Development and Change
Published on behalf of the Institute of Social Studies, The Hague

Huawei, 5G and Security: Technological Limitations and Political Responses

Karsten Friis and Olav Lysne

ABSTRACT

How did Chinese 5G providers, such as Huawei, become a security concern in the USA and Europe? Were the security concerns related to 5G and Chinese suppliers based upon technological features of the systems, or were they a product of geopolitical rivalry? How did European approaches to 5G distinguish themselves from those of the USA? This article addresses these questions using an interdisciplinary approach via the framework of securitization theory. The authors argue that the technological features of 5G made securitization more likely compared to 4G, and that screening and control of software was unlikely to defuse securitization concerns. They also show how Europe chose its own path for the securitization of 5G. In short, the article argues that the American macrosecuritization of China largely failed in Europe, whereas the niche securitization of 5G was more successful.

INTRODUCTION

Until a few years ago, security in mobile telecoms networks was primarily a technical issue. It was about standards and procedures designed to maintain operational functionality and avoid disruptions. Furthermore, while cybersecurity and state-sponsored hacking have become growing concerns for Western governments over the last few decades, the focus was primarily on traditional information and communications technology (ICT) systems and not on mobile telecoms. This was initially due to the limited capacity of the mobile networks to carry data, but the cybersecurity discourse largely continued to neglect mobile telecoms even when the fourth generation (4G) broadband networks were rolled out about a decade ago. Even though these 4G networks in many ways resembled other ICT networks, security remained a question of technical functionality.

The authors would like to thank the guest editors of this special issue, Nana de Graaff and Jeff Henderson, for their invitation, advice and suggestions. We would also like to thank the journal editors, and in particular the four peer reviewers, for their excellent comments and suggestions. In addition, we would like to thank Erik Kursetgjerde for his valuable research assistance.

Development and Change 52(5): 1174–1195. DOI: 10.1111/dech.12680

This changed dramatically as Western states begun preparing for the fifth generation (5G) networks. The United States embarked upon a global campaign to prevent Chinese suppliers — and in particular the company Huawei — from delivering 5G infrastructure. The American claim was that Chinese equipment would represent a national security hazard for those depending upon it — not because of its technical functionality and stability, but because it allegedly could be a gateway for Chinese espionage and sabotage of Western critical infrastructure. In other words, 5G and Chinese suppliers were securitized. The topic was elevated from the realm of ordinary politics and treated as an emergency, thus legitimizing extraordinary countermeasures (Buzan et al., 1998).

How did this happen? In this article we will explore this question and ask if the securitization of Chinese 5G suppliers was simply a subset of the US's broader securitization of China, or if there was something particular about 5G that distinguished it from previous generations of cellular networks. Further, we will ask if the ban on Chinese companies such as Huawei was an appropriate remedy. Could the securitization of 5G have been isolated from the broader securitization of China and Chinese suppliers? Finally, we will ask how the US's European allies and partners responded to this securitizing move. Did European states follow the American approach, and if not, how did they differ?

The article is an interdisciplinary attempt to address both political and technical aspects of the securitization of 5G. We use securitization theory to help frame the empirical analysis, but also engage with the interplay between the material and social dimensions in securitization theory. We argue that the material nature of 5G technology made securitization more likely, but we also demonstrate that Europe, to a large extent, chose a somewhat different approach to the US. By limiting securitization to the 5G technology ('niche securitization'), rather than applying it to China as a whole ('macrosecuritization'), European states achieved enhanced 5G security without confronting China more broadly.

SECURITIZATION

Securitization theory is about the social construction of a threat and the response to it. The theory emerged in the 1990s as a reaction to and rejection of rationalist notions in the then dominant theories in International Relations of dangers and risks as objective givens (Buzan et al., 1998). Instead, securitization theory emphasizes the political processes that make something a security issue. The theory has since evolved in many directions, but the key idea is that 'an issue is given sufficient saliency to win the assent of the audience, which enables those who are authorized to handle the issue to use whatever means they deem most appropriate. In other words,

securitization combines the politics of threat design with that of threat management' (Balzacq et al., 2016: 495).

The theory comprises a securitizing actor (e.g. an individual or a state), securitizing moves (e.g. speeches and practices), an audience (e.g. a society or a parliament), and a referent object (that which is being securitized, e.g. terrorism or migration). In this article, we use a simple model to enhance an empirical study of the row over 5G in the West. We define the United States as the securitizing actor that securitized 5G through speeches and diplomatic practices in an attempt to convince Europe (the audience) to follow suit.

Applying the theory to processes taking place *between* states rather than inside them has been labelled *macrosecuritization* by Buzan and Wæver (2009). This aspect of securitization theory has not been explored as broadly as many other facets of the theory. Buzan and Wæver's model is complex and multidimensional, including level of analysis (local to global), degree of comprehensiveness (from niche to inclusive), and degree of success in convincing the audience. Macrosecuritizations, they write, 'are necessarily launched as candidates for top-rank threats', such as 'geo-economics, terrorism, [and] nuclear proliferation' (ibid.: 258–59). Niche securitizations, on the other hand, 'get onto the agenda as accepted threats, but do not rise to top priority'; examples include 'environmental threats, epidemic diseases, organised crime, [and] drugs' (ibid.). Buzan and Wæver also point out that macrosecuritizations are more vulnerable to breakdown than mid- or micro-level securitizations, as the mid-level units (states) may pull out or reject the securitizing move. A reason for this could be that there are usually weaker relations between the securitizing actor and the audience on the macro/global level than in mid- or micro-level cases.

Inspired by Buzan and Wæver's model, we borrow some of its concepts for our empirical study, but do not apply it in its full complexity. In our case, the US government was not dependent upon European consent to implement restrictions on Chinese 5G suppliers on American soil. This was a domestic securitization process. The securitizing move we study, however, happened after the initial US securitization and was about convincing other states to undertake their own national securitizations of the 5G rollout. This was an American attempt at comprehensive macrosecuritization of China, with a niche securitization of 5G.

Another dimension of the theory that we engage with here is the material or technological dimension. As Buzan and Wæver (2009: 255) point out: 'In principle, securitizing actors can attempt to construct anything as a referent object. In practice, however, the constraints of facilitating conditions mean that they are much more likely to be successful with some types of referent object than with others'. In our case we argue that the features of 5G technology — its weaknesses and vulnerabilities as well as its expected role as a critical infrastructure in our societies — are important to understanding securitization processes. In other words, these processes were constrained and impacted by the material 'realities' of 5G technology. Understanding,

for instance, if the dangers pointed to by the securitizing actor (such as espionage) can be addressed or resolved through technological solutions, is crucial. Such understanding can help us navigate the political terrain and enhance our understanding of securitization processes. This does not mean that the technological specificities of 5G telecoms in any way *determine* political outcomes — but they do affect them. In short, if a simple technical solution could mitigate all the concerns raised by the securitizing actor, securitization would fail.

AMERICAN SECURITIZATION OF CHINESE TELECOMS

Voices calling for the securitization of Chinese telecommunications companies in the US can be traced back to at least 2010. At that time, the FBI, politicians and US experts repeatedly pointed out that Chinese companies could pose a security threat to the United States (Barboza, 2010). In 2012 Congress warned that the 'United States should view with suspicion the continued penetration of the US telecommunications market by Chinese telecommunications companies' (US House of Representatives, 2012: vi).

At the time, these warnings did not gain too much traction. The overall political mood when it came to Chine was one of inclusion. Since the 1990s, the US and the West had had a clear strategy to bring China (and others, such as Russia) into the existing world order. In practice, this meant that they were invited into existing regimes, such as the World Trade Organization, and that trade and dialogue were promoted with the hope that authoritarian regimes would open up and gradually democratize. This policy had been questioned and criticized for a while, but as the Trump administration took office in 2016, a distinct shift in both rhetoric and practices could be noted. Trump embarked upon a confrontational approach towards China in many areas, not least in trade, tariffs and industrial production, but also in security. The argument was that the strategy of inclusion and change had failed, and that China had abused American openness to subsidize its industry, manipulate currency, steal technology and position itself in global markets. Increasingly authoritarian political developments in China and growing pressure on neighbouring countries were also referred to by US government officials. The securitization of Chinese 5G must therefore be seen in this broader context of American securitization of China in general.

It was the Chinese telecoms company Huawei that became a particular target (referent object) of securitization in the US. As a world leader in 5G technology, and a provider of the 4G networks in many Western countries, Huawei was a strong candidate to secure many 5G contracts. However, the Trump administration took a robust stance against the company, citing the risks of espionage from China. They claimed that Huawei and other Chinese technology companies represented a serious threat to national security, as

their 5G systems could be misused for the purpose of espionage or even sabotage by China (Cartwright, 2020).

Questions were asked about its ownership structure and the influence the Chinese Communist Party had over Huawei (Hawes and Li, 2017; Rühlig, 2020). In particular, critics of Huawei referred to the 2017 Chinese Intelligence Law, which requires Chinese companies to turn over information to, and comply with, China's intelligence and security services (Rühlig and Björk, 2020: 9). As a result, in 2018 the US decided to ban the use of Huawei and ZTE, another Chinese telecommunications company, in the Armed Forces (US Congress, 2018). Furthermore, in May 2019 the US put Huawei on its 'Entities List', a list of companies not allowed to buy American products (Federal Register, 2019). This meant that Huawei could no longer use US-made chips and other components in its products.

In April 2020, the then Secretary of State, Mike Pompeo, announced that the United States would introduce a '5G Clean Path' system that would ensure that no correspondence from US embassies would go through Chinese networks or systems. This was later extended to the 'Clean Network', whose purpose was to 'secure national resources, including citizens' computer security and the company's most sensitive information from aggressive intrusions by malicious actors, such as the Chinese Communist Party' (US Department of State, 2020a). The Clean Network included 'Clean Apps', 'Clean Carrier', 'Clean Store', 'Clean Cable', 'Clean Cloud' and 'Clean Path'. The purpose was to exclude Chinese companies from app stores, remove American apps from Chinese app stores, and refrain from using Chinese networks, cloud services and cables.

At the same time that Huawei was securitized domestically, the Trump administration embarked upon a global campaign to make other countries follow suit. The language used by US officials was forthright, with no diplomatic filters. For instance, in 2020 the then Secretary of Defense, Mark Esper, stated that: 'If countries choose to go the Huawei route, it could well jeopardize all the information sharing and intelligence sharing we have been talking about, and that could undermine the alliance, or at least our relationship with that country' (quoted in Sanger and McCabe, 2020). In short, the securitization of Huawei consisted of rhetoric focused on risks and dangers, restrictive legislation and a global campaign, which we will return to below.

However, the campaign against Huawei was not restricted to telecoms security. The company was accused by US authorities of racketeering and theft of trade secrets. The conflict peaked in 2019 when Huawei and its chief financial officer, Meng Wanzhou, were indicted for fraud and sanctions evasion. The arrest of Meng Wanzhou in Canada and subsequent — seemingly retaliatory — arrests of Canadian citizens in China contributed to a strained political climate between China, the US and Canada (Blanchfield, 2020). However, none of this had anything to do with 5G security. According to

Sanger and McCabe (2020), 'The Huawei fight is just one part of a bigger US–China battle, as Washington tries to contain Beijing's influence and power and ensure that the world's second-largest economy does not come to dominate advanced industries that could give it an economic and military edge'. Furthermore, they hold, 'The United States is also trying to limit China's access to American technology more broadly and is considering restricting sales of microchips, artificial intelligence, robotics and some types of advanced software, along with preventing tech companies from teaming up — or even sharing research — with Chinese firms' (ibid.). Hence, the securitization of Huawei was about more than just 5G security; geopolitics and economic rivalry were also important factors (Inkster, 2019; Mascitelli and Chung, 2019). The securitization of 5G and Huawei was therefore part of a broader US policy of confronting and securitizing China across a spectrum of issues. It was part of a comprehensive and global macrosecuritization of China.

This broader American macrosecuritization of China raises some important questions: is the niche securitization of primarily Chinese 5G a subset of this? Were the 5G security concerns inflated or used as a fig leaf to cover for economic interests and geopolitical rivalry? Was, for instance, Mark Esper's concern that the 5G network may be exploited for espionage or sabotage exaggerated to cover for a political agenda? We cannot know the exact motivations for the US's 5G securitization. There were probably several overlapping agendas at play. However, we can get a better idea of the technical security risks associated with 5G, and thus at least be able to assess whether the securitization could be substantiated on technological grounds or not. In theoretical terms this means exploring the technical–material foundation on which the securitizing act is based, without arguing that securitization *had* to happen. It will, however, indicate the strength of the arguments that the securitizing actors relied on in the process.

ICT SECURITY AND 5G

Are there technical aspects in 5G technology that make it more likely or vulnerable to be misused for espionage and sabotage than previous generations of mobile telecoms networks? The backdrop to this discussion is that over the previous two decades all modern societies have transformed and moved their critical infrastructures onto a foundation consisting of digital systems. This movement has been driven by technological innovation, economic forces and a demand for improved services to society as a whole. In parallel with this development, new vulnerabilities emerged, which were debated and addressed as they became apparent. Vulnerabilities tied to the supply chain of digital services and equipment received little attention and were not subject to serious scientific studies until relatively recently (Boyson, 2014).

The movement of mobile phones onto a digital platform started with the Global System for Mobile Communication (GSM), that was rolled out in many countries from the early 1990s (Dunnewijk and Hultén, 2007). GSM replaced a first generation of cellular equipment that consisted of a plethora of different analogue technologies. The simple services of speech and messaging that this second generation allowed were enriched with a more comprehensive internet connection when 3G appeared in the early years of this millennium. While 4G could be seen as a relatively straightforward improvement on the third generation of mobile technology, 3G enabled a whole range of new applications. In sum, these applications have in a very short span of time changed most aspects of modern life, and the rollout of 3G can arguably be seen as the event that turned mobile phones and related infrastructures into indispensable elements of modern societies. The expectations around 5G are that it will bring about changes that are as important as those we saw for 3G. Speculations abound, but three application areas stand out as being both technically viable and having significant potential for disruption.

First, 5G is designed to be a single wireless communication technology that can cover the needs of all use cases. A common situation in any given country today is that there is one infrastructure for distribution of mobile telephony, one for distribution of radio channels, one for distribution of TV signals, one for public safety, and yet another to cover the needs of the armed forces. 5G is designed to be able to support the convergence of all these different networks with different properties into one infrastructure. This is done through a concept called 'network slicing' (Foukas et al., 2017). We can therefore see a future where all special purpose networks are replaced with a software-based 'network slice' in one 5G network.

Second, 5G is designed so that the limit on the number of connected devices is practically removed. This will prepare for a future where many, or even most, of our possessions have sensors in them and are connected to the internet (Xia et al., 2012). This phenomenon goes by the name 'internet of things' (IoT), and 5G is designed to be the communication technology that this phenomenon utilizes. Where the development of IoT will lead us is at this point hard to guess. Some applications, such as intelligent lightbulbs, ovens and loudspeakers are already here, but on the horizon we can see applications including intelligent roofs and insulation in buildings, and milk bottles that can tell how much milk is left, what temperature it is, how old it is, and, when it is empty, whether it has been recycled correctly.

The final standout application area is robotics and remote control. There are several improvements in 5G that support such functions. Enhanced security and robustness are factors, but the feature that really opens new doors is that the latency of communication is drastically reduced from 4G to 5G. This means that the time that passes from when a decision has been made in a

central server until this decision takes effect in a deployed robot somewhere will be measured in milliseconds rather than in tenths of seconds. This will allow for applications like automated traffic control with drastically higher utilization of roads and tracks, and with significantly fewer accidents and casualties than we have today.

In short, as the potential of 5G is realized over the next decade or so, 5G infrastructures will take on an importance that surpasses that of any digital infrastructure we have previously relied upon. Even if the application areas listed above only partly come to fruition, 5G networks will be the most critical infrastructures we have ever seen. This is why the material or technological nature of 5G incites a more urgent security debate than was necessary for 4G. While malicious actors could also exploit 4G networks for espionage, the implications of this risk appear to increase significantly with 5G, given its broader societal function. Furthermore, as 5G becomes a backbone for new functions — remote control, IoT and automated systems — the consequences of potential sabotage also increase.

The securitization of 5G did not *have* to happen. But as security experts began to realize the critical societal function 5G could have in the near future, and how it could be exploited by malicious actors, their arguments gained momentum. This, combined with the broader political macrosecuritization of China as one such malicious actor, made niche securitization of 5G more likely.

THE LIMITATIONS OF SCREENING

Even if the importance of 5G for societal and national security has increased compared to 4G, however, does that mean that a ban on Huawei was necessarily an appropriate remedy? In other words, could the securitization of 5G be isolated from the broader securitization of China and Chinese suppliers? Again, a study of the technological aspects can guide us. More concretely, we can ask if the security concerns pointed to above could be resolved through other means, such as screening and control of the software in 5G networks. If such technical screening was possible, it would be irrelevant who the suppliers of the equipment were. In that case, securitization of 5G would be likely to fail.

Trade of tools and equipment between societies that do not trust each other is historically commonplace. Even trade of military weaponry has taken place between untrusted parties, but such exchanges have always been accompanied by detailed inspections of the traded equipment. This inspection of equipment is key to understanding how such trade can take place. It transforms the need for trust between the trading parties to a need for the buyer to trust his/her own inspection of the traded goods. Clearly, if buyers of equipment for 5G networks could fully investigate the equipment, the same transformation would take place. Countries of the West would not

need to fully trust the Chinese companies that built the equipment. It would suffice for them to trust their own inspection of it.

This was the basis of the counterargument from the Chinese as the pressure from the US grew. Huawei put a lot of effort into demonstrating transparency in its systems and was open to investigations of its 5G equipment. In 2018, it announced the opening of an information security lab in Germany where operators and regulators could review the source code that went into Huawei equipment. A similar centre had already been operational in the United Kingdom since 2010. The centre in the UK is called the Huawei Cyber Security Evaluation Centre (HCSEC); it is owned and operated by Huawei, and it is controlled by an oversight board that reports to the UK's National Cyber Security Centre (NCSC).

In 2018, however, serious concerns arose regarding the feasibility of providing security through openness. The oversight board in the UK wrote the following in their annual report: 'Due to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated. We are advising the National Security Adviser on this basis' (HCSEC, 2018: 4). In short, what HCSEC concludes is that a full inspection of electronic equipment is not feasible. This conclusion is also supported by others (see, e.g., Lysne, 2018). It is a complex topic, but let us outline some of the properties that prevent comprehensive investigations of electronics systems.

The first element making inspection hard is the complexity of a computing system. Even though inspection of both software and hardware is done routinely in security companies, the slow speed of manual analysis mandates that only small fractions of a full code base are analysed. Morrison and colleagues estimated that a full analysis of the Windows code base would take between 35 and 350 mistake-free person-years, even if the source code was available to the reverse engineers (Morrison et al., 2015). This is made even more difficult by the fact that the operating system is only one of many parts of the entire system. In addition to the operating system, there is hardware consisting of multiple integrated circuits, some of which can have billions of logic gates. There will also be an application doing the actual work, for example, controlling distribution in a power grid. Finally, all the analysis must be finished in a relatively short time span. When a new version of software appears, the analysis of the software must start from the beginning again, and it should preferably be finished before the new version is installed in a critical system. This indicates that a full analysis of the code base of even a simple PC is practically impossible. This example does not represent a complete discussion of the topic at hand, because manual code analysis is only one of several methods for analysis of electronics. Nonetheless, it portrays the complexity that renders a complete analysis of electronic equipment impossible.

Software updates present a separate challenge to screening equipment (Sanger et al., 2021). While the hardware of a device is fixed throughout the lifetime of the product, the software will typically be replaced many times before the device is decommissioned. The reasons for such replacements, or software updates, are manifold. One common reason is that security holes have been detected and need to be corrected. Another frequent motivation is that one wants to equip the device with new functionality that was not present at the time of shipment. Not installing software updates provided by the manufacturer of the device is not a feasible option. Hence, it does not suffice to trust the vendor at the time of procurement of the equipment. A relation of trust in the vendor has to prevail throughout the lifetime of the product. The trust that Western countries need to have in Huawei in order to buy 5G equipment from them must therefore have a duration that lasts many years into the future.

One obvious approach to screening equipment would be to use machine-based techniques that have been developed to detect viruses, Trojans and worms that can infect a previously healthy system. Successes in this field constitute some of the finest stories in computer security. Yet, these methods fall short of solving the problem of screening a computer system for back doors deliberately placed there by the developers of the system themselves. The reason for this is that all of the successful methods in this area are based, explicitly or implicitly, on comparing a potentially infected system with a system that is known to be healthy (Egele et al., 2008). While this is an effective way to detect changes to a system inserted by a third-party wrongdoer, it will have no effect when looking for malicious code that is inserted by the system developer. If the malicious code is in the product itself, there will be no healthy system with which to compare it.

While detection of malicious code inserted by the makers of the product is close to impossible, it is sometimes possible to detect the malicious actions as they take place. Discovering when equipment is being exploited to conduct espionage, for instance, consists of detecting information leaking out in an irregular manner. A full discussion of this topic is beyond the scope of this article, but there are many ways by which information can leak. Our ability to detect irregular information leaks depends greatly on their extent; in general, higher bandwidth of leakage makes it easier to detect the leak. Unfortunately, it is possible to leak information in ways that have proven to be undetectable (Che et al., 2014). These methods provide low capacity, which means that the information leak is limited to a rather slow rate, but nonetheless, from an espionage standpoint, a lot of damage can be done even at a very low bandwidth.

Sabotage is usually a lot easier to detect. On the other hand, it will already be too late once the damage has occurred. In some cases, sabotage is intended to be detected as part of a deterrence strategy, or as an extortion strategy. Sabotage can also be used to undermine competitiveness through

means which, from the outside, are seemingly 'technical issues'. Such sabotage will have the same weakness with regard to detection as espionage; that at a larger scale it becomes easier to detect. Still, there is every reason to assume that a resourceful adversary would be able to balance sabotage in such a way that detectability is controlled.

In short, therefore, the technical nature of ICT and 5G systems makes investigating such equipment at the time of purchase futile. Stopping malicious functionality from entering through software updates appears to be impossible, and we should be careful not to assume that exploitation of undesired functionality in our 5G equipment will always be detected.

The securitization of Huawei in 5G by the United States could therefore draw on and refer to technical expertise. Huawei's attempt to rebuke the securitization by offering exceptional transparency and inspection of their systems was insufficient to address all concerns. As previously mentioned, this conclusion does not mean that the US could not have additional motives for excluding Huawei from American systems — but it does demonstrate that the security concerns expressed at the political level were in line with the concerns expressed by technical expertise. Despite this, the US's effort to make Europe securitize Huawei in the same way was not straightforward. While European states were under pressure from both Washington and Beijing, it seems they chose a somewhat different approach, which we will turn to next.

THE SECURITIZATION OF 5G IN EUROPE

Initially, most European states were relatively open and positive and had good experiences with the 3G and 4G networks provided by Huawei. The European Commission drafted an 'Action Plan' for 5G in 2016, but safety and security were not really evaluated in the document. Instead, the emphasis was on the strategic opportunity 5G represented, and the need for Europe to be prepared for 5G (European Commission, 2016). However, a gradual securitization of 5G did take place in many European states, with warnings coming from security officials, intelligence services and technical experts. As a result, the European Union (EU) also became part of the securitization discourse. In 2019 the European Parliament wrote a report on 'Security Threats Connected with the Rising Chinese Technological Presence in the EU' (European Parliament, 2019). As we see from the title, in this document it was China more broadly that was securitized, with 5G being one factor. However, on the same day, the European Commission presented a document entitled 'EU–China: A Strategic Outlook' in which China was described as 'simultaneously, in different policy areas, a cooperation partner', 'a negotiating partner', 'an economic competitor', and 'a systemic rival' (European Commission, 2019a: 1). In other words, while recognizing the differences between China and the EU in values and governance, the EU was simultaneously seeking a more balanced (i.e. less securitized) approach to China

than the US. Later that year, the European Commission for the first time recommended that member states take concrete steps to assess the cybersecurity risks of 5G networks and strengthen risk mitigation measures (European Commission, 2019b). However, here the focus was limited to 5G; China was not mentioned.

At the same time, the Trump administration initiated a broad international campaign to securitize Huawei and Chinese telecoms technology in general (Reuters, 2019). The aim was to make other countries ban Huawei and other Chinese suppliers from their 5G and other ICT networks. The language was firm. For instance, during a trip to Italy in 2020, then Secretary of State Mike Pompeo called Huawei's investments 'predatory actions'. Furthermore: 'Their investments are not private because they are subsidized by the (Chinese) State. Hence they are not transparent, free, commercial transactions like many others but they are rather carried out to the exclusive benefit of (China's) security apparatus' (Reuters, 2020a).

In addition to diplomatic tools, the aforementioned Clean Network initiative was elevated by the State Department to an international collaboration network, with a number of countries, telecoms companies and suppliers throughout the world listed as participants. In this context, in 2019 and 2020 the US State Department initiated a series of 'Joint Declarations on 5G Security' with allies in Eastern and Central Europe. All NATO countries in this part of Europe, except Hungary, signed such agreements (*LRT English*, 2020; Republic of Slovenia, 2020; Reuters, 2020b; *Romania Insider*, 2020; US Department of State, 2020b, 2020c, 2020d; US Embassy in Estonia, 2019; White House, 2019). Furthermore, in the western Balkans, North Macedonia signed a similar declaration, Kosovo signed a Memorandum of Understanding, and in 2020 Albania stated its intention to join the Clean Network initiative (Taylor, 2020; US Department of State, 2020e, 2020f). Serbia also made a number of pledges related to 5G (Ruge and Vladisavlej, 2020). Many of these countries are also members of China's Belt and Road Initiative. The fact that no Western European states were asked to sign similar joint declarations makes one suspect there is an element of geopolitical rivalry at play, for influence in presumably less consolidated democracies. For instance, in May 2021 a bipartisan bill was introduced in the US Congress to help fund 5G infrastructure in Eastern Europe, 'to develop international 5G standards that favor democratic institutions, not further authoritarianism spread by China', as the bill's sponsors Marcy Kaptur and Adam Kinzinger put it (RFE/RL, 2021). The language in the US thus remained explicitly anti-Chinese, while the joint declarations with the Europeans did not refer to Huawei or China. In other words, the Europeans seem to have avoided a macrosecuritization of China, while joining the US in the niche securitization of 5G. Hence, in the joint statements generic terms were used, such as commitment to 'exclude high-risk vendors' from the construction of 5G networks.

The Prague Proposals

Such a differentiated approach to China was in line with the 'EU–China: A Strategic Outlook' document (European Commission, 2019a), but also with an approach developed explicitly in relation to 5G, which first emerged at a conference in Prague in May 2019. The purpose of this conference was to arrive at a set of recommendations on how to introduce 5G networks securely. In addition to European states, the US, Israel, Australia, New Zealand, Japan and South Korea participated, with 32 countries in total. The resulting document, The Prague Proposals (2019), lists 20 principles the countries should adhere to when rolling out their 5G networks. It states that: 'Every country is free, in accordance with international law, to set its own national security and law enforcement requirements, which should respect privacy and adhere to laws protecting information from improper collection and misuse' (ibid.: 3). But it then adds:

> The overall risk of influence on a supplier by a third country should be taken into account, notably in relation to its model of governance, the absence of cooperation agreements on security, or similar arrangements, such as adequacy decisions, as regards data protection, or whether this country is a party to multilateral, international or bilateral agreements on cybersecurity, the fight against cybercrime, or data protection. (ibid.)

As we can see, neither China nor Huawei are mentioned, but the references to 'model of governance' and absence of security cooperation appear to point to non-democratic and non-Western countries, such as China. This attempt to decouple the 5G debate from the broader American macrosecuritization of China was probably welcomed by European states who were uneasy about aspects of the global rivalry between the US and China. The fact that the United States and most Western countries agreed on the Prague proposals contributed to discussions that resulted in concrete security solutions. Questions about the US's 'real' motivation, trade policies and global rivalry could be left aside. Hence, by focusing on the technical challenges and principles, solutions could be found that were less likely to be securitized. Still, the 20 principles needed to be operationalized further.

The EU 5G Toolbox

In October 2019, the EU published a report assessing cybersecurity risks in 5G networks (NIS Cooperation Group, 2019). It stated that state actors represent the most significant threat and that several EU members had identified 'certain non-EU countries' as a particular threat to their national interests. Thus, China is not mentioned in words but, quite clearly, this can be read between the lines. Furthermore, the report emphasized diversification — in that one should not become dependent on only one supplier — to be

resistant to errors and disturbances. Then, in January 2020, the European Commission published a so-called 'toolbox', the purpose of which was to identify some common measures that could reduce the most severe digital threats to 5G networks (NIS Cooperation Group, 2020). China is not mentioned here either, and the toolbox includes all kinds of risks, not just government intrusion. Nevertheless, it states that governments can impose restrictions and exclude suppliers they consider to be a risk to critical functions.

Importantly, these are only recommendations, and although the EU member states should report the implementation of the recommendations in the toolbox, this is still voluntary. Thus, the various EU initiatives helped the countries implement adequate security in the new 5G networks but left it to each country how they would handle China and Huawei. However, most seem to have chosen an approach similar to that of the EU; neither countries nor vendors are mentioned explicitly in 5G regulation, but the Chinese company could still be excluded entirely or partially based on security assessments and the need for diversification. The aforementioned East European joint declarations with the US were therefore in line with both the Prague Proposals and the EU toolbox, but these documents may have assisted the Europeans in finding a less confrontational approach towards China. In short, 5G was securitized, but China and Huawei were not.

European Solutions

The Prague Proposals and the EU toolbox thus provided European states with a range of solutions that they could use to enhance 5G security without unnecessary macrosecuritization of China. Nonetheless, further national legislation and regulations were necessary to guide telecoms providers in their processes of selecting 5G vendors. Poland, for instance, emphasized the non-technical part of the Prague Proposals and stated that it would conduct a 'rigorous evaluation' of suppliers based on the ownership structure and ethical corporate behaviour of vendors (White House, 2019).

Another approach envisaged in these documents was to prohibit procurement of products manufactured in countries with which the host country did not have formalized security cooperation agreements. This approach effectively prevented the inflow of Chinese products, but opened up the market to non-NATO countries, such as Sweden and Finland, home to Huawei's main competitors, Ericsson and Nokia. Another potential measure was to impose geographical limitations on the 5G radio access network, making sure that particularly sensitive areas, such as military bases or government offices, would not be within reach of antennas produced outside the West. Yet another variant was to limit the percentage of the network that could be produced in countries without security agreements.

Norway, for example, declared in 2019 that a minimum 50 per cent of the 5G base stations should be delivered from countries with which it has security cooperation (Government of Norway, 2019). This decision was based on a new Security Act passed the previous year. The government was also keen to stress that it was up to the telecoms providers to choose their vendors, not the government. This approach probably diverted external political pressure from the authorities to the telecoms providers, thus reducing the chances of securitization of China. The result of the 50 per cent rule was nonetheless that none of the telecoms companies chose Huawei as their 5G supplier, despite having Huawei in their existing 4G networks.[1] Having several vendors in the same network would probably have been both expensive and technically challenging. Importantly, there were no public complaints from Huawei or China over this solution.

The UK initially chose a similar solution. In January 2020, the UK government granted Huawei a limited role in the non-core elements of its 5G network. Up to 35 per cent of the base stations could be supplied by Huawei, with the exception of those near high-risk sites, such as nuclear facilities and military installations (UK Government, 2020a). Predictably perhaps, the US government strongly opposed the British decision. US Secretary of State, Mike Pompeo, called it a 'momentous decision' (Parker et al., 2020a).

Then, a few months later, the UK government made a 180 degree turn and decided not only to ban Huawei from 5G, but also to rip out any equipment from earlier generations of telecoms (UK Government, 2020b). The reason, they said, was because Huawei was now on the aforementioned US Entities List barring it from using US technology or software in its systems. This, it was argued by British security agencies, significantly reduced the security of Huawei equipment since Huawei would have to secure its components from elsewhere (Helm, 2020). Cynical observers argued that the sudden British change probably owed more to political pressure than to a new security assessment (Parker et al., 2020b). This was certainly the interpretation of Huawei and China which both responded angrily. Liu Xiaoming, China's ambassador to the UK, tweeted that 'it has become questionable whether the UK can provide an open, fair and non-discriminatory business environment for companies from other countries', and warned that there would be 'consequences' if Britain started to treat China as a 'hostile country' (ibid.).

Another country that received strong reactions from China was Sweden. On 20 October 2020, the Swedish Post and Telecom Authority issued a statement about the forthcoming 5G spectrum auctions. There it noted that: 'New installations and new implementation of central functions for the radio use in the frequency bands must not be carried out with products from the

1. Norway's leading telecoms provider, Telenor, chose Ericsson as its 5G vendor, but stated that it would continue to use Huawei to 'upgrade to 5G coverage in selected areas of Norway' (Telenor, 2019).

suppliers Huawei or ZTE' (PTS, 2020). The reason was 'to ensure that the use of radio equipment in these bands does not cause harm to Sweden's security' (ibid.). Unsurprisingly, such an explicit ban of Huawei and ZTE immediately became a hot political issue. Huawei appealed to the courts, but the case was dismissed (Reuters, 2021). The Chinese government accused Sweden of violating World Trade Organization rules and using 'so-called national security justifications to reject Chinese companies' and made it clear that China would 'take all necessary measures' in response (Lau, 2021). Interestingly, Ericsson Chief Executive Börje Ekholm also criticized the Swedish government, possibly fearing retaliatory moves by China against Ericsson's investments there (ibid.).

In Germany the 5G debate has been long and fierce but may come to a close in 2021. A new IT Security Law is under preparation which does not explicitly ban any vendor but requires a 30-day technical and political screening period. As discussed above, one may question the utility of such a technical screening, but the political screening may offer a way to prevent untrusted vendors gaining access to the network. However, apparently the law 'only allows for the exclusion of a vendor if all involved authorities are unanimous in their decision to enact a ban' (Thomas, 2021). This means that it is necessary for policy makers to reach a unified decision, or else the supplier would by default be allowed to participate in the 5G rollout (ibid.). This may result in Huawei equipment in German 5G networks after all, provided that the telecoms companies want it. However, the businesses may still choose to be on the safe side, even if the political will to put restrictions on Chinese products has been more muted in Germany compared to many other European states.

The French position is officially neutral. There is no explicit ban, but the French cybersecurity agency, ANSSI, stated in 2020 that it was 'inciting' operators not to choose Huawei (Reuters, 2020c). Countries that were initially positive towards Huawei, such as Portugal, also appear to have changed their minds; their telecoms providers reported in 2020 that they had decided against Huawei in their 5G networks (Reuters, 2020d). The Portuguese government stressed that it had 'not drawn any conclusions directed against any particular supplier', but the result is nonetheless the same (ibid.). In short, the predominant pattern in Europe seems to be that Huawei have lost the 5G battle, with some exceptions.[2] But few states have followed the US and securitized Huawei and China by explicitly prohibiting Huawei in their networks. The majority seem to have used discreet regulatory measures and signalled their security concerns more or less officially to their telecoms branches. In this way it seems that Europe has succeeded in securitizing 5G without securitizing Huawei and China.

2. Hungary, for instance, has opened up for substantial Chinese investments and has no plans to exclude Huawei (Paszak, 2020).

CONCLUSION

In this article we looked at how the US's macrosecuritization of China, and the accompanying niche securitization of Chinese telecoms and 5G, emerged and evolved, both domestically and in Europe. We investigated whether there was something particular about 5G that distinguished it from previous generations of cellular networks, thus making it more susceptible to securitization. We argued that the technological features of the 5G technology, combined with the expected central role it will play in Western societies, do make it more likely to be securitized compared to previous generations of cellular networks. Further, we asked whether the ban on Chinese companies such as Huawei was an appropriate remedy, or whether screening of the products could be an alternative solution. We concluded that screening or similar control mechanisms would not address the main concerns that securitizing actors have raised, such as espionage and sabotage. 5G security could therefore not be resolved at the technical level alone but was likely to be securitized also on the political level.

However, we also found that Europe has, to a large extent, chosen a somewhat different approach to the US. While European states also securitized 5G, they largely limited it to the legal-political aspects and avoided an explicit securitization of Chinese companies. In this way, European states achieved enhanced 5G security without confronting China more broadly. In other words, they subscribed to the American niche securitization of 5G, but avoided the broader macrosecuritization of China. Interestingly, those that securitized Huawei and explicitly banned the company from 5G networks (the UK and Sweden) seem to have paid a political price for it in terms of Chinese responses to their actions. In effect, securitizing Huawei implied also securitizing China. The rest of Europe seems to have avoided this, even if the presence of Chinese 5G equipment on the continent appears to be very limited.

The article also aimed to contribute to the academic exploration and evolution of securitization theory. We have demonstrated the importance of understanding material or technological factors when studying the securitization of complex technology. The technological features of 5G did provide the securitizing actors with some strong arguments — even if they in no way determined the outcome of the securitization. Our discussion of the technological features also demonstrated that the counter-argument launched by Huawei (proposing transparency and screening) was unlikely to convince the other side to desecuritize 5G. This demonstrates the utility of interdisciplinary research. The article has also contributed empirically to the underexplored concept of macrosecuritization: the Europeans chose a somewhat different approach to their biggest ally, the USA, a finding which supports Buzan and Wæver's (2009) point that macrosecurizations are more fragile than mid-level securitizations tend to be.

The securitization of 5G in the West, as explored here, may serve as an indicator of how security relations between China and the West will evolve in the years to come. Many observers argue that an increasingly divided or decoupled world is emerging, in which Western states rely on solely intra-Western supply chains and China relies on non-Western sources (Inkster, 2020; Rühlig and Björk, 2020). In general, relations between China and the EU appear to be souring, as the authoritarian aspects of the Chinese Communist Party gain increased attention in Europe. Suspicion, exchanges of sanctions, and failures of trade and investment agreements seem to dominate the agenda (Ni, 2021). At the same time, however, the Biden administration has indicated a somewhat more nuanced approach to China than the Trump administration. In his first meeting with NATO allies, US Secretary of State Antony Blinken stated that 'The United States won't force our allies into an us-or-them choice with China' (Bloomberg, 2021). Overall, the picture appears to be mixed: future relations between the West and China may therefore consist of an overarching value-based macrosecuritization, combined with more concrete niche securitizations in specific sectors, such as property, infrastructure and digital technology. In any case, securitization is likely to remain a central part of the relationship going forward.

REFERENCES

Balzacq, T., S. Léonard and J. Ruzicka (2016) '"Securitization" Revisited: Theory and Cases', *International Relations* 30(1): 494–531.

Barboza, D. (2010) 'Scrutiny for Chinese Telecom Bid', *New York Times* 22 August. www.nytimes.com/2010/08/23/business/global/23telecom.html (accessed 10 February 2021).

Blanchfield, M. (2020) 'Canada a "Disgraceful" Accomplice to US in Meng Wanzhou Arrest, China Ambassador Says', *Global News* 11 December. https://globalnews.ca/news/7517944/canada-accomplice-disgraceful-ambassador-meng/(assessed 17 June 2021).

Bloomberg (2021) 'Blinken Says US Won't Force "Us-or-Them" Choice with China', Bloomberg 24 March. www.bloomberg.com/news/articles/2021-03-24/blinken-says-biden-won-t-force-us-or-them-choice-with-china (accessed 28 May 2021).

Boyson, S. (2014) 'Cyber Supply Chain Risk Management: Revolutionizing the Strategic Control of Critical IT systems', *Technovation* 34(7): 342–53.

Buzan, B. and O. Wæver (2009) 'Macrosecuritisation and Security Constellations: Reconsidering Scale in Securitisation Theory', *Review of International Studies* 35(2): 253–76.

Buzan, B., J. de Wilde and O. Wæver (1998) *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

Cartwright, M. (2020) 'Internationalising State Power through the Internet: Google, Huawei and Geopolitical Struggle', *Internet Policy Review* 9(3). https://doi.org/10.14763/2020.3.1494

Che, P.H., M. Bakshi, C. Chan and S. Jaggi (2014) 'Reliable, Deniable and Hidable Communication', in *IEEE 2014 Information Theory and Applications Workshop (ITA)*. Piscataway, NJ: IEEE. https://doi.org/10.1109/ITA.2014.6804271

Dunnewijk, T. and S. Hultén (2007) 'A Brief History of Mobile Communication in Europe', *Telematics and Informatics* 24(3): 164–79.

Egele, M., T. Scholte, E. Kirda and C. Kruegel (2008) 'A Survey on Automated Dynamic Malware-analysis Techniques and Tools', *ACM Computing Surveys (CSUR)* 44(2): 1–42.

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

European Commission (2019a) 'EU–China: A Strategic Outlook. Joint Communication to the European Parliament, the European Council and the Council'. JOIN(2019) 5 final, 12 March. Strasbourg: European Commission.

European Commission (2019b) 'Commission Recommendation: Cybersecurity of 5G Networks'. C(2019) 2335 final, 26 March. Strasbourg: European Commission.

European Parliament (2019) 'Security Threats Connected with the Rising Chinese Technological Presence in the EU and Possible Action on the EU Level to Reduce Them'. 2019/2575(RSP), 12 March. Strasbourg: European Parliament.

Federal Register (2019) 'Addition of Entities to the Entity List', *Federal Register*, 21 May. www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list (accessed 19 July 2019).

Foukas, X., G. Patounas, A. Elmokashfi and M.K. Marina (2017) 'Network Slicing in 5G: Survey and Challenges', *IEEE Communications Magazine* 55(5): 94–100.

Government of Norway (2019) 'Viktig steg for digitaliseringen av Norge' ['Important step for the Digitalization of Norway']. Press statement, Ministry of Local Government and Modernization 13 December. www.regjeringen.no/no/aktuelt/-viktig-steg-for-digitaliseringen-av-norge/id2682654/(accessed 22 February 2021).

Hawes, C. and G. Li (2017) 'Transparency and Opaqueness in the Chinese ICT Sector: A Critique of Chinese and International Corporate Governance Norms', *Asian Journal of Comparative Law* 12(3): 41–80.

HCSEC (2018) 'Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2018: A Report to the National Security Adviser of the United Kingdom, July 2018'. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf (accessed 12 May 2021).

Helm, T. (2020) 'Pressure from Trump Led to 5G Ban, Britain Tells Huawei', *The Guardian* 18 July. www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei (accessed 10 May 2021).

Inkster, N. (2019) 'The Huawei Affair and China's Technology Ambitions', *Survival* 61(1): 105–11.

Inkster, N. (2020) *The Great Decoupling: China, America and the Struggle for Technological Supremacy*. London: Hurst.

Lau, S. (2021) 'Sweden Faces Chinese Blowback over Huawei Ban', *Politico* 21 January. www.politico.eu/article/sweden-faces-chinese-blowback-over-huawei-ban/(accessed 10 May 2021).

LRT English (2020) 'Latvia Signs 5G Declaration with US to Sideline China', *LRT English* 28 February. www.lrt.lt/en/news-in-english/19/1146924/latvia-signs-5g-declaration-with-us-to-sideline-china (accessed 20 May 2021).

Lysne, O. (2018) *The Huawei and Snowden Questions*. London: Springer Nature.

Mascitelli, B. and M. Chung (2019) 'Hue and Cry over Huawei: Cold War Tensions, Security Threats or Anti-competitive Behaviour?', *Research in Globalization* 1: 100002.

Morrison, P., K. Herzig, B. Murphy and L. Williams (2015) 'Challenges with Applying Vulnerability Prediction Models', in D. Nicol (ed.) *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*, pp. 1–9. New York: Association for Computing Machinery (ACM).

Ni, V. (2021) 'EU Parliament "Freezes" China Trade Deal over Sanctions', *The Guardian* 20 May. www.theguardian.com/world/2021/may/20/eu-parliament-freezes-china-trade-deal-over-sanctions (accessed 28 May 2021).

NIS Cooperation Group (2019) 'EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks. Report 9 October 2019'. Brussels: EC/NIS Cooperation Group. www.politico.eu/wp-content/uploads/2019/10/Report-EU-risk-assessment-final-October-9.pdf

NIS Cooperation Group (2020) 'Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures. CG Publication January 2020'. Brussels: EC/NIS Cooperation Group. https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

Parker, G., H. Warrell and K. Stacey (2020a) 'Huawei Decision Jolts UK–US Special Relationship at Sensitive Time', *Financial Times* 29 January. www.ft.com/content/5bd4e754-41d4-11ea-bdb5-169ba7be433d (accessed 19 May 2021).

Parker, G., N. Fildes, H. Warrell and D. Sevastapulo (2020b) 'UK Orders Ban of New Huawei Equipment from End of Year', *Financial Times* 15 July. www.ft.com/content/997da795-e088-467e-aa54-74f76c321a75 (accessed 10 May 2021).

Paszak, P. (2020) 'Huawei in Poland and Hungary. Could It be a Part of 5G?'. Warsaw: Warsaw Institute Foundation. https://warsawinstitute.org/huawei-poland-hungary-part-5g/(accessed 23 February 2021).

Prague Proposals (2019) 'The Chairman Statement on Cyber Security of Communication Networks in a Globally Digitalized World'. Prague 5G Security Conference, Prague (3 May).

PTS (2020) 'Four Companies Approved for Participation in the 3.5 GHz and 2.3 GHz Auctions', Swedish Post and Telecom Authority 10 October. https://pts.se/en/news/press-releases/2020/four-companies-approved-for-participation-in-the-3.5-ghz-and-2.3-ghz-auctions/(accessed 26 January 2021).

Republic of Slovenia (2020) 'Slovenia and the US Sign a Joint Declaration on 5G Security'. Ministry of foreign affairs 13 august. www.gov.si/en/news/2020-08-13-slovenia-and-the-us-sign-a-joint-declaration-on-5g-security/(accessed 20 May 2021).

Reuters (2019) 'US Warns European Allies Not to Use Chinese Gear for 5G Networks', Reuters 5 February. www.reuters.com/article/us-usa-china-huawei-tech-eu/u-s-warns-european-allies-not-to-use-chinese-gear-for-5g-networks-idUSKCN1PU1TG (accessed 22 February 2021).

Reuters (2020a) 'Huawei's Investments are "Predatory Actions", Pompeo to Paper', Reuters 2 October. www.reuters.com/article/us-huawei-5g-pompeo-idUSKBN26N0OC (accessed 20 May 2021).

Reuters (2020b) 'Czechs Sign Joint 5G Security Declaration with United States', Reuters 6 May. www.reuters.com/article/us-czech-usa-5g/czechs-sign-joint-5g-security-declaration-with-united-states-idINKBN22I33O (accessed 21 May 2021).

Reuters (2020c) 'France Won't Ban Huawei, but Encouraging 5G Telcos to Avoid It: Report', Reuters 5 July. www.reuters.com/article/us-france-huawei-5g-idUSKBN2460TT (accessed 10 May 2021).

Reuters (2020d) 'Exclusive: Portugal Telcos Won't Use Huawei for Core 5G Networks though no Government Ban', Reuters 30 July. www.reuters.com/article/us-huawei-5g-portugal-exclusive-idUSKCN24V22L (accessed 23 February 2021).

Reuters (2021) 'Swedish Court Dismisses Huawei Appeal over 5G Network Ban', *Reuters* 15 January. www.reuters.com/article/us-sweden-huawei-appeal/swedish-court-dismisses-huawei-appeal-over-5g-network-ban-idUKKBN29K0VE (accessed 10 May 2021).

RFE/RL (2021) 'US Bill Seeks Funding for 5G Networks in Eastern Europe to Counter Chinese Influence', RFE/RL 20 May 2021. www.rferl.org/a/us-funding-networks-huawei/31264443.html (accessed 20 May 2021).

Romania Insider (2020) 'Romania, US Sign Memorandum on 5G Technologies "In Line with Rule of Law Principles"', *Romania Insider* 22 August. www.romania-insider.com/romania-us-5g-memorandum (accessed 21 May 2021).

Ruge, M. and S. Vladisavljev (2020) 'Serbia's 5G Deal with Washington: The Art of Muddling Through'. European Council on Foreign Relations 22 September. https://ecfr.eu/article/commentary_serbias_5g_deal_with_washington_the_art_of_muddling_through/(accessed 20 May 2021).

Rühlig, T. (2020) 'Who Controls Huawei? Implications for Europe'. UI Paper 5/2020. Stockholm: The Swedish Institute of International Affairs.

Rühlig, T. and M. Björk (2020) 'What to Make of the Huawei Debate? 5G Network Security and Technology Dependency in Europe'. UI Paper 1/2020. Stockholm: The Swedish Institute of International Affairs.

Sanger, D.E. and D. McCabe (2020) 'Huawei Is Winning the Argument in Europe, as the US Fumbles to Develop Alternatives', *New York Times* 17 February. www.nytimes.com/2020/02/17/us/politics/us-huawei-5g.html (accessed 10 February 2021).

Sanger, D.E., N. Perlroth and J.E. Barnes (2021) 'As Understanding of Russian Hacking Grows, So Does Alarm', *New York Times* 2 January. www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html?referringSource=articleShare (accessed 10 February 2021).

Taylor, A. (2020) 'Albania Joins US "the Clean Network", Pledges not to Use Huawei 5G', *Exit News* 13 August. https://exit.al/en/2020/08/13/albania-joins-us-the-clean-network-pledges-not-to-use-huawei-5g/(accessed 20 May 2021).

Telenor (2019) 'Telenor Completes 5G Vendor Selection for Norway', Telenor Media 13 December. www.telenor.com/media/press-release/telenor-completes-5g-vendor-selection-for-norway (accessed 31 May 2021).

Thomas, B. (2021) 'What Germany's New Cyber Security Law Means for Huawei, Europe, and NATO'. *European Council of Foreign Relations* 5 February 2021. https://ecfr.eu/article/what-germanys-new-cyber-security-law-means-for-huawei-europe-and-nato/

UK Government (2020a) 'Press Release: New Plans to Safeguard Country's Telecoms Network and Pave Way for Fast, Reliable and Secure Connectivity'. Department of Digital, Culture, Media and Sport 28 January. www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity (accessed 22 February 2021).

UK Government (2020b) 'Press Release: Huawei to be Removed from UK 5G Networks by 2027'. Department of Digital, Culture, Media and Sport 14 July. www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027 (accessed 22 February 2021).

US Congress (2018) 'John S. McCain National Defense Authorization Act for Fiscal Year 2019'. Washington, DC: US Congress.

US Department of State (2020a) 'The Clean Network'. https://2017-2021.state.gov/the-clean-network/index.html (accessed 22 February 2021).

US Department of State (2020b) 'United States–Republic of Lithuania Memorandum of Understanding on 5G Security', 17 September 2020. https://2017-2021.state.gov/united-states-republic-of-lithuania-memorandum-of-understanding-on-5g-security/index.html (accessed 20 May 2021).

US Department of State (2020c) 'United States–Slovak Republic Joint Declaration on 5G Security', 23 October 2020. https://2017-2021.state.gov/united-states-slovak-republic-joint-declaration-on-5g-security/index.html (accessed 20 May 2021).

US Department of State (2020d) 'United States–Republic of Bulgaria Joint Declaration on 5G Security', 23 October 2020. https://2017-2021.state.gov/united-states-republic-of-bulgaria-joint-declaration-on-5g-security/index.html (accessed 20 May 2021).

US Department of State (2020e) 'United States–Republic of North Macedonia Joint Declaration on 5G Security', 23 October 2020. https://2017-2021.state.gov/united-states-republic-of-north-macedonia-joint-declaration-on-5g-security/index.html (accessed 20 May 2021).

US Department of State (2020f) 'United States–Kosovo Memorandum of Understanding on 5G Security', 23 October 2020. https://2017-2021.state.gov/united-states-kosovo-memorandum-of-understanding-on-5g-security/index.html (accessed 20 May 2021).

US Embassy in Estonia (2019) 'United States–Estonia Joint Declaration on 5G Security', 1 November 2019. https://ee.usembassy.gov/joint-declaration-on-5g/(accessed 20 May 2021).

US House of Representatives (2012) 'Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE'. 112th Congress, 8 October. https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf

White House (2019) 'US–Poland Joint Declaration on 5G'. *Press release 5 September*. www.presidency.ucsb.edu/documents/press-release-us-poland-joint-declaration-5g (accessed 19 February 2021).

Xia, F., L.T Yang, L. Wang and A. Vinel (2012) 'Internet of Things', *International Journal of Communication Systems* 25(9): 1101–02.

Karsten Friis (corresponding author; kf@nupi.no) is a Senior Research Fellow and Head of the Security and Defence Research Group at the Norwegian Institute of International Affairs (NUPI), Oslo, Norway. He holds a PhD from the University of Groningen and his main area of expertise is security and defence policies and cyber security.

Olav Lysne (olavly@simula.no) is Director of Simula Metropolitan, and Professor of Communication Systems at the Oslo Metropolitan University, Norway. He headed the national commission on digital vulnerabilities in 2014/2015 and later the commission that evaluated the use of lawful interception of Internet traffic crossing the national borders of Norway.