, which include mandatory SIM card registration and extensive surveillance. The projection of cyber power is also reflected in the elaboration of technical standards. While the efforts to establish itself as a dominant force in ICT standard-setting can be traced back by at least two decades [62], the strong support of the Chinese government for the development of new standards has been a source of concern for Western policymakers as the primacy of standards does not only secure a first-mover advantage [62], but also constitutes an ‘instrument of international power competition’ [44].

National dynamics

With security as the main determinant of public policy in relation to 5G, a paradox noted by Edwards gains new meaning: ‘the route to national security is more global approaches to the management of technology. But national security is at the centre of current approaches to global security’ [63]. Security measures previously deployed in the cyber domain, characterized by a ‘fundamental uncertainty’ [64], have generally included personnel vetting and restricted access to sensitive information, software-level protections such as antiviruses, insurance and certification schemes, and, more recently, government-mandated limitations in selecting infrastructure providers. In 5G, the governance of (systemic) risk is closely related to complexity, uncertainty and ambiguity [65, 66], further translated into a bundling of arguments combining national security with state objectives in defence, economy and society domains. In its 2019 threat landscape report, the European Union Agency for Cybersecurity (ENISA) concluded that the most pressing 5G threats fall in the three main traditional categories of cybersecurity risk, being related to the compromise of confidentiality, availability and integrity [24]. A survey of EU member states showed that disruptions to the local or global 5G networks are most feared (availability), followed by spying of traffic and data circulated (confidentiality) and modifications or alterations of traffic and information systems (integrity, confidentiality and availability).

Against the existing global challenges, 5G connectivity changes the current cybersecurity paradigm, due to a virtualized environment that augments large-scale risks [67]. National strategies to cope with these new forms of uncertainty began to emerge in 2018, when states started recognizing that the nature and the fast pace of technological developments require a regular reclassification of what constitutes critical infrastructure [68] and what constitutes risk [69]. The reliance on software updates for the maintenance of the networks is an additional source of concern considering that the network operators might become heavily dependent on foreign (and potentially untrustworthy) network suppliers. As governments start auctioning

1 Formerly: UN Governmental Group of Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE).

2 The Tech Accord is a Microsoft-led alliance of tech and security companies formed in April 2018 to oppose the use of their technologies for cyberattacks and surveillance. By 2019, it had >90 members.

3 Certain functions, such as the Radio Access Network (RAN), are only provided in large scale by these companies, also known as the ‘Big 3’. Open source alternatives, such as the OpenRAN initiative promoted by Telecom Infra Project, aiming to develop vendor-neutral hardware and decoupled software, represent an exception [53].

4 According to the Strategy Analytics report from 17 March 2020, out of 600 member companies in the 3GPP, Huawei is the clear leader in contributions

to Release 15 and 16, followed by Ericsson, Nokia, Qualcomm and China Mobile.

frequencies for 5G deployment, the limited vendor diversity emerges as a wicked problem for designing national strategies.

Moreover, the distinction between core and edge technology plays an important role in policymaking given that the core layer has much greater control of the overall infrastructure while the edge layers will operate as an access point for connectivity [70]. However, many critics contend that the distinction between core and edge is misleading, since 5G networks use virtualized hardware [71], implying that security threats cannot be mitigated by restricting the access of high-risk vendors to ‘edge’ infrastructure only [72]. Given that the processing of information occurs on virtually separated networks⁵, the fear is that the frequent software updates, required for the maintenance of the network, can be used to incorporate vulnerabilities into the network, thus making it possible to gain access to the core of the network.

In the absence of universally accepted norms or international treaties on 5G deployment, do governments rely on path dependency or risk governance for structuring their national approaches? As of July 2020, the imposition of a full or partial ban on the use of Chinese-origin equipment or high-risk vendors has remained limited to a few countries: the United States, Australia, New Zealand and the UK. Many other countries, especially from the EU, remain undecided on the issue and have asked for technology reviews and security screenings before proceeding with regulation (Germany, the Czech Republic). Others—like France—have preferred introducing national safeguards (e.g. licensing, contracting requirements). Few countries went ahead with planning for their 5G infrastructure without any restrictions for Chinese providers (primarily those associated with the BRI). Between August 2018 and July 2020, the trajectories followed by most governments active on 5G have not been linear. Table 1 below provides a chronological overview of the main developments that have led to the adoption of national positions. The measures taken during this period form the basis for our selection of countries to include in the analysis, further discussed in the methodology section.

Having outlined the evolution of regulatory measures in the 5G field, we now turn towards the rationale put forward by countries in their discussions of security safeguards needed prior to opening a competitive market for wireless technology. National 5G policy design is scrutinized below to understand whether path dependency or risk governance are deliberate choices. Our research provides the first systematic analysis of the arguments put forward in governing 5G-related risks, filling an important gap in the cyber risk literature and grounding key policy discussions about new wireless technology. Our analysis starts with the identification of the main differences between the path-dependent and risk-based trajectories in two groupings: the EU and the FVEY.

Method

In this study, we used a qualitative approach relying on thematic analysis to identify the key security-related sub-themes emerging in the 5G debates between mid-2018 and mid-2019. A thematic analysis of sources of risk and regulatory approaches was performed for seven states belonging to two multilateral groupings, the EU and FVEY. The states included in the analysis were the first to react to Huawei’s involvement in the 5G rollout. For the period comprised between

mid-2018 and end of 2019, the analysis focuses on the Czech Republic, France, Germany, UK, as members of the EU; and the UK, Australia, New Zealand and the United States, as members of the FVEY alliance, respectively. Part of the two groupings, the UK deserved a separate case study, for which we complemented the analysis with national policy documents, literature and news reports released until the end of July 2020. Thematic analysis, not strictly linked to epistemological or theoretical traditions, has proved to be useful for analysing ongoing developments, in particular by providing a degree of flexibility in finding and interpreting a patterned response or meaning in the dataset [73–75].

Two factors determined the selection of countries included in this study: (i) the availability of public documents and policy proposals in the early phase of the 5G debates (as indicated in Table 1) in the countries that reacted first; and (ii) the possibility to follow the debates at the national level, which resulted in privileging English, French and German sources that the researchers could analyse. The seven countries thus selected (presented in Fig. 1 below) share certain commonalities such as membership in the FVEY intelligence sharing alliance or EU membership, which are likely to influence their multilateral constraints and result in 5G policy convergence. At the time of writing, the UK was part of both groupings, requiring further contextualization of its position.

Our dataset was made up of policy documents released between August 2018 and July 2019⁶ on the deployment of 5G in seven countries. The corpus comprised 33 national documents and 4 supranational documents issued by the EU, which included executive orders, supranational direction documents, national legislation and guidance, reports and non-binding affirmations of principles. An overview of these is available in Annexure 1. Two coders read the documents to identify, adjust and group the themes for the final analysis. In the second stage of the research, we updated the information regarding regulatory measures with documents released between July 2019 and August 2020 for the case of the UK and followed the same process.

Thematic analysis requires various iterations of data interpretation and its multi-stage process includes: text familiarization, coding, generating and reviewing themes and defining and interpreting the themes [76]. A theme is then identified not according to quantifiable measures, but according to its ‘keyness’ [74] or centrality. In our analysis, it was important to scrutinize qualitatively the semantic content employed in each document, as the phrasing for individual themes differed across various national contexts. Three dimensions of analysis were then identified: (i) sources of concern, (ii) security arguments framing and (iii) approach to regulation. Table 2 below presents a few such instances based on our thematic mapping:

The themes assigned in our analysis underscore the key narratives supporting regulatory action in the 5G market. The first two, sources of concern and security arguments, presented the highest code co-occurrence, leading us to explore the extent of their overlap in the section below. The second focus in our analysis, the approach to regulation, brought forward how the risk and threat framing influenced governmental action.

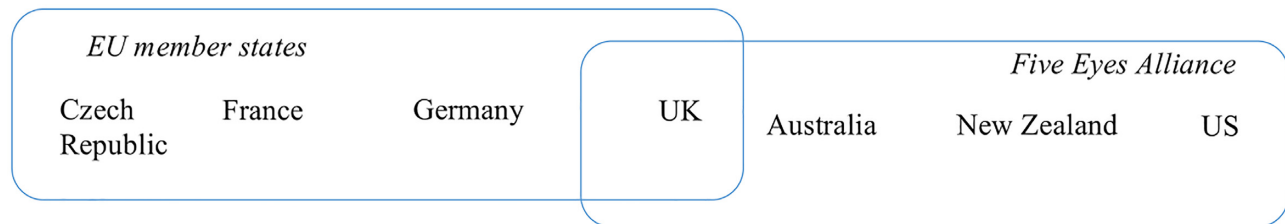
Findings

⁵ The separation between the ‘core’ and the ‘edge’ of the network is made possible through a key feature, the ‘Software Defined Networks’, which allows users to connect their devices onto virtual rather than physical networks.

⁶ Out of these, three were issued prior to 2018 and were kept in the analysis as they informed policy approaches or decisions adopted during the period under investigation in this study.

Table 1: Overview of main developments in 5G policy discussions between August 2018 and end of 2019

Date	Country	Event
13 August 2018	US	National Defense Authorization Act approved by the Congress, banning governmental purchasing of Huawei and ZTE equipment or services
23 August 2018	Australia	Telecommunications Sector Security Reforms passed, prohibiting Chinese companies from participating in the national 5G rollout
8 November 2018	UK	Telecoms Supply Chain Review Report published, detailing supplier and procurement aspects related to network security
28 November 2018	New Zealand	Spark-Huawei bid for the first 5G deployment rejected by the Government Communications Security Bureau
17 December 2018	Czech Republic	Warning issued by the Czech Republic National Cyber and Information Security Agency (NCSISA) against the use of Huawei and ZTE
December 2018	Japan	Directive prohibiting government purchases of communications equipment that pose a security risk
22 February 2019	US	Government threatens to end intelligence-sharing with allies that buy Huawei equipment.
22 March 2019	EU	European Council expresses support for a concerted approach to the security of 5G network.
26 March 2019	EU	European Commission recommendation calling on member states to complete national risk assessments and review national measures, to work together at EU level on a coordinated risk assessment and to prepare a toolbox of possible mitigating measures
28 March 2019	UK	Huawei Cyber Security Evaluation Centre report published, criticizing the technical quality and security of Huawei equipment
15 May 2019	US	Executive Order passed by President Trump prohibits US companies from using technology from companies deemed a national security threat; Department of Commerce adds Huawei to the Entity List, preventing US firms from selling components to Huawei.
3 July 2019	France	National task force proposes a bill to increase governmental oversight of 5G network rollout, specifying 'defense and national security parameters'.
15 October 2019	Germany	Actualization of the security requirements for telecommunication systems
13 November 2019	Germany	Completion of the review of the security requirements for telecommunication systems
27 April 2019	Czech Republic	Czech President expresses support for Huawei's participation in 5G deployment during a meeting with Huawei founder Ren in Beijing.
3 May 2019	Czech Republic	Czech Republic holds a meeting with like-minded EU and NATO nations on 5G security best practices (Prague Proposals).
1 August 2019	France	The Law N 2019-810 passed, allowing authorities to restrict, prohibit or impose requirements or conditions for the supply, deployment and operation of 5G equipment by mandating an authorization from the Prime Minister before rolling-out and operating sensitive equipment for 5G networks
9 October 2019	EU	The European Commission and ENISA publish a report on the EU Coordinated Risk Assessment on Cybersecurity in 5G Networks.

**Figure 1:** Country case selection representation according to their main multilateral commitments.

The timely rollout of 5G has been a strong commitment by many governments around the world, in particular for seizing economic opportunities and technological benefits for their populations. But what governance approaches are they choosing for the rollout of this new wireless technology? In the seven countries we analysed, the introduction of 5G has been heatedly debated between mid-2018 and mid-2019, when regulatory stances started to crystalize. The high-level statements, policy positions and reports issued in response to proposals for upgrading wireless infrastructure have cut across sectoral boundaries, garnering reactions from heads of state, members of the executive, parliamentarians, heads of businesses and intelligence agencies. The latter have exerted increasing influence over norm-

setting in cyberspace in recent years [77] and have forged new links between the technical assessment of intrusion and the public debate, previously a prerogative of media actors [78].

The progression and sophistication of the 5G security arguments reveal fundamental tensions not only on a technical, but also on a political level. The clearest example comes from the United States, where officials have tried to influence other national debates and push for a rejection of Chinese components in 5G infrastructure, in particular among the FVEY allies: Australia, Canada, New Zealand, the UK. The latter's policy reversal is strongly linked to this pressure, which manifested itself at various points in time between 2018 and 2020, as discussed below. Both unilateral and multilateral constraints

Table 2: Examples of coding decisions

Doc. date	Doc. name	Case	Excerpt	Theme assigned
17 December 2018	3012/2018-NUKIB-E/110 Warning	CZ	The legal and political environment of the People's Republic of China ('PRC') in which the companies primarily operate and whose laws are required to comply with, requires private companies to cooperate in meeting the interests of the PRC.	Sources of concern
15 May 2019	Executive Order on Securing the Information and Communications Technology and Services Supply Chain	US	The unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured or supplied by persons owned by, controlled by or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy and economy of the United States.	Sources of concern
28 November 2018	TICSA Factsheet	NZ	The telecommunications infrastructure is a highly attractive target for states seeking to engage in espionage, sabotage or foreign interference, or for criminal actors looking to exploit New Zealand businesses and individuals.	Security arguments
26 March 2019	A common EU approach to the security of 5G networks	EU	5G is a key asset for Europe 'to compete in the global market' and its cybersecurity is crucial 'for ensuring the strategic autonomy of the Union'.	Security arguments
23 August 2018	Government Provides 5G Security Guidance to Australian Carriers	AU	EU Member States have the right to exclude companies from their markets for national security reasons, if they do not comply with the country's standards and legal framework. Carriers may still need to apply controls regardless of the vendor they choose. These controls would not displace existing cyber security practices or business risk mitigations. Government is well positioned to address these risks in partnership with industry.	Regulatory approach
22 July 2019	UK Telecoms Supply Chain Review Report	UK	Based on experience from security testing and security incidents, the NCSC assesses that 'existing vendor agnostic security mitigations, as applied across the telecoms sector, are at best only moderately effective'.	Regulatory approach

thus appear to have played an important role in shaping the direction of policy for 5G infrastructure. The EU, on the other hand, as a grouping that does not have competence in national security, encouraged member states to consider 'technical risks and risks linked to the behaviour of suppliers or operators, including those from third countries' [79], recommending national assessments. Leaving the final choice to national authorities, the EU proposed a market-based policy toolbox built on risk assessment, influencing decision-making at the member-state level.

Since the technical and political rationales are closely interlinked in the debates we analysed, they were examined together. Our analysis looked at how the identification of 5G risks or threats translates into regulatory approaches in different national contexts and across two multilateral groupings, comparing similarities and differences. Based on the two dominant modes of governance explored in the theoretical discussion, the analysis revealed the ways in which the national positioning is linked to path dependency or risk-based approaches, summarized in Table 3 below.

Security focus: risks vs threats

In the 5G rollout, the identification of areas of insecurity appears to be a precondition to regulatory action, justifying the imposition of special measures or the adoption of a laissez-faire, market-driven

Table 3: Key elements of path-dependent and risk-based governance approaches in 5G debates

	Path dependency	Risk-based governance
Grouping	FVEY	EU
Security focus	Insurmountable threats	Controllable risks
Regulatory stance	Pre-emptive bans	National controls

approach. A risk-based strategy to 5G network security comprises both technical and non-technical elements, whereas a path dependency trajectory builds on previous efforts to classify Chinese vendors as high-risk or exclude them from an internal market even in the absence of new evidence of danger.

Our analysis shows that the identification of sources of concern in the 5G debates is tied to a strong ideological and geopolitical rationale, without concrete references to tangible evidence of vulnerabilities or security breaches. Politicians often emphasized strategic concerns related to the incorporation of Chinese components in new wireless infrastructure, but that also transpired in the official warnings released by specialized agencies, such as National Cyber and Information Security Agency (NUKIB) in the Czech Republic or the National Cyber Security Centre (NCSC) in the UK.

Such concerns ranged from legal requirements forcing Huawei to collaborate with the Chinese authorities to informal connections between corporate leadership and the Communist Party. In 2018, the NUBIK noted that the personal links between the two tech giants (Huawei and ZTE) and the Chinese state raised ‘concerns that the interests of the People’s Republic of China may be prioritised over the interests of the users of these companies’ technologies’ [80]. The NCSC guidance on ‘high-risk vendors’ lists Huawei as the only provider for which it ‘currently has in place a bespoke risk mitigation strategy’ [81], making explicit reference to China’s national intelligence law and the history of state-backed cyberattacks against the UK.

Many of the expert reports informing the debates focused primarily on classifying dangers, not quantifying their chances of occurring. As Rothstein, Borraz and Huber note for the German case, the public hearings created to better evaluate the probabilities of potential dangers often proved infertile because the participants placed more emphasis on identifying the risks than evaluating their likelihood and gravity [36]. Notably, the instrumental use of evidence to support security arguments, frequently deployed in highly politicized discussions [37, 82], does not appear as a dominant strategy in framing 5G arguments. Members of the German Parliamentary commission on the 5G security issues echoed concerns about the opacity of the companies’ leadership structures [83], although the German government explained that it would not comment on national matters of other states [84]. In this highly politicized space, the framing of risks and threats is key to understanding the type of pressure exerted in the FVEY and EU groupings.

Risks

In our thematic analysis, EU members tended to refer more frequently to *risk* sources, whereas FVEY states tended to prioritize *threats* in their discourse. But many of the FVEY countries had historically designated high-risk providers and that differentiator continued to apply to Huawei. The majority of the risks identified in the EU were directly linked to Chinese-origin technology, but reflections on the full breadth of political concerns were not uncommon. ‘They don’t want to undermine our relationship with NATO, or the EU, unlike the Russians. What they are really keen on is to squeeze as much technological information from us as possible’ [85], said a former chief of the Czech military-intelligence service with regard to suspicions of surveillance embedded in Chinese-built wireless infrastructure. The chief’s assessment revealed the mounting fears of many Western governments: Chinese technology could come with built-in backdoors and ways for Chinese state authorities to spy on governments, businesses and private citizens alike. The Czech NUKIB went as far as issuing a warning to the government noting risks of Chinese-origin technology that could result in service disruption and illicit information gathering [80]. By the same token, the NCSC provided a detailed security analysis to the government in July 2019, identifying ‘concerning issues in Huawei’s approach to software development bringing significantly increased risk to UK operators’ [86].

Among the risks presented by public officials in relation to 5G Chinese components, general information gaps and incomplete control over quality standards were often voiced. German politicians and intelligence experts also stressed a high level of uncertainty rising from knowledge gaps. According to them, the fast pace of 5G technology development could lead to an imbalance in levels of expertise. Technicians of the public sector who are tasked with testing the foreign technology might struggle to keep up-to-date with the

ever-growing number of software loopholes⁷ or have insufficient information to assess the network updates [87, 88]. These points also resonated with French experts who underlined the scale of network-related risks. First, the anticipated use of 5G for new domains, with countless applications in future IoT, smart and connected devices, would dramatically increase the scale of any potential harm emanating from faulty networks [89]. Second, 5G would allow operators to compartmentalize their provision of connectivity in order to offer different levels of service to their customers by creating different network layers.⁸ Unlike in previous generations, the ‘network slicing’ would be operated by software.

The complex infrastructure was perceived to enhance existing risks of (un-) intended backdoors and security vulnerabilities, which would be made easier to hide inside the sub-networks. These could, in turn, be exploited by states and malicious actors [90]. In Germany, where the assessment of risks was overseen by the Federal Institute of Risk Assessment (BfR) and traditionally bolstered with theme-specific public hearings [36], parliamentarians also mentioned risks related to disruptions, limited network availability and potential ‘kill switches’ that could be used to turn off parts of the wireless connectivity grid [84, 91]. But EU member states stressed that awareness and controls could mitigate these risks and keep them in check.

On a strategic level, the discussion around securing the infrastructure in the EU emphasized the need for adequate measures, standards and market options to adopt a multiple trusted vendors approach. The belief in controllable risks prompted French President Macron to allow Chinese providers to operate in the market, while announcing stricter controls over national telecommunication infrastructures in May 2019.

Threats

The emphasis on threats brought about by Chinese-origin 5G infrastructure was dominant among the members of the FVEY, combining rationales that overlap along alliance and geographical lines. The framing of threats correlated closely with foreign state control. Explicit fears pointed to the Chinese legal environment and personal ties between Chinese corporate officials and the Communist Party of China, while more implicit concerns reflected the growing influence of China in the global ICT market. The fear of espionage took greater proportions in 2019, following repeated warnings by American officials against incorporating Chinese-origin components into national networks. In many instances, the United States also pursued diplomatic means to reach out to allies, threatening to reduce or suspend intelligence collaboration with NATO allies who relied on Chinese 5G suppliers [92–94]. This strong stance was also reiterated by the President’s National Security Telecommunications Advisory Committee, which concluded that ‘the cybersecurity threat now poses an existential threat to the future of the [n]ation’ [95]. The committee was composed of telecommunications industry representatives and briefed the President on concerns surrounding 5G and ICT supply chain in November 2019, aligning itself with previous US positions.

The long-standing allegations of collusion between Huawei and the Communist Party of China surfacing in the 5G discussions dated back to 2012, when the ‘Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies

7 Unlike previous generations of wireless network, 5G antennae will require regular software updates.

8 For example, autonomous cars could be operated on a sub-network with lower latency than a smartphone operating on another sub-network.

Huawei and ZTE' was published. The recommendation has then been to avoid including the above-mentioned providers in US infrastructure [96]. Just like the formal sharing of information with the Chinese authorities, the informal exchanges continued to be regarded with suspicion by Western officials in the context of next generation networks. Notably, the past of Huawei's president and founder, Ren Zhengfei, has been the source of suspicion. US intelligence community and politicians have cast doubts over Huawei's origin as a five-person start-up company turned market leader. This and a number of other allegations regarding the company's lack of independence from the Chinese government led the US government to assess that Huawei is a company created by the Chinese government [96]. Similarly to the United States, a report in the UK pointed to uncertainties regarding the role of Huawei's president and founder, a former engineer in China's army and member of the Communist Party since 1978 [97].

Australia's decision to exclude Huawei and ZTE from infrastructure bids also follows the 'insurmountable threat' logic. In the '5G Security Guidance to Domestic Carriers' issued in August 2018, the possibility to circumvent 'traditional security controls by exploiting equipment in the edge of the network—exploitation which may affect overall network integrity and availability, as well as the confidentiality of customer data' represents the main threat, in particular as the 'government has found no combination of technical security controls that sufficiently mitigate the risks' [68]. Concerns related to unauthorized access and interference operated via hardware vulnerabilities was also exposed in the UK, revealing that the threat is imminent:

'The number and severity of vulnerabilities discovered, along with architectural and build issues, by the relatively small team in HC-SEC is a particular concern. If an attacker has knowledge of these vulnerabilities and sufficient access to exploit them, they may be able to affect the operation of the network, in some cases causing it to cease operating correctly. Other impacts could include being able to access user traffic or reconfiguration of the network elements' [86].

In New Zealand, medium and long-term consequences on trade relations with China surfaced following the banning of a local contract for 5G equipment involving Huawei. Noting solely that 'a significant network security risk was identified' [98], the Government Communications Security Bureau (GCSB) Director-General Andrew Hampton remained elliptic about the reasons behind banning the partnership between a local provider (Spark) and Huawei. Without specifying the risk discovered, the GCSB pointed to the telecom infrastructure as a 'highly attractive target for states seeking to engage in espionage, sabotage, or foreign interference, or for criminal actors looking to exploit New Zealand businesses and individuals' [99].

In the FVEY states included in the analysis, security experts and politicians often cited threats emanating from China's extensive control of technology and of its corporations, through its legal environment [86, 100, 101] and privileged relationships with corporate leadership. Most grievances were directly connected with Article 7 of the Amendment to the National Intelligence Law of the People's Republic of China of 27 June 2017, which makes it an obligation for an organization or citizen to support, assist and cooperate with national intelligence when required and keep that work confidential. The language used by US President Trump in his May 2019 order also pointed out that 'the unrestricted acquisition or use [of such technology] was augmenting 'the ability of foreign adversaries to create and exploit vulnerabilities' in US infrastructure. As such, that constituted an 'unusual and extraordinary threat to the national security, for-

eign policy, and economy of the United States' [3]. Outside of the FVEY grouping, there has been more hesitation to exclude Huawei and ZTE from national markets for a variety of reasons, including fears of economic retaliation. As French Senator Procaccia explained, ~30% of the European telecommunications sector was made up of Chinese investments [100].

Emerging regulatory approaches

While the aim of building national resilience is clearly present in all national strategies, the distinct policy options emerging in the early days indicate that a balancing act was necessary for aligning technical and non-technical rationales. Apart from a laissez-faire approach adopted in countries that have traditionally been allied with China, 5G regulation talks in the West mainly focused on two policy options: (i) excluding high-risk vendors from the core or from the entirety of the network; (ii) adopting a vendor-agnostic approach based on further checks and verifications, as well as certifications. The countries that have issued bans provided only summary reasoning for their decisions in terms of the threats identified, accompanying the measures with high-level political statements generally directed at the Chinese. In the FVEY alliance, path dependency had clearly shaped the policy approach adopted. In the '5G common approach' issued on 26 March 2019, the EU made it clear that the potential exclusion of companies from national markets remains a member state competency, should it be warranted by national security concerns. For a harmonized way forward, it recommended national risks assessments as a first step towards building a coordinated EU assessment and EU-wide certification framework for 5G networks and equipment. It also recommended the use of existing EU-wide rules, embedded in the telecommunication regulations, the Directive on Security of Network and Information Systems and the Cybersecurity Act, alongside a new certification scheme for 5G networks. The combination of new and old legislative and policy instruments to tackle 5G insecurity and to ensure the 'strategic autonomy of the Union' [102] proposed by the EU was grounded in risk governance approaches. The level of national controls to be imposed had subsequently been arduously discussed in Germany, France and the United Kingdom.

Pre-emptive bans—complete or partial

The three countries (Australia, New Zealand and the United States) that have issued total or partial bans against foreign 5G equipment providers have justified their decision on national security grounds, but did so employing distinct methods and instruments. Whereas the United States focused on both government procurement and mobile operator partnerships in building and operating the 5G networks of their countries, Australia and New Zealand addressed the carriers only, designing new guidance for telecom operators and implicitly restricting certain vendors from building the 5G infrastructure. As our findings show, the national normative culture also plays out in whether the limitations imposed are Huawei specific or vendor agnostic, whereas the form of regulation imposed is path dependent.

The case of the United States is particularly telling, as the implementation of a ban against Huawei took several pieces of legislation from various parts of the government. Every adopted step became a trigger for another action. The Department of Commerce added Huawei to the Entity List in May 2019 citing the company's violation of US sanctions against Iran, in order to 'prevent American technology from being used by foreign owned entities in ways that potentially undermine US national security or foreign policy interests' [103]. Further sanctions against the Chinese hardware giant

were later applied in May 2020, restricting its ability to use American technology for the design or manufacturing of its semiconductors abroad. At the other end of the spectrum, New Zealand has not opted for an outright ban of Huawei from its 5G networks, suggesting that contracts with the Chinese might be possible in the future [104]. The UK trajectory represents an exception, as its approach to high-risk vendors changed in the first part of 2020, when it pledged to exclude Huawei gear from its 5G networks, as discussed in detail below.

Pre-emptive bans are not new in the infrastructure space: like the United States, Australia has previously excluded Huawei from building its fibre-optic network. For the 5G rollout, the Australian government took the lead on limiting ‘high-risk’ providers from taking part in its next-generation infrastructure auctions. In August 2018, it issued new security guidance to vendors and telecommunications companies building the 5G networks in the country. On that occasion, the joint statement by Treasurer Scott Morrison and Communications Minister Mitch Fifield suggesting that such a ban was justified by an undisclosed ‘high security risk’ [68]. New Zealand invoked the same rationale in blocking Spark’s Huawei 5G plan in what can be considered a ‘partial ban’ targeted at the Chinese giant. Importantly, the Australian guidance was the first to recognize that regulation needed to evolve together with the technology and specific regulatory interventions may be required later.

Among the countries that have issued bans on foreign providers, New Zealand stood out because the veto-ing of the Chinese partnership was done directly by the intelligence services under the Telecommunications Interception Capability and Security Act. In November 2018, the Spark–Huawei bid for the first 5G deployment was rejected by the GCSB based on the identification of a ‘significant network security risk’ in the plans put forward. Domestic legislation passed in 2014 obliged telecom companies to inform security services of significant changes to their networks.

As revealed by the present analysis, deciding whether to limit Chinese-origin 5G vendors represented first and foremost a political process with multiple pressure points. Whether vendor-agnostic approaches or targeted measures against Chinese manufacturers were preferred, both strategies resulted in open conflicts with China and threats of economic retaliation. In Australia, the move to disqualify any company that was ‘likely subject to extrajudicial directions from a foreign government that conflict with Australian law’ [105], was, however, contested by the Chinese at the World Trade Organization as a ‘discriminatory market access prohibition on 5G equipment’ [106]. Among FVEY alliance members, economic seemed to count less than the desire to eliminate the source of danger entirely at the national level and as a block. The decision to follow in the footprints of previous policy approaches also weighted in for evaluating the risk of endangering the signal intelligence sharing, with significant military and (national) security repercussions. The path dependency approach was thus aligned with a realist, ‘hard power’ understanding of geopolitics, which ultimately shaped a set of national 5G strategies.

National controls

The second set of countries debating Huawei’s participation in the 5G rollout—many of them part of the EU, such as the Czech Republic, France and Germany—mandated public inquiries and leaned towards adopting a vendor-agnostic risk management approach. The French report, for example, opened by indicating that France and Europe should not let themselves get drawn into a trade war that did not concern them, especially considering that nearly 30% of the Chinese providers’ revenue is generated in Europe [100]. Ger-

many’s push for increasing minimum security standards for 5G components for all operators was accompanied by a budgetary increase for and a strengthening of its cybersecurity agencies. Remaining undecided on the position of Huawei in the country, the Czech Republic hosted an international meeting with like-minded EU and NATO members resulting in the Prague Proposals and signed a joint declaration with the United States on 5G security [107, 108]. Internally, it established a permanent parliamentary committee to investigate hybrid threats and assess systemic risks, working in close cooperation with academia and non-profits.

In line with the assertion of Krieger and Rothstein *et al.* that there is no uniformity in risk-based governance, alternatives to banning 5G infrastructure providers emerged amid long political negotiations at the domestic level [35, 36]. At the time of writing, no European state had excluded foreign infrastructure providers from building next-generation networks, with the exception of the UK, which reversed its initial decision to allow Huawei to control up to 30% of the market. Another case, that of the Czech Republic, shows that disagreements over the handling of Chinese providers may lead to policy oscillation. As early as December 2018, the intelligence services raised concerns about Huawei’s participation in the 5G rollout, leading to announcements by the Ministries of Health and Justice of bans on public sector contracts with the company [109]. But the Czech Minister of Industry countered this ban, concluding that it was ‘not acceptable from the business point of view, and communication point of view, to in advance reduce the group of potential investors, potential suppliers’ [110], a view shared by the country’s President⁹. Nonetheless, an advisory body issued recommendations to exclude Chinese and Russian suppliers following NUBIK’s warning. In reaction to the findings of the cybersecurity agency, the Czech Prime Minister ordered his office to refrain from using Huawei equipment. Moreover, the report led to a national investigation of technology used by the ministry and caused Huawei and ZTE to be excluded from a national tender, later cancelled. The Czech Ministry of Defence also ordered its employees to delete all sensitive information from Huawei phones and to refrain from using them [85]. Diplomatic discussions on 5G gear with both China and the United States followed.

The European Commission clarified, in the ‘5G common approach’ issued on 26 March 2019, that member states have the right to exclude companies from their markets, should this be warranted by national security concerns. As a harmonized way forward, it recommended national risks assessments as a first step towards building a coordinated EU assessment and EU-wide certification framework for 5G networks and equipment. Overall, the EU proposed a combination of new and old legislative and policy instruments to tackle 5G insecurity and to ensure the ‘strategic autonomy of the Union’ [102], in line with risk governance approaches. It recommends the use of existing EU-wide rules, embedded in the telecom regulation, the Directive on Security of Network and Information Systems and the Cybersecurity Act, alongside a new certification scheme for 5G networks. Similar initiatives have been discussed in Germany, France and the United Kingdom. The latter’s Huawei Cyber Security Evaluation Centre Oversight Board concluded, in its 2019 report, that it could ‘only provide limited assurance’ in terms of the long-term mitigation strategy for UK’s critical networks [86] and NSCS guidance in January 2020 indicated that a market cap for Huawei’s involvement was necessary.

9 Observers of Czech politics note that the 5G debate further reflected the country’s divide on whether to adopt a more pro-Western or pro-Eastern approach [111]. This led to contradicting statements made by various bodies of the government.

In Germany, as well, diverging opinions emerged: the German Federal Office for Security in Information Technology (BSI) granted Huawei the benefit of the doubt, while the Ministry of Foreign Affairs and the German Intelligence Services did not [112, 113]. While the BSI argued that it had not been provided with concluding evidence that would warrant the isolation and exclusion of certain providers as an adequate security mechanism [112], it had started rewording its provisions regarding the trustworthiness of components in critical infrastructure [114]. Arne Schönbohm, president of the BSI, framed the planned measures as a ‘preventive approach’ according to which all operators will have to be certified by the organization [115]. The modified version will likely entail that (i) critical core components can only be acquired from trusted producers (requirement will apply to all manufacturers/producers of the value chain) and that proof of trustworthiness will have to be provided to the BSI, and (ii) ‘no-spy agreements’ will have to be signed by all suppliers, including those within the value chain [116].

Despite public statements that the German government would not pre-emptively exclude telecommunication providers and suppliers, stricter rules for the operation and supply of network parts are also being introduced by other state agencies. On 7 March 2019, the Federal Network Agency (‘Bundesnetzagentur’) published additional security requirements for the operation of telecommunication networks [117, 118]. In parallel, the German government was working on updating the provisions of the German telecommunications law in order to force telecommunication operators to abide by the newly established security catalogue [114] and include a certification requirement from network providers to get permission to establish infrastructure.

After the French government saw its rushed attempt at including an amendment for protective measures for its networks into the PACTE bill¹⁰ rejected in February 2019, it introduced another bill in April 2019, often referred to as ‘Loi Huawei’ (‘the Huawei law’). After a careful examination by senators and parliamentarians in the mixed commission of economic affairs¹¹, the legal text was adopted on 23 July 2019, allowing France to become the first European country to adopt legislation for the protection of its networks against 5G-related risks. Like in Germany, the French law foresees that telecommunication operators will have to file for authorization for the use of certain equipment in their network. The decision of authorization will lie with the Prime minister, who has two months to pronounce himself on the matter. Given that not all telecommunication providers operate critical infrastructure, the decisions would be taken on a case-by-case basis. The legal text will only apply to 5G and future technologies and not to prior technologies. The stricter controls are intended for any equipment from foreign providers, not only from non-European ones [100]. Importantly, this risk mitigation strategy against network sabotage addresses the mobile operator’s processes and requires thorough network planning.

In some cases, national checks are exercised through additional harmonized mechanisms, such as the provisions of the EU Directive

on Security of Network and Information Systems (NIS), the Cybersecurity Act or the screening frameworks for foreign direct investments (FDI). The NIS Directive applies indirectly to 5G equipment vendors, requiring operators of essential services to take appropriate security measures and imposing an obligation to notify competent national authorities about serious incidents. The 2019 Cybersecurity Act provides a framework for cybersecurity certification at the EU level, which applies to new wireless technologies as well. The ENISA Toolbox developed for mitigating the main 5G cybersecurity risks includes measures such as strengthening the role and power of regulatory authorities, applying restrictions for high-risk suppliers or ensuring that operators adopt an appropriate multi-vendor strategy to avoid strict reliance on a single supplier.

In this analysis, we observed that several European member states adopted risk-based governance approaches. The initial absence of direct responses to the allegations of insecure Huawei technology from individual member states and the wait for the Prague Conference to develop a coordinated and united stance is not only proof of increasing political integration of the Union. It is also reflective of the fact that, in the evaluation of risks, states tend to align and look for common solutions when faced with unprecedented situations and high levels of uncertainty. The EU had also discussed, since 2017, a regulatory proposal for screening FDI into the Union. Adopted on 19 March 2019, this regulation gave member states competences in this area on grounds of security or public order, in particular for FDI in critical infrastructure and key enabling technologies. With it also came a cooperation mechanism for exchanging information between member states and the Commission to consider the FDI context and circumstances, ‘in particular whether a foreign investor is controlled directly or indirectly, for example through significant funding, including subsidies, by the government of a third country or is pursuing State-led outward projects or programmes’. Certain forms of insecurity related to large Chinese investments could be addressed via such screening mechanisms.

Policy reversal: the case of the UK

The 5G regulatory paths emerging since 2018 in the seven countries analysed have not been linear. Many states, including supranational bodies such as the EU, have tightened their policies regarding Chinese infrastructure technology in the second half of 2019 and the beginning of 2020. Yet the case of the UK stands out, as it originally followed a risk-based approach in line with other EU countries, but switched towards a full ban of Huawei in 2020. In early January, the NCSC issued guidance on the use of equipment from high-risk vendors in UK telecoms network, leading to a government decision to exclude them from core and sensitive parts of the 5G network and to restrict their market share to a maximum of 35%. In July 2020, the NCSC guidance was updated in light of the US sanctions, resulting in a complete ban of all purchase of Huawei 5G equipment as of January 2021.

A member state of the EU and of the FVEY intelligence sharing alliance at the time, the UK deserves a separate discussion here to understand the change in its stance on 5G over the course of two years. Being the only country in the world with a dedicated expertise centre for Huawei-related risks, the UK was among the first nations to recognize that the large market share of the Chinese giant in its 4G infrastructure requires close monitoring. The Huawei Cyber Security Evaluation Centre (HCSEC) identified major quality and security issues in the equipment manufactured by the Chinese giant in both 2018 and 2019, leading the Board to assess that it could provide only ‘limited assurance’ for the mitigation of critical risks. In

10 The Plan d’Action Pour La Croissance et la Transformation des Entreprises (PACTE) is an economic stimulus package for the growth and (digital) transformation of businesses. The amendment aimed at strengthening its cybersecurity agency and protecting its infrastructures from foreign technology providers. The argument was rejected by the Senate that argued that the matter was too important to be waived through and demanded an in-depth debate on the subject.

11 Nonetheless, the commission criticized the French government for transforming a rejected amendment into a law without making it a bill proposal first. This step would have allowed Parliament to request an impact study as well as the State Council’s opinion.

parallel, the UK Telecom Supply Chain Review completed in July 2019 revealed that faults and vulnerabilities in network equipment represented only one of the four areas of major concern. The other three included: dependence on a single (high-risk) vendor, ‘backdoor’ threats and vendor administrative access to equipment support.

The HCSEC Oversight Board deplored the lax supervision of the Chinese supply chain and the lower quality of Huawei engineering and software configuration in a 2018 report [97]. In 2019, they noted that ‘no material progress’ had been made by Huawei to fix the technical issues previously identified and pointed out new ones. Classifying the above-mentioned risks as ‘moderate’, the UK initially adopted verification methods to allow national authorities to intervene in case of security breaches or suspected espionage acts carried out through 5G infrastructure. The following year, however, the evaluation of risks was reconsidered and they were deemed unmanageable by the National Cyber Security Centre, following a new set of US sanctions imposed on Huawei in May 2020.

Whereas the immediate decision had been to ban Huawei from the sensitive ‘core’ parts of the network and cap the market share of Huawei at 30% on the edge network, the revised assessment from July 2020 led the government to opt for a full exclusion of its equipment from 5G networks. The final decision was justified by pointing to additional risks linked to the design and production of semiconductors outside of the United States, ‘making it impossible to continue to guarantee the security of Huawei equipment in the future’ [67]. With this U-turn, the UK government aligned more closely with the policies adopted by other FVEY countries and mandated the complete removal of any Huawei existing equipment from its networks by 2027.

Complementing our analysis of path dependency and risk-based governance in two multilateral groupings, the UK represented a special case of a country with membership in both the EU and the FVEY alliance at the time. It pursued a long process of oscillation between the two governance approaches discussed here, before settling on a Huawei ban. The final policy decision reflected both internal and external pressures to sideline Huawei and minimize dependencies on Chinese providers, in response to strong political pressure exerted by the US administration and specific changes in the US sanctions regime. While the gradual distancing between the British government and the European counterparts in the Brexit negotiations might have played a role, peer pressure and FVEY priorities alignment appear to be a stronger explanation for this policy reversal.

Conclusion

From the threat of an immediate disruption to the fear of building long-term vulnerability into national networks, 5G debates reveal a continuous tension around the balancing of interests at the technical, economic and political levels. Our analysis, based on themes and topics present in the public discourse between mid-2018 and mid-2019, shows that the plethora of concerns expressed in relation to 5G security has important regulatory underpinnings. The operation of Huawei in the local markets has been the epicentre of tensions in both the EU and among FVEY member states. Whether Chinese manufacturers of 5G gear were perceived as a controllable risk or an insurmountable threat in the public discourse made a difference for the policy options that countries leaned towards.

The first countries to discuss 5G rollout were all technologically advanced and relatively important markets for the next generation of wireless equipment. Yet some had defaulted to long-standing policy stances in relation to the access of Chinese providers to key in-

frastructure, while others opted to evaluate the new risks posed by companies such as Huawei and ZTE and design new approaches. In the FVEY grouping, regulatory approaches have generally followed the pre-emptive bans adopted in relation to previous wireless generations, generally showing path-dependent trajectories. As a consequence, full or partial bans were imposed on Huawei in the United States, Australia, New Zealand and the UK by mid-2020. The existential threat posed by Chinese-origin components to both national networks and to cross-national efforts to share intelligence within the alliance emerged as a dominant theme in the public discourse.

Conversely, members of the EU preferred, during the early stage of the 5G discussions, to combine various policy instruments as part of their risk-based approaches. France, Germany and the Czech Republic have opted for applying further checks, verifications, as well as authorizations and certifications on foreign providers, in order to prioritize resilience without compromising market competition. These policies were based on the assessment that risks emanating from Chinese vendors, although serious, remained controllable through appropriate policy and technical measures. The rich discussions that weighed the pros and cons of mitigating the risks associated with Chinese-origin equipment also showed the growing importance assigned to strategic autonomy and cyber sovereignty. France adopted a national law aimed at protecting its telecommunication infrastructure, equipping its Minister of Economy and Finances with the power to vet specific operators. In turn, Germany planned changes to its telecommunication law and other contingent legal statutes to introduce certification schemes for critical infrastructure suppliers. The United Kingdom initially relied on verification methods that allowed national authorities to intervene in case of security breaches or suspected espionage acts carried out through 5G infrastructure, later deciding for an outright exclusion of Huawei from its networks. The EU itself had proposed working towards an EU-wide risk assessment and certification scheme.

The nascent regulatory approaches in the 5G debates offer valuable contribution to current theories of security governance, which do not fully capture the extent of policymaking coordination. As a first step in understanding the (in)security of new-generation wireless networks, the public discourse and governmental inquiries from 2018 to 2020 present the full breadth of risk and threats in relation to Chinese vendors. Yet the focus on Huawei has eluded other key conversations about cyber accountability in the 5G infrastructure bids and meaningful security differentiators for domestic industry and suppliers. As new policy instruments emerge, more research is needed to examine the extent to which the risk and the threat narratives cross sectoral boundaries and influence the implementation of 5G.

Funding

The work of Roxana Radu was supported by the Swiss National Science Foundation under grant P2GEP1_178007.

Conflict of interest statement. None declared.

References

1. Herman A. The war for the world's 5G future. *Forbes* 2018.
2. Obiodu E, Giles M. *The 5G Era: Age of Boundless Connectivity and Intelligent Automation*. London: GSMA Intelligence, 2018, 1–42.
3. The White House. Executive order on securing the information and communications technology and services supply chain. *White House* 2019.

4. Hoffmann S, Bradshaw S, Taylor E. Networks and geopolitics: how great power rivalries infected 5G. Oxford Information Labs 2019.
5. Radu R. The monopoly of violence in the cyber space: challenges of cyber security. In: Fels E, Kremer J-F, Kronenberg K (eds). *Power in the 21st Century: International Security and International Political Economy in a Changing World*. New York: Springer, 2012, 137–50.
6. Radu R. Power technology and powerful technologies: global governmentality and security in the cyberspace. In: Kremer J-F, Müller B (eds). *Cyberspace and International Relations: Theory, Prospects and Challenges*. Berlin: Springer, 2014, 3–20.
7. Mueller M. Is cybersecurity eating internet governance? causes and consequences of alternative framings. *Digit Policy Regul Gov* 2017;19:415–28.
8. Cavelti MD. *The Militarisation of Cyberspace: Why Less May Be Better*. Tallinn: NATO CCD COE Publications, 2012, 1–13.
9. Gouvernement.fr. Tech for good summit: digital stakeholders make concrete commitments for the common good. 2018. <https://www.gouvernement.fr/en/tech-for-good-summit-digital-stakeholders-make-concrete-commitments-for-the-common-good>. July 27, 2021.
10. Stoltenberg J. Remarks by NATO secretary general Jens Stoltenberg at the Cyber Defence Pledge Conference, London. NATO 2019.
11. Guterres A. UN Secretary General address at the opening ceremony of the Munich Security Conference. 2018. <https://www.un.org/sg/en/content/sg/statement/2018-02-16/secretary-general%E2%80%99s-address-opening-ceremony-munich-security>. July 30, 2021.
12. Li Y, Taeiagh A, De Jong M. The governance of risks in ridesharing: a revelatory case from singapore. *Energies* 2018;11:1277.
13. Bell S. Do we really need a new ‘constructivist institutionalism’ to explain institutional change? *Br J Pol Sci* 2011;41:883–906.
14. Lowndes V, Roberts M. *Why Institutions Matter the New Institutionalism in Political Science*. Basingstoke: Palgrave Macmillan, 2013.
15. David PA. Path dependence: a foundational concept for historical social science. *Cliometrica J Hist Econ Econom Hist* 2007;1:91–114.
16. Pierson P. *Politics in Time: History, Institutions, and Social Analysis*. Princeton: Princeton University Press, 2004.
17. Pierson P. Increasing returns, path dependence, and the study of politics. *Am Pol Sci Rev* 2000;94:251–67.
18. North DC. *Institutions, Institutional Change and Economic Performance*. Cambridge, NY: Cambridge University Press, 1990.
19. Ostrom E. *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge, NY: Cambridge University Press, 1990.
20. North DC. Institutions. *J Econ Perspect* 1991;5:97–112.
21. Hacker JS. *The Divided Welfare State: The Battle over Public and Private Social Benefits in the United States*. 1st ed. New York: Cambridge University Press, 2002.
22. Karl TL. *The Paradox of Plenty: Oil Booms and Petro-States*. University of California Press, 1997.
23. Bednar J, Page S. *A Model of Institutional Path Dependence*. Washington, D.C., 2005.
24. ENISA. *Threat Landscape for 5G Networks: Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G)*. ENISA, 2019, 87.
25. Hussain SR, Echeverria M, Chowdhury O. et al. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. *Proceedings 2019 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society, 2019.
26. Borgaonkar R, Hirschi L, Park S. et al. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. *Proc Priv Enhanc Technol* 2019;2019:108–27.
27. Newman LH. 5G Is More Secure Than 4G and 3G—Except When It’s Not. *Wired*. <https://www.wired.com/story/5g-more-secure-4g-except-when-not/>. July 30, 2021.
28. Chirgwin R. Huawei banned from Australia’s NBN: reports. *The Register* 2012.
29. Muncaster P. US bill prohibits state use of tech linked to Chinese government. *The Register* 2013.
30. Sanderson I. Evaluation, policy learning and evidence-based policy making. *Public Administration* 2002;80:1–22.
31. Hood C, Rothstein H, Baldwin R. *The Government of Risk: Understanding Risk Regulation Regimes*. Oxford, United Kingdom: Oxford University Press, 2004.
32. PwC. *Technology Companies: In the Sweet Spot for Risk Resiliency and Agility*. PwC report, 2016.
33. Murphy S. What is the linkage between risk management and resilience? BCI 2018.
34. DTCC. *Resilience First: Promoting Financial Stability by Planning for Disruption*. DTCC white paper. 2019.
35. Krieger K. The limits and variety of risk-based governance: the case of flood management in Germany and England: institutions and risk-based governance. *Regul Gov* 2013;7:236–57.
36. Rothstein H, Borraz O, Huber M. Risk and the limits of governance: exploring varied patterns of risk-based governance across Europe: risk and the limits of governance. *Regul Gov* 2012;7:215–35.
37. Hawkins B, Parkhurst J. The “good governance” of evidence in health policy. *Evid Policy* 2016;12:575–92.
38. Bromberg L, Godwin A, Ramsay I. Fintech sandboxes: achieving a balance between regulation and innovation. *J Bank Financ Law Pract* 2017;28:314–36.
39. Truby J. Fintech and the city: sandbox 2.0 policy and regulatory reform proposals. *Int Rev Law Comput Technol* 2018;34:1–33.
40. Black J, Baldwin R. Really responsive risk-based regulation. *Law Policy* 2010;32:181–213.
41. Karaboytcheva M. *Effects of 5G Wireless Communication on Human Health*. European Parliamentary Research Service (EPRS), 2020, 11.
42. World Health Organization. Radiation: 5G mobile networks and health. 2020. <https://www.who.int/news-room/q-a-detail/radiation-5g-mobile-networks-and-health>. July 27, 2021.
43. Finley K. Worried about 5G’s health effects? Don’t be. *Wired* 2019.
44. Seaman J. *China and the New Geopolitics of Technical Standardization*. Paris, France: Ifri, 2020, 34.
45. Triolo P, Allison K. *Eurasia Group White Paper: The Geopolitics of 5G*. Eurasia Group report, 2018.
46. Radu R. Steering the governance of artificial intelligence: national strategies in perspective. *Policy Soc* 2021;40:1–16.
47. Deibert R, Palfrey J, Rohozinski R. et al. (eds). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 2010.
48. Mueller M. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press, 2010.
49. DeNardis L. *The Global War for Internet Governance*. New Haven: Yale University Press, 2014.
50. Radu R. *Negotiating Internet Governance*. Oxford, UK: Oxford University Press, 2019.
51. Mueller M. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press, 2002.
52. Henriksen A. The end of the road for the UN GGE process: the future regulation of cyberspace. *J Cybersec* 2019;5, DOI: 10.1093/cyb-sect/y009.
53. Boustany A, Solanky D. OpenRAN. *Telecom Infra Project*. <https://telecominfrastructure.com/openran/>. July 30, 2021.
54. Duesterberg TJ. 5G: China’s dream to dominate world technology. *The Japan Times*, 22 December 2017.
55. Medin M, Louie G. *The 5G Ecosystem: Risks & Opportunities for DoD*. Defense Innovation Board, 2019.
56. Tugendhat T, Gallagher M. China’s dominance of 5G is a threat. *The Times*, 19 April 2019.
57. Duesterberg T. The multitier battle against chinese 5G dominance. *Forbes* 1 July 2020.
58. Strategy Analytics. Strategy analytics: infrastructure giants lead 5G standardization. 2020. <https://news.strategyanalytics.com/press-release/press-release-details/2020/Strategy-Analytics-Infrastructure-Giants-Lead-5G-Standardization/default.aspx>. July 27, 2021.
59. IPlytics. *Who Is Leading the 5G Patent Race? A Patent Landscape Analysis on Declared SEPs and Standards Contributions*.

2019. https://www.iplytics.com/wp-content/uploads/2019/01/Who-Leads-the-5G-Patent-Race_2019.pdf. July 30, 2021.
60. Ip A. *Huawei May Have Largest 5G Patent Portfolio – Starting to Flex IPR Muscle*. <https://wccftech.com/huawei-has-largest-5g-patent-portfolio-starting-to-flex-ipr-muscle/>. July 30, 2021.
61. Broeders D, Adamson L, Creemers R. *A Coalition of the Unwilling? Chinese and Russian Perspectives on Cyberspace*. The Hague: The Hague Program for Cyber Norms, 2019.
62. Kim M, Lee H, Kwak J. The changing patterns of China's international standardization in ICT under techno-nationalism: a reflection through 5G standardization. *Int J Inf Manage* 2020;54:102145.
63. Edwards B. *Insecurity and Biotechnology: Governing Misuse Potential*. Cham: Palgrave Macmillan, 2019.
64. Christensen KK, Petersen KL. Public-private partnerships on cyber security: a practice of loyalty. *Int Aff* 2017;93:1435–52.
65. Klinken A, Renn O. A new approach to risk evaluation and management: risk-based, precaution-based, and discourse-based strategies. *Risk Anal* 2002;22:1071–94.
66. OECD. *Emerging Systemic Risks in the 21st Century: An Agenda for Action*. Paris: OECD, 2003, 291.
67. Levy I. Security, complexity and Huawei; protecting the UK's telecoms networks. *Natl Cyber Secur Cent* 2019.
68. Fifield M, Scott M. Government provides 5G security guidance to Australian carriers. *Parliam Aust* 2018.
69. Secretary of State for Digital, Culture, Media and Sport. UK Telecoms Supply Chain Review Report, 2019.
70. NIS Cooperation Group. *EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks*. European Commission, 2019.
71. Hartman L. *Get smart: Core vs. edge in 5G networks [infographic]*. ShareAmerica. 2019.
72. Gilding S. 5G choices: a pivotal moment in world affairs. *ASPI* 2020.
73. Guest G, MacQueen K, Namey E. *Applied Thematic Analysis*. Thousand Oaks, CA: SAGE Publications, Inc., 2012.
74. Braun V, Clarke V. Using thematic analysis in psychology. *Qual Res Psychol* 2006;3:77–101.
75. Clarke V, Braun V. Teaching thematic analysis: over-coming challenges and developing strategies for effective learning. *The Psychologist* 2013;26:120–3.
76. Boyatzis RE. *Transforming Qualitative Information: Thematic Analysis and Code Development*. Thousand Oaks, CA: Sage Publications, 1998.
77. Georgieva I. The unexpected norm-setters: intelligence agencies in cyberspace. *Contemp Secur Policy* 2020;41:33–54.
78. Shires J. Hack-and-leak operations: intrusion and influence in the Gulf. *J Cyber Policy* 2019;4:235–56.
79. European Commission. European Commission recommends common EU approach to the security of 5G networks. 2019. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_19_1833. July 27, 2021.
80. National Cyber and Information Security Agency. *Warning*. Brno: National Cyber and Information Security Agency, 2018.
81. National Cyber Security Centre. NCSC advice on the use of equipment from high risk vendors in UK telecoms networks. *Natl Cyber Secur Cent* 2020.
82. Oliver K, Lorenc T, Innvær S. New directions in evidence-based policy research: a critical analysis of the literature. *Health Res Policy Syst* 2014;12:34.
83. “heute im bundestag” (hib). Sicherheitsbedenken beim 5G-Ausbau. *Deutscher Bundestag*. <https://www.bundestag.de/presse/hib/628670-628670>. July 4, 2019.
84. Bundesministeriums des Innern, für Bau und Heimat (BMI). *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Matthias Büttner, Andreas Mrosek und der Fraktion der AfD – Drucksache 19/4419 – Nationale Sicherheit und digitale Infrastruktur*. Deutscher Bundestag, 2018, 1–8.
85. Heijmans P. The U.S.–China tech war is being fought in central Europe. *The Atlantic* 5 March 2019.
86. Cabinet Office, National security and intelligence. Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report, 2019, 1–46.
87. Benner T. Vertrauen in Huawei ist riskant. *Der Tagesspiegel*. <https://www.tagesspiegel.de/politik/5g-mobilfunk-vertrauen-in-huawei-ist-riskant/23731840.html>. May 4, 2020.
88. FOCUS. Ex-BND-Chef Schindler warnt vor Risiken bei Netzausbau mit Huawei. *FOCUS Online*. https://www.focus.de/finanzen/boerse/wirtschaft/aftsticker/unternehmen-ex-bnd-chef-schindler-warnt-vor-riesen-bei-netzausbau-mit-huawei_id_10315636.html. August 9, 2019.
89. Cuvelliez C, Quisqater J-J. L'Europe, la sécurité et la 5G : regardons au-delà du problème « chinois ». *La Tribune*. <https://www.latribune.fr/opinions/tribunes/l-europe-la-securite-et-la-5g-regardons-au-dela-du-probleme-chinois-831379.html>. October 23, 2019.
90. Poireault K. Pourquoi la 5G est aussi une rupture en matière de cyber-risques? *Industrie & Technologies*. <https://www.industrie-techno.com/article/pourquoi-la-5g-est-aussi-une-rupture-en-matiere-de-cyber-risques.57554>. July 27, 2021.
91. Schulz U, Cotar J, Ependiller M. et al. *Antrag der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Ependiller, Dr. Götz Frömming, Marc Bernhard, Stephan Brandner, Jürgen Braun, Marcus Bühl, Matthias Büttner, Tino Chrupalla, Peter Felser, Dietmar Friedhoff, Wilhelm von Gottberg, Armin-Paulus Hampel, Verena Hartmann, Martin Hebner, Lars Herrmann, Martin Hess, Karsten Hilde, Nicole-Höchst, Martin Hohmann, Dr. Marc Jongen, Jens Kestner, Jörn König, Dr. Rainer Kraft, Andreas Mrosek, Christoph Neumann, Ulrich Oehme, Gerold Otten, Dr. Robby Schlund, Thomas Seitz, Detlev Spangenberg, Dr. Dirk Spaniel, Beatrix von Storch, Dr. Harald Weyel, Dr. Christian Wirth und der Fraktion der AfD – Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausrüstern*. Deutscher Bundestag, 2019, 1–4.
92. Esper MT. Remarks by Secretary Esper at an International Institute for Strategic Studies webinar. *US Embassy and Consulates in China*. 2020.
93. Wintour P. US Defence Secretary warns Huawei 5G will put alliances at risk. *The Guardian* 2020.
94. Jee C. The US threatens to stop sharing intelligence with allies if they use Huawei. *MIT Technol Rev* 2020.
95. Wheeler T. If 5G is so important, why isn't it secure? *The New York Times*. 21 January 2019. <https://www.nytimes.com/2019/01/21/opinion/5g-cybersecurity-china.html>.
96. Rogers M, Ruppersberger CAD. *Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. U.S. House of Representatives, 2012, 60.
97. Cabinet Office, National Security and Intelligence. Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2018, 2018, 1–33.
98. Greenfield C. New Zealand rejects Huawei's first 5G bid citing national security risk. *Reuters* 2018.
99. Jolly J. New Zealand blocks Huawei imports over 'significant security risk.' *The Guardian*. <https://www.theguardian.com/business/2018/nov/28/new-zealand-blocks-huawei-5g-equipment-on-security-concerns> (4 May 2020, date last accessed).
100. Procaccia C. *Rapport No. 579 (2018-2019) Fait Au Nom de La Commission Des Affaires Économiques (1) Sur La Proposition de Loi, Adoptée Par l'Assemblée Nationale Après Engagement de La Procédure Accélérée, Visant à Préserver Les Intérêts de La Défense et de La Sécurité Nationale de La France Dans Le Cadre de l'exploitation Des Réseaux Radioélectriques Mobiles*. Sénat, 2019, 114.
101. “heute im bundestag” (hib). 5G-Vergabe beschäftigt Ausschuss. *Deutscher Bundestag*. <https://www.bundestag.de/presse/hib/628608-628608>. July 4, 2019.
102. European Commission. A common EU approach to the security of 5G networks. 2019. http://europa.eu/rapid/press-release_IP-19-1832_en.html. July 30, 2020.
103. U.S. Department of Commerce. Department of commerce announces the addition of Huawei Technologies Co. Ltd. to the entity list. 2019. <https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list>. July 30, 2021.

104. Fitzgerald K. Huawei "never were not" allowed to run 5G network: Jacinda Ardern. *Newshub*. <https://www.newshub.co.nz/home/politics/2019/02/huawei-never-were-not-allowed-to-run-5g-network-jacinda-ardern.html> (5 September 2020, date last accessed).
105. Slezak M, Bogle A. Huawei banned from 5G mobile infrastructure rollout in Australia. *ABC News*. <https://www.abc.net.au/news/2018-08-23/huawei-banned-from-providing-5g-mobile-technology-australia/10155438> (4 May 2020, date last accessed).
106. Needham K, Hunter F. China takes Australia's Huawei 5G ban to global trade umpire. *The Sydney Morning Herald*. <https://www.smh.com.au/world/asia/china-takes-australia-s-huawei-5g-ban-to-global-trade-umpire-20190413-p51dwu.html> (4 May 2020, date last accessed).
107. The Prague proposals: the Chairman Statement on cyber security of communication networks in a globally digitalized world. 2019. <https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/>. July 30, 2021.
108. U.S. Department of State. Joint statement on United States–Czech Republic joint declaration on 5G security. 2020. <https://cz.usembassy.gov/joint-statement-on-united-states-czech-republic-joint-declaration-on-5g-security/>. July 30, 2021.
109. Santora M, de Goeij H. Huawei was a czech favorite. Now? It's a national security threat. *The New York Times*. <https://www.nytimes.com/2019/02/12/world/europe/czech-republic-huawei.html> (3 September 2020, date last accessed).
110. Hovet J. New Czech minister sees no one ruled out of 5G, nuclear power expansion. *Reuters*. <https://www.reuters.com/article/czech-minister-havlicek-idUSL5N22C2WJ>. July 9, 2019.
111. Brokes F. Huawei hoopla: 'business as usual' after Czech 5G Warning. *Balkan Insight*. <https://balkaninsight.com/2019/11/01/huawei-hoopla-business-as-usual-after-czech-5g-warning/>. August 22, 2020.
112. Bundesministeriums des Innern, für Bau und Heimat (BMI). *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Matthias Büttner, Dr. Dirk Spaniel, Wolfgang Wiehle, weiterer Abgeordneter und der Fraktion der AfD – Drucksache 19/8593 – Sicherheitsüberprüfung von Netzelementen durch das Bundesamt für Sicherheit in der Informationstechnik*. Deutscher Bundestag, 2019, 1–8.
113. Bundesministeriums des Innern, für Bau und Heimat (BMI). *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD – Drucksache 19/8650 – Sicherstellung der technischen Integrität der künftigen 5G-Mobilfunkinfrastruktur*. Deutscher Bundestag, 2019, 1–8.
114. Feicht A. *Antwort auf - Schriftliche Frage an die Bundesregierung im Monat März 2019, Fragen Nr. 170*. Bundesministerium für Wirtschaft und Energie (BMWi), 2019, 2.
115. Benner T. 5G-Netz: Kontrolle ist besser. *Die Zeit*. <https://www.zeit.de/politik/ausland/2018-12/5g-netz-mobilfunk-huawei-deutschland-china-telekom-sicherheit/komplettansicht>. August 2, 2019.
116. Bundesministerium für Wirtschaft und Energie. *Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Reinhard Houben, Michael Theurer, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 19/8226 – Verwendung von Huawei-Technologie in deutschen Mobilfunknetzen*. Deutscher Bundestag, 2019, 1–8.
117. Bundesnetzagentur. Bundesnetzagentur veröffentlicht Eckpunkte zusätzlicher Sicherheitsanforderungen für Telekommunikationsnetze. 2019. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2019/20190307_ITsicherheitskatalog.html. July 30, 2021.
118. Bundesnetzagentur. Bundesnetzagentur aktualisiert den Katalog von Sicherheitsanforderungen. *Bundesnetzagentur* 2019. https://www.bundesnetzagentur.de/EN/Areas/Telecommunications/Companies/ServiceProviderObligation/PublicSafety/Catalogue/Catalogue_node.html. July 30, 2021.

Annexure 1: Documents included in the analysis (listed in alphabetical order)

- Australian Government, Department of Communications and the Arts. 2017. "5G—Enabling the Future Economy." Strategy paper. Canberra: Australian Government. <https://www.communications.gov.au/documents/5g-enabling-future-economy>.
- Bundesministerium für Wirtschaft und Energie. 2019. "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Reinhard Houben, Michael Theurer, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP—Drucksache 19/8226—Verwendung von Huawei-Technologie in deutschen Mobilfunknetzen." Parliamentary Inquiry Drucksache 19/9194. Deutscher Bundestag.
- Bundesministeriums des Innern, für Bau und Heimat (BMI). 2018. "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Matthias Büttner, Andreas Mrosek und der Fraktion der AfD—Drucksache 19/4419—Nationale Sicherheit und digitale Infrastruktur." Antwort der Bundesregierung Drucksache 19/4804. Deutscher Bundestag.
- . 2019a. "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Matthias Büttner, Dr. Dirk Spaniel, Wolfgang Wiehle, weiterer Abgeordneter und der Fraktion der AfD—Drucksache 19/8593—Sicherheitsüberprüfung von Netzelementen durch das Bundesamt für Sicherheit in der Informationstechnik." Parliamentary Inquiry Drucksache 19/9041. Deutscher Bundestag.
- . 2019b. "Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD—Drucksache 19/8650—Sicherstellung der technischen Integrität der künftigen 5G-Mobilfunkinfrastruktur." Parliamentary Inquiry Drucksache 19/9621. Deutscher Bundestag.
- Bundesnetzagentur. 2016. "Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz (TKG)." Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen.
- . 2019a. "Bundesnetzagentur aktualisiert den Katalog von Sicherheitsanforderungen." Public consultation. Bundesnetzagentur. 2019. https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/aktualisierung_sicherheitsanforderungen/aktualisierung_sicherheitsanforderungen-node.html.
- . 2019b. "Bundesnetzagentur veröffentlicht Eckpunkte zusätzlicher Sicherheitsanforderungen für Telekommunikationsnetze." Press release. Bundesnetzagentur. 7. März 2019. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2019/20190307_ITsicherheitskatalog.html.
- . 2019c. "Konsultation zum Katalog der Sicherheitsanforderungen gemäß § 109 Abs. 6 TKG." Press release. Bundesnetzagentur. 15. Oktober 2019. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilung/DE/2019/20191014_ITsicherheitsk.html.
- Cabinet Office, and National security and intelligence. 2018. "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2018." Corporate report. <https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2018>.
- . 2019. "Huawei Cyber Security Evaluation Centre Oversight Board: Annual Report 2019." Corporate report. <https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019>.
- Commission Mixte Paritaire. 2019. Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.
- Culture, Media and Sport Department for Digital. 2019. "UK Telecoms Supply Chain Review Report." CP 158. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

- European Commission. 2019a. "Commission Recommendation: Cybersecurity of 5G networks." Press release. European Commission. 26 March. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1832.
- . 2019b. "European Commission recommends common EU approach to the security of 5G networks." 26 March. http://europa.eu/rapid/press-release_IP-19-1832_en.htm.
- . 2019c. "A Common EU Approach to the Security of 5G Networks." Press release. European Commission. 26 March. https://ec.europa.eu/commission/news/common-eu-approach-security-5g-networks-2019-mar-26_en.
- Feicht, Andreas. 2019. "Antwort auf—Schriftliche Frage an die Bundesregierung im Monat März 2019, Fragen Nr. 170." Parliamentary Inquiry Fragen Nr. 170. Bundesministerium für Wirtschaft und Energie (BMWi).
- Fifield, Mitch, und Morrison Scott. 2018. "Government Provides 5G Security Guidance to Australian Carriers." Press release. Parliament of Australia. 23. August 2018. https://parlinfo.aph.gov.au/parlInfo/download/media/pressrel/6164495/upload_binary/6164495.pdf;fileType=application%2Fpdf#search=%22media/pressrel/6164495%22.
- Gallagher, Jill C, und Michael E DeVine. 2019. "Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress." Congressional Research Service.
- Gény-Stephann, Delphine, und Mounir Mahjoubi. 2018. "5G—Une feuille de route ambitieuse pour la France." Ministère de l'Economie et des Finances.
- Government Communications Security Bureau. 2018a. "GCSB statement." Official Website. Government Communications Security Bureau. 28 November. <https://www.gcsb.govt.nz/news/gcsb-statement/>.
- . 2018b. "TICSA Factsheet." Factsheet. Government Communications Security Bureau. <https://www.gcsb.govt.nz/assets/Uploads/TICSA-Factsheet2.pdf>.
- Huawei. 2019. "Czech President Welcomes Huawei's Participation in 5G Deployment." Huawei News. 27 April. <https://www.huawei.com/en/press-events/news/2019/4/czech-president-huawei-participation-5g>.
- Kaska, Kadri, Henrik Beckvard, und Tomáš Minárik. 2019. "Huawei, 5G and China as a Security Threat." NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE, 26 March.
- Le Gendre, Gilles, Éric Bothorel, Christine Hennion, und Paula Forteza. 2019. Proposition de loi visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles.
- Medin, Milo and Gilman Louie. 2019. "The 5G Ecosystem: Risks & Opportunities for DoD." DIB 5G Study. Defense Innovation Board. https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.
- National Cyber and Information Security Agency. 2018. "Warning." 110–536/2018. Brno: National Cyber and Information Security Agency.
- National Cyber Security Centre. 2020. "NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks." Guidance. National Cyber Security Centre. 28 January. <https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks>.
- NIS Cooperation Group. 2019. "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks." European Commission. <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>.
- Pirie, Andrew. 2018. "GCSB Declines Spark's Proposal to Use Huawei 5G Equipment." Official Website. Spark NZ. 28 November. https://www.sparknz.co.nz/news/GCSB_declines_Spark_proposal_Huawei/.
- Procaccia, Catherine. 2019. "Rapport no. 579 (2018–2019) fait au nom de la commission des affaires économiques (1) sur la proposition de loi, adoptée par l'Assemblée Nationale après engagement de la procédure accélérée, visant à préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles." 579. Sénat.
- Schulz, Uwe, Joana Cotar, Michael Ependiller, Götz Frömming, und Marc Bernhard. 2019. "Antrag der Abgeordneten Uwe Schulz, Joana Cotar, Dr Michael Ependiller, Dr Götz Frömming, Marc Bernhard, Stephan Brandner, Jürgen Braun, Marcus Bühl, Matthias Büttner, Tino Chrupalla, Peter Felser, Dietmar Friedhoff, Wilhelm von Gottberg, Armin-Paulus Hampel, Verena Hartmann, Martin Hebner, Lars Herrmann, Martin Hess, Karsten Hilse, Nicole Höchst, Martin Hohmann, Dr Marc Jongen, Jens Kestner, Jörn König, Dr Rainer Kraft, Andreas Mrosek, Christoph Neumann, Ulrich Oehme, Gerold Otten, Dr Robby Schlund, Thomas Seitz, Detlev Spangenberg, Dr Dirk Spaniel, Beatrix von Storch, Dr Harald Weyel, Dr Christian Wirth und der Fraktion der AfD—Schutz der Kritischen 5G-Infrastruktur vor staatsnahen Netzwerkausüstern." Draft proposal. Deutscher Bundestag.
- Standing Committee of the National People's Congress. 2018. "National Intelligence Law of the People's Republic of China (2018 Amendment)." 27 April. <http://en.pkulaw.cn/display.aspx?cgid=313975&lib=law>.
- "The Prague Proposals—The Chairman Statement on cyber security of communication networks in a globally digitalized world." 2019. https://www.vlada.cz/assets/media-centrum/aktualne/PRG_proposals_SP_1.pdf.
- The White House. 2019. "Executive Order on Securing the Information and Communications Technology and Services Supply Chain." 15 May. <https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/>.
- U.S. Congress. 2017. "National Defense Authorization Act For Fiscal Year 2018—Conference Report to Accompany H.R. 2810." 115–404. U.S. Congress. <https://www.congress.gov/115/crpt/hrpt404/CRPT-115hrpt404.pdf>.
- U.S. Department of Commerce. 2020. "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies." Press release. U.S. Department of Commerce. 15. Mai 2020. <https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts>.