Royal United Services Institute
for Defence and Security Studies

The Globalisation of Technology
Occasional Paper

5G Cyber Security

A Risk-Management Approach

James Sullivan and Rebecca Lucas

5G Cyber Security

A Risk-Management Approach

James Sullivan and Rebecca Lucas

The Globalisation of Technology

RUSI Occasional Paper, February 2020

RUSI
www.rusi.org

Royal United Services Institute
for Defence and Security Studies

189 years of independent thinking on defence and security

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 189 years.

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution.

Published in 2020 by the Royal United Services Institute for Defence and Security Studies.

RUSI Occasional Paper, February 2020. ISSN 2397-0286 (Online); ISSN 2397-0278 (Print).

Printed in the UK by Kall Kwik.

Royal United Services Institute
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org

RUSI is a registered charity (No. 210639)

Contents

Executive Summary

THIS PAPER ARGUES that approaches to the security of 5G telecommunications networks should depend on national context, including the geographic location of equipment, national cyber security experience, vendor availability and cost. The main policy priority for states should be the implementation of pragmatic technical cyber risk management measures that protect against the majority of risks to 5G networks. In January 2020, the UK's National Security Council made the decision to exclude Huawei technology from the most sensitive parts of the UK's 5G network, while allowing it to supply peripheral components such as mobile phone masts and antennae. From a purely technical perspective, this was a practical and realistic decision that adheres to the principles of cyber risk management and reflects the expert view of the UK's national technical authority, the National Cyber Security Centre.

This research identifies a range of measures to manage risk to 5G networks, including resilient network architecture, access management, testing and monitoring, and cyber security standards. The findings demonstrate how core and edge functions do remain technically distinct in 5G networks and highlight multiple ways to isolate and localise risks. It recognises that 5G poses new challenges for cyber security practitioners, owing to technical concepts such as virtualisation and low-latency communication, but concludes that there are measured ways to manage the risk.

The paper acknowledges that for some states, political and economic considerations may end up being the overriding factors that lead to the decision to ban a particular vendor from a particular state. This may be an entirely legitimate national approach. However, states must be clear about the extent to which political, rather than technical, factors inform their decision-making relating to 5G and other technology. Otherwise, it confuses the argument and undermines the authority of national technical experts.

Finally, the paper argues that 5G is one instance of a much wider set of issues around the globalisation of technology relating to the pivot of technology innovation from West to East. It recommends that states should rapidly identify those advanced technology areas where greater vendor diversity and/or sovereign technology is required and develop an industrial strategy to address these gaps.

I. Introduction

THIS PAPER EXAMINES high-level cyber risks relating to 5G telecommunications infrastructure and assesses to what extent a risk-management approach could mitigate them. The analysis in this paper is based on extensive research of academic literature, media reports, open source government documents and in-depth semi-structured interviews with senior cyber security experts. For these interviews, experts were chosen based on their subject-matter expertise and experience, using a non-probabilistic (selective) sampling method. Interviewees included government officials, law enforcement, private sector experts and academics.[1] Interviews reflect the perspectives of these individuals and should not be interpreted to represent the positions of corporations or governments. Research findings and recommendations also draw on academic and policy literature relating to 5G, open source government documents, media reports and consultation with experts at roundtable events. As with any qualitative research study, there are some limitations. The interview findings inevitably reflect the perspectives, insights and experiences of participants. Furthermore, research is largely limited to information available in the public domain only.

This research is the first in a series of papers to be published as part of a RUSI research project, 'The Globalisation of Technology'. The series examines the cyber security implications of the growing presence of foreign-made components in Western telecommunications infrastructure, how governments perceive the accompanying risks and the actions they are taking in response. Subsequent papers in the series will look beyond 5G to wider risks from the globalisation of technology.

The paper comprises five sections. First, it provides background on the nature of 5G technology and the security threat it could pose. Second, it details overarching risks to 5G networks for policymakers to consider. Third, it examines methods of risk mitigation. Fourth, it addresses the specific question of Huawei. Finally, this report examines the role of government in addressing these challenges and provides a set of recommendations for policymakers to consider. The primary purpose of this paper is to inform policymakers and cyber security practitioners of the range of factors to consider when making policy decisions linked to the rollout of 5G infrastructure, including decisions regarding vendor selection.

[1] Throughout this report, an anonymised coding system is used to refer to interview data. The prefix 'UK G' is used to refer to UK government officials, 'US G' is used for US government officials, 'T' is used for members of the telecommunications sector, and 'A' refers to academic experts. The views expressed by members of government are not intended to represent the government's official position. The views expressed by members of the telecommunications sector are not intended to represent any corporation's official position. The views expressed by members of academia are not intended to represent any institution's official position.

Background

Governments are struggling to determine how to best protect new 5G telecommunications networks, some of which are classed as 'critical national infrastructure' (CNI) in the UK.[2] In particular, global debate continues as to how governments should manage the presence of Chinese technology in the rollout of 5G infrastructure. Citing national security concerns, some governments advocate a blanket ban of Chinese companies like Huawei. Others have decided not to restrict Huawei's participation in 5G networks at all. In January 2020, the UK's National Security Council made the decision to exclude Huawei technology from the most sensitive parts of the UK's 5G network, while allowing it to supply peripheral components such as mobile phone masts and antennae. In addition, their UK market share of peripheral 5G components will be capped at 35%.[3] This approach acknowledges that Huawei is a high-risk vendor (HRV), but the risk is deemed to be manageable.

As with any complex network, 5G networks tend to have vulnerabilities.[4] As they require regular updates, operators frequently grant network access to third parties.[5] Original network components, as well as software updates, are the product of complex, international supply chains that are difficult to trace. The apparent national origin of a product is not a reliable guide to where its components were designed or manufactured. Meanwhile, technology to comprehensively map networks and their components does not yet exist.[6]

Risk management is the process of identifying threats and risks in a particular context and taking action to prevent or reduce them.[7] Cyber risk management is no different. It acknowledges that it is impossible to eradicate risk, especially in complex, multifaceted technology-dependent activities. Instead, the challenge is to set a realistic risk tolerance or level of acceptable risk and develop mitigation methods – typically involving people, processes and technology – that

[2] The UK government defines 'critical national infrastructure' as 'those facilities, systems, sites, information, people, networks, and processes necessary for a country to function and upon which daily life depends … In the UK, there are 13 national infrastructure sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport, and Water'. See Centre for the Protection of National Infrastructure, 'About: Critical National Infrastructure', <https://www.cpni.gov.uk/critical-national-infrastructure-0>, accessed 20 January 2020.

[3] Department for Digital, Culture, Media and Sport (DCMS), 'New Plans to Safeguard Country's Telecoms Network and Pave Way for Fast, Reliable and Secure Connectivity', press release, 28 January 2020, <https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity>, accessed 31 January 2020.

[4] Author's interview with T1, member of the telecommunications sector, 27 September 2019.

[5] *Ibid.*; author's interview with UK G1, UK government official, 29 October 2019.

[6] Author's notes from a techUK event, 30 September 2019.

[7] Collins, 'Risk Management', <https://www.collinsdictionary.com/dictionary/english/risk-management>, accessed 28 January 2020.

have the greatest likelihood of supporting that risk tolerance. Cyber risk-management decisions are fundamentally informed by the degree of confidence in the security of components and infrastructure. This is not a binary objective. There is no such thing as full confidence in equipment, or 'trustworthy' vendors in any context.[8]

In relation to 5G, some states argue for a pragmatic cyber security risk-management approach.[9] Such an approach could keep technology where there are lower degrees of confidence around security, such as from China, out of the most sensitive parts of the network. However, such an approach could still permit the use of Chinese technology in less sensitive or less critical areas. For others, a blanket ban on Chinese equipment is asserted to be the only way to manage the security risks resulting from using Chinese technology in 5G. The US has pressed its allies to ban Chinese companies, primarily Huawei, from providing any 5G network components, originally citing an extremely low degree of confidence in the security of Chinese technology. It has specifically raised concerns about vulnerabilities in Huawei equipment that could give the company, or the Chinese government, access to 5G networks.[10]

The US government has been vocal about its preference that all countries implement a full ban. It has threatened that it will no longer share intelligence with countries which include Huawei in their 5G networks.[11] US officials have alleged that, should the UK include Huawei components in 5G networks, it would 'put our information at risk'.[12] They have even gone so far as to say that the US could not base resources, such as a military base or an embassy, in a country that uses Huawei equipment.[13] These statements are part of an ongoing effort to pressure the UK, and other countries, to exclude Huawei entirely from their 5G networks.

The 5G debate is not just about cyber security. It has become part of a wider geopolitical conversation. It relates to political perceptions of China's place in the world, as well as to economic factors, including Western reliance on Chinese technology and manufacturing,

[8] Author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019.

[9] For a detailed explanation of countries' approaches to 5G, see the written evidence submitted by RUSI for the Joint Committee on the National Security Strategy's inquiry, 'Ensuring Access to "Safe" Technology: The UK's 5G Infrastructure and National Security Issue', <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/national-security-strategy-committee/ensuring-access-to-safe-technology-the-uks-5g-infrastructure-and-national-security/written/105189.html>, accessed 30 January 2020.

[10] Author's interview with US G1, US government official, 15 October 2019.

[11] Zak Doffman, 'US Threatens UK On Huawei and Intelligence-Sharing', *Forbes*, 29 April 2019.

[12] David Bond et al., 'US Cyber Chief Warns UK Against Giving Huawei "Loaded Gun"', *Financial Times*, 24 April 2019.

[13] *The Economist*, 'Britain Lets Huawei into Part of Its 5G Networks,' 24 April 2019.

advanced Chinese innovation in technology and fears that the West is falling behind.[14] There are also human rights concerns, including about how Chinese technology companies have enabled the Chinese government to suppress its citizens.[15] Many countries have found themselves caught between the US and China and have yet to make a definitive decision on Huawei.[16] Meanwhile, the deployment of 5G infrastructure is ongoing in many countries, often using Huawei's low-cost equipment or building on existing previous-generation Huawei infrastructure.[17] There is a business cost to 'ripping out' Huawei equipment and starting again.[18]

However, there is more to 5G networks than Huawei.[19] An overwhelming focus on one technology, one company and one state – while understandable – masks broader issues about the proliferation of technology and innovation, and how best to manage the accompanying risks, for 5G and beyond. All 5G networks, whether they include Huawei equipment or not, face common technical risks and challenges.

While both technological and geopolitical factors could shape risk-management decisions on 5G, research has evidenced the importance of clearly distinguishing between the two.[20] The use of geopolitical and economic criteria may be a legitimate national approach in terms of 5G vendor selection. However, governments must be clear about the extent to which political or economic factors, rather than technical assessments, inform their decision-making relating to 5G. Otherwise, they risk undermining technical authorities by masking political or economic considerations with weak assertions about technical risk that fail to acknowledge the multiple measures that exist to secure networks. For example, the UK's National Cyber Security Centre (NCSC) will have a leading role in how the UK makes policy decisions on cyber risk from the globalisation of technology over the next decade and beyond.

What is 5G Technology?

5G telecommunications networks promise download speeds 10 to 20 times faster than legacy networks. In some instances, ensuring their confidentiality, integrity and availability will be

[14] Author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G4, UK government official, 11 November 2019.

[15] Zak Doffman, 'Has Huawei's Darkest Secret Just Been Exposed By This New Surveillance Report?', *Forbes*, 29 November 2019.

[16] See evidence presented in House of Commons, Science and Technology Committee, 'Oral Evidence: UK Telecommunications Infrastructure, HC 2200', 10 June 2019, <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/uk-telecommunications-infrastructure/oral/102931.html>, accessed 24 July 2019.

[17] *Ibid.*

[18] Mark Sweney, 'Huawei Ruling Will Cost Us £500m, Says BT', *The Guardian*, 30 January 2020.

[19] Tom Wheeler and Robert D Williams, 'Keeping Huawei Hardware Out of the US Is Not Enough to Secure 5G', *Lawfare*, 20 February 2019.

[20] Author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019.

a matter of national security.[21] They promise the opportunity to connect more devices to a faster network compared with existing telecommunications networks. Potential 5G use cases foresee the network supporting millions of devices from phones and smart refrigerators, to critical functions like power plants and emergency communications.[22] Current mobile networks support fewer devices and provide fewer critical services. 5G dependence, including for critical services, will increase the impact on societies if 5G infrastructure were to fail.[23] However, sceptics say that the risks from 5G are overhyped. Not many new use cases for critical services have emerged so far. Huge capital expense, and approval from authorities governing sectors such as transportation or energy, would be required to deliver them.[24]

At present, 5G is not a revolutionary telecommunications transformation. The underlying technology is primarily an evolution from previous generations of telecommunications equipment.[25] Current 5G networks are non-stand-alone, meaning they are built on top of existing telecommunications networks. While future stand-alone 5G networks may include revolutionary technology, such networks are not yet feasible.[26] Some countries are working hard to deliver stand-alone 5G networks.[27] Regardless, both non-stand-alone and stand-alone networks are characterised by high speed, minimal delays and the ability to accommodate more devices.[28] Such characteristics rely on features such as virtualisation, or the increased use of software rather than hardware, and edge computing, which enables networks to move

[21] Availability entails ensuring users who need the network can access it at any time. Integrity requires that the network provide accurate information about where data is coming from and who (or what) generated it. Confidentiality is protecting user data and metadata from unauthorised access. The three are often referred to as network 'CIA'.

[22] World Economic Forum, 'The Impact of 5G: Creating New Value Across Industries and Society', 7 January 2020.

[23] Author's interview with UK G7, UK government official, 21 November 2019.

[24] Ferry Grijpink et al., 'Cutting Through the 5G Hype: Survey Shows Telcos' Nuanced Views', McKinsey & Company, February 2019.

[25] Author's interview with A1, academic and legal expert, 15 October 2019; author's interview with UK G3, UK government official, 8 November 2019.

[26] DCMS, *UK Telecoms Supply Chain Review Report* (London: DCMS, 2019), p. 16; NIS Cooperation Group, 'EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks', 9 October 2019, p. 19.

[27] Matt Kapko, 'SK Telecom Boasts Standalone 5G "First," Readies Launch', *SDX Central*, 21 January 2020, <https://www.sdxcentral.com/articles/news/sk-telecom-boasts-standalone-5g-first-readies-launch/2020/01/>, accessed 28 January 2020.

[28] Author's interview with UK G5, UK government official, 31 October 2019. High speed and minimal delays are both part of 'ultra-reliable, low-latency (URLL)' connections and are one of the key new features of 5G. Experts anticipate URLL connections will be essential for proposed use cases such as automated vehicles; World Economic Forum, 'The Impact of 5G', p. 7.

processing power closer to the user.[29] Analysts predict that these characteristics will allow 5G to support more functions across society, from autonomous vehicles to smart cities.[30]

5G networks comprise multiple 'layers' that perform varying parallel functions across the network (see Table 1). Each layer has access to different amounts of information and can transport data packets to and from other layers within the network. Individual components within a layer transmit and receive different amounts and types of information across the network, depending on their access rights to other parts of the network.

5G functions can be divided into two groups – the core and the edge. The core consists of components that have much greater control over the network than access-layer (edge) components. Core components know much more about the context of a 5G network and include routing and switching functions on base stations. If they fail or are compromised, the impact on the rest of the network could be high, as the core has components that determine functions that overlay and control the entire network.[31] Without these functions, the rest of the network could cease to operate.[32] In the UK, 5G networks will have more cores than previous networks, though the exact number and location remains the purview of operators.[33]

Edge functions are, as would be expected, located at the periphery of the network. The definition of core and edge is not a precise science. For the purposes of this paper, the authors adopt the NCSC's definition that edge components only sit within the access layer of a 5G network.[34] This part of the network is closest to end users and is the interface between the network and its customers. Data within this layer includes who is accessing the network and the information sent to and from it by the customer. The failure of individual components at the edge, such as

[29] NIS Cooperation Group, 'EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks', p. 33; author's interview with UK G7, UK government official, 30 October 2019; author's interview with T5, member of the telecommunications sector, 3 October 2019.

[30] Author's interview with T5, member of the telecommunications industry, 3 October 2019; World Economic Forum, 'The Impact of 5G'.

[31] Core components include network function virtualisation infrastructure, virtual network function, management and network orchestration, operational support systems and business support systems.

[32] Ian Levy, 'Security, Complexity, and Huawei; Protecting the UK's Telecoms Networks', blog, National Cyber Security Centre (NCSC), 22 February 2019, <https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks>, accessed 22 July 2019.

[33] Author's interview with UK G1, UK government official, 29 October 2019. 'There are essentially more cores because of the distribution'.

[34] The authors chose to use this definition as this reflects the risk-management approach adopted by the UK, and it is the approach that has been scrutinised by other nations. It defines that peripheral 5G components will only sit within the access layer of the network. It is a precise definition that makes a clear distinction between the access layer (edge) and other parts of the network. The definition of edge does not include the transport layer (that is, wires, fibres, microwaves and other methods of transmission).

a radio access network (RAN)[35] antenna, usually only affects a small area of the network and can be easily isolated and mitigated.[36] At this layer, the impact of failure or compromise has a limited impact radius with other parts of the network and there is limited access to the sensitive data that helps run the network.

Table 1: 5G Network Layers Explained.

Layer and Examples**	Function	Access to Data*	Impact Radius*	Importance*
End User Device (such as phones and other Internet of Things devices)	Means by which the customer performs various functions using the network.	Varies	Limited***	Varies
Access Layer	Communicates directly with end user devices to transport packets. Often categorised as edge.	Low	Local	Medium
Transport Layer	Moves information between nodes.	Low	Local	Low
Routing and Switching	Decides which information is most important and where packets need to travel. Often categorised as core.	Moderate	Local or network-wide****	Medium
Management Plane	Coordinates all other functions. Often categorised as core.	High	Network-wide	High

Source: Author generated.

[35] The radio access network is the part of 5G network infrastructure that connects end user devices with the network's transport and transmission layer that aggregates traffic and carries it to the network's central control functions. The UK Supply Chain Review Report assessed that RAN carried less critical security risks than other parts of the network, which could be sufficiently mitigated through diversity of supply. DCMS, *UK Telecoms Supply Chain Review Report*, p. 26; House of Commons, Science and Technology Committee, 'Oral Evidence'.

[36] Author's interview with UK G3, UK government official, 8 November 2019. '[B]ase station on the roof is going to fail at some point – what does that mean? … Well it can only talk to the base stations nearby'. In Levy, 'Security, Complexity, and Huawei', it is noted that 'Transport nodes only care about the directly adjacent nodes that they're physically connected to'.

** 'Access to data' refers to the amount of data packets this layer of a 5G network needs to function. 'Impact radius' refers to the potential impact on the rest of a 5G network if some equipment from this layer were to be compromised. 'Importance' refers to the importance of this layer to the overall functioning of a 5G network.*

*** Terminology and network mapping vary across users. This particular division was taken from Ian Levy, 'Security, Complexity, and Huawei; Protecting the UK's Telecoms Networks,' National Cyber Security Centre, 22 February 2019, <https://www.ncsc.gov.uk/blog-post/blog-post-security-complexity-and-huawei-protecting-uks-telecoms-networks>, accessed 22 July 2019; Department for Digital, Culture, Media and Sport, 'UK Telecoms Supply Chain Review Report', 22 July 2019, p. 26, <https://www.gov.uk/government/publications/telecoms-supply-chain-review-terms-of-reference>, accessed 22 July 2019; European Union Agency for Cybersecurity, 'ENISA Threat Landscape for 5G Networks', 21 November 2019, <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>, accessed 21 November 2019.*

**** The impact on the wider 5G network from an end user device could be severe if core functions were to be moved closer to the edge of the network, or if the end user device transmitted sensitive data relating to routing and switching functions.*

***** This depends on the type of router that fails. Although mostly local, this does depend on which section of routing fails. If it is a Customer Edge router (CE), then it is local impact. If it is a Provider Router (P Node), the impact radius would be significantly higher.*

Some experts argue that the distinction between the core and the edge of 5G infrastructure no longer exists.[37] This argument often draws on two key points.

[37] Chris Duckett, '5G Stakes Couldn't Be Higher So We Advised Huawei Ban: ASD', *ZDNet*, 30 October 2018; Elsa B Kania, 'Securing Our 5G Future: The Competitive Challenge and Considerations for US Policy', Center for a New American Security, 7 November 2019; Justin Sherman, 'Making Sense of a Huawei "Partial Ban"', blog post, New America, 3 July 2019, <https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/making-sense-huawei-partial-ban/>, accessed 13 December 2019; Leigh Hartman, 'Get Smart: Core vs. Edge in 5G Networks', US Embassy and Consulates in the United Kingdom, 17 September 2019, <https://uk.usembassy.gov/get-smart-core-vs-edge-in-5g-networks/>, accessed 13 December 2019; Colin Packham, 'Australia Spy Chief Says 5G Risks High, in Nod to China Firms' Exclusion', *Reuters*, 30 October 2018. The article quotes Mike Burgess, Director-General of the Australian Signals Directorate: '[b]ut the distinction between core and edge collapses in 5G networks'. Tom Wheeler, '5G in Five (Not So) Easy Pieces', report, Brookings, 9 July 2019: 'The U.K. government has tried to find a middle ground solution by screening all Huawei software and keeping the company out of the core network … however, the 5G core network is virtualized in software and moved to the edge of the network'. Kiran Stacey, 'UK's Approach to Huawei is Flawed, Warns Ericsson's US Boss', *Financial Times*, 24 June 2019: 'Asked whether it made sense for countries to try to distinguish between core and noncore parts of the network, [Niklas Heuveldop] said: "Not really … I don't understand that" ... Paul Triolo, a technology policy expert at Eurasia Group, said: "The real issue is that so much of 5G is intended to be software-based … that the traditional distinctions between core and edge do begin to blur"'. In House of Commons, Science and Technology Committee, 'Oral Evidence', see the evidence

First, 5G networks will use virtualised hardware, meaning that in some instances, multiple functions across the network can now be run using the same shared physical components, in a cloud-based environment. Historically, software has been run on proprietary hardware, meaning that there would be specific physical boxes for specific network functions. Meanwhile, the commodity hardware used in 5G runs software from multiple vendors, within the same physical box, to perform multiple network functions. The perceived cyber risk is that, in this new context, there is no physical or logical separation between core and edge functions.[38] Instead, virtualised hardware boxes could be increasingly exposed to malicious or vulnerable code from multiple vendors, which could in turn compromise multiple network functions. However, it is important to note that the diversity of software and network functions within multiple boxes can actually increase wider network security and resilience.[39] For example, there would be no single point of failure because of the variety of multi-functional boxes. Furthermore, firewalls and other measures are already being used to segregate network layers in a virtualised environment.[40] The challenge for cyber security practitioners is to ensure that this is done effectively in the context of 5G networks. Past approaches to cyber security remain applicable.

Second, 5G networks are designed to support low-latency data transfer in microseconds which enables extremely fast communications. Achieving such speeds requires moving processing power closer to the edge of the network than ever before. This requires having more network cores and putting core functions closer to the end user. In theory, this could require moving some core components to the same location as edge components – for example, putting core functions on RAN antennae. However, strong arguments have been made that pushing core functions so far out would be unwise and unnecessary.[41] There are no use cases where this is currently required, and it would put core components at greater risk.

If the distinction between core and edge were no longer meaningful for 5G networks, this would have serious consequences for risk-management approaches to 5G cyber security. If it were no longer possible to distinguish between critical and non-critical parts of the network, in theory a threat actor could gain access to any part of the network and move laterally to more sensitive parts of the network without any restrictions. It would mean that some existing cyber security measures, such as network segmentation, would be ill-equipped to manage 5G cyber risk.

given by Steve Sampson ('One aspect of moving to this core edge component is that there will be core components, but there will also be virtualised RAN as we discussed. That means that the distinction between core and RAN is no longer so simple') and Mikko Karikytö ('Then the barrier between core and edge will be blurred').

[38] Simeon Gilding, '5G Choices: A Pivotal Moment in World Affairs', Australian Strategic Policy Institute, 29 January 2020, <https://www.aspistrategist.org.au/5g-choices-a-pivotal-moment-in-world-affairs/>, accessed 31 January 2020.

[39] Author's interview with UK G3, UK government official, 8 November 2019.

[40] Amazon Web Services, 'Shared Responsibility Model', <https://aws.amazon.com/compliance/shared-responsibility-model/>, accessed 31 January 2020.

[41] Levy, 'Security, Complexity, and Huawei'.

However, core and edge functions do remain technically distinct in 5G infrastructure, if measures are implemented to a high standard.[42] This should inform national 5G cyber risk-management approaches. Network operators and international standards bodies have published standards to segment a network and separate the layers.[43] For example, operators design and install firewalls and security gateways between the edge and core.[44] This paper will demonstrate multiple measures designed to make it difficult for someone with access to one layer to move to another, even in a virtualised environment.[45] Research revealed that adhering to these measures and standards increases the likelihood that different layers remain separate from one another, although it is impossible to make a complete guarantee.[46] On top of common standards, all operators have different configurations using different components that can have an impact on the security of a network.[47]

To address these differences, all governments – to some extent – regulate how operators must build their networks or what components to include. In the UK, the Department for Digital, Culture, Media and Sport (DCMS) has recommended new regulations to ensure cyber security in the telecommunications sector. This would not just be for 5G.[48] Not all components are instrumentally important to network security in 5G technology. The challenge is knowing which components are, and managing the risks accordingly. The assertion that there is no distinction at all between sensitive and non-sensitive parts of a 5G network dismisses multiple measures that have historically reduced risk to telecommunications networks.

[42] *Ibid.*

[43] House of Commons, Science and Technology Committee, 'Oral Evidence'.

[44] Nic Fildes, 'Can the 5G Network Be Secured Against Spying?', *Financial Times*, 19 January 2020.

[45] 3GPP's most recent set of standards for 5G came out in autumn 2019. See 3GPP, 'Release 15', 26 April 2019, <https://www.3gpp.org/release-15>, accessed 16 December 2019. Final iterations of Release 16 will not be available until June 2020; author's interview with T3, member of the telecommunications sector, 3 October 2019.

[46] DCMS, *UK Telecoms Supply Chain Review Report*, p. 26; NIS Cooperation Group, 'EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks'; author's interview with T1, member of the telecommunications sector, 27 September 2019; author's interview with T3, member of the telecommunications sector, 3 October 2019.

[47] Author's interview with T5, member of the telecommunications sector, 29 October 2019.

[48] DCMS, *UK Telecoms Supply Chain Review Report*.

II. 5G Cyber Security: A Risk-Management Approach

SECURITY VULNERABILITIES IN 5G networks could derive from a range of sources. Poor network design and operation by network operators can create weaknesses in security that can be exploited by a range of actors. Russian state-sponsored actors, for example, leveraged vulnerabilities associated with poor network administration to conduct a series of cyber attacks in 2018.[49] At the more sophisticated end of the scale, threat actors could launch cyber attacks exploiting such vulnerabilities to affect the way particular technology works, as well as to extract data. A further potential risk arises if the technology is deliberately altered at the source, to enable exploitation once it is deployed to the customer. This could be from a remote cyber attack conducted by hostile cyber actors, or potentially on the behest of a government of a country in which the technology is produced. In practice, telecommunications networks are open to threats in multiple ways, and the national origin of the equipment involved is a long way from being the most significant risk area. Russia, for example, has always been one of the leading sources of cyber threats, but virtually none of the UK's CNI is Russia-sourced.[50]

Software invariably contains accidental flaws,[51] some of which will create security vulnerabilities for the network. Often, when these vulnerabilities are discovered, companies provide patches. If a known vulnerability is deliberately left unpatched, it becomes a bug door.[52] On the other hand, if a vulnerability is intentionally inserted and not disclosed, it is called a backdoor.[53] Whatever the source of the vulnerability, deliberate or accidental, it can expose the network to the risk of exfiltration, disruption or sabotage. Bug doors and backdoors are concerning because

[49] NCSC, 'Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices', Technical Alert, 16 April 2018, <https://www.ncsc.gov.uk/files/Russian%20State%20Sponsored%20Actor%20Advisory.pdf>, accessed 28 January 2020, p. 4. Specifically, the actors took advantage of operators' use of legacy management protocols and their failure to ensure and maintain the security of network devices.

[50] Levy, 'Security, Complexity, and Huawei'.

[51] Author's interview with T4, member of the telecommunications sector, 7 October 2019.

[52] Justin Sherman and Robert Morgus, 'Not Every Huawei Flaw is a Backdoor', *New America Weekly*, No. 248, 9 May 2019, <https://www.newamerica.org/weekly/edition-248/not-every-huawei-flaw-backdoor/>, accessed 10 December 2019.

[53] *Ibid.*; John N Stewart, 'Features, Bugs, and Backdoors: The Differences, How Language Can Be (Mis) Used, And A Word of Caution', *Cisco Blogs*, 18 December 2013, <https://blogs.cisco.com/security/features-bugs-and-backdoors-the-differences-how-language-can-be-misused-and-a-word-of-caution>, accessed 29 January 2020.

a malicious actor does not have to spend time searching for them.[54] Instead, they already know that the vulnerability exists.

5G's increased use of software presents additional challenges.[55] In previous generations, resilience for telecommunications operators meant replacing hardware that had unexpectedly failed.[56] Put simply, this involved having sufficient replacement parts to quickly fix the network.[57] 5G's varying reliance on software has changed the way in which operators can improve resilience and build in cyber security.[58] Further, the transition to virtualisation could create new issues in 5G networks that operators have less experience managing.[59]

Threats to 5G infrastructure originate both inside and outside the network. Attacks could originate from aggressive states, organised criminals and individual hacktivists, either infiltrating or abusing their privileged access inside the network.[60] Opponents of Huawei's inclusion in 5G networks often express the fear that the company could install a backdoor allowing them to shut down the entire network at will.[61] This seems simplistic considering the complexity of 5G networks and the supply chains. Even if an attacker could compromise the core by leveraging edge components, no one has yet successfully demonstrated how such an attack could occur with current security measures.

Risks to 5G Infrastructure

Research identified three principal risks to 5G networks for policymakers to consider. They apply to all 5G networks, regardless of the vendors. As the NCSC has pointed out, Russia has hacked into UK systems numerous times without ever supplying telecommunications components.[62] A narrow focus on one vendor risks obscuring broader questions about the measures necessary to adequately secure 5G networks from a diverse set of adversaries.[63]

- Risk 1: Supply chain complexity.
- Risk 2: An increased attack surface and attack opportunities.
- Risk 3: Lack of vendor diversity.

[54] Author's interview with T4, member of the telecommunications sector, 7 October 2019.

[55] Author's interview with UK G7, UK government official, 21 November 2019.

[56] *Ibid.*

[57] *Ibid.*

[58] *Ibid.*

[59] *Ibid.*

[60] Author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019; European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape for 5G Networks: Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G)* (Athens and Heraklion: ENISA, 2019).

[61] Author's interview with US G1, US government official, 15 October 2019; Elsa B Kania, 'Securing our 5G Future'.

[62] Levy, 'Security, Complexity, and Huawei'.

[63] *Ibid.*

Mitigation measures for each of these risks are addressed in the next section, immediately following the risk considerations.

Risk 1: Supply Chain Complexity

Supply chains for 5G network components are long and complex.[64] Subcontractors are likely to be located in multiple countries, making it almost impossible to determine the national origin of a component.[65] Vendors' ability to control quality is low at the early stage of a product's lifecycle.[66] At the same time, the potential impact of sabotage earlier in the product's lifecycle is high.[67] There are opportunities for malicious actors to infiltrate the supply chain at multiple points, either through a compromised vendor or by abusing insider access.[68]

To ensure a high degree of confidence in the equipment produced by a vendor – whether hardware or software – at least three conditions for the primary vendor and all companies in its supply chain are needed:

1. The vendor has an effective quality control process to find accidental or deliberate security vulnerabilities, especially in software.
2. The vendor regularly screens all employees to identify anyone who could tamper with equipment (as part of hacktivism, organised crime, government pressure or espionage).
3. The vendor has physical and information security measures in place that protect unauthorised access to its intellectual property and processes.

Most companies cannot fully satisfy these given the size and scale of their supply chains. No vendor guarantees trustworthy equipment. Instead, it is important to assess the security of equipment based on degrees of confidence, rather than complete certainty. The software that supports 5G networks comprises millions of lines of code drawn from multiple locations.[69] Experience shows that defects per thousand lines of code (KLOC) exist on a large scale, many of which cause vulnerabilities.[70] Research on the exact number varies widely, but it has been

[64] Author's interview with UK G4, UK government official, 11 November 2019; NIS Cooperation Group, 'EU Coordinated Risk Assessment of the Cybersecurity of 5G networks', p. 11.

[65] Author's interview with UK G1, UK government official, 29 October 2019; Bruce Schneier, 'Every Part of the Supply Chain Can Be Attacked', *New York Times*, 25 September 2019. Note also that the vendor is normally considered to be at the top of the chain and subcontractor relationships traverse the tree on the branches below.

[66] Author's interview with T1, member of the telecommunications sector, 27 September 2019.

[67] Ariel (Eli) Levite, 'ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies', Carnegie Endowment for International Peace, 4 October 2019, <https://carnegieendowment.org/2019/10/04/ict-supply-chain-integrity-principles-for-governmental-and-corporate-policies-pub-79974>, accessed 7 October 2019.

[68] *Ibid.*

[69] Author's interview with T4, member of the telecommunications sector, 7 October 2019.

[70] *Ibid.*

suggested that it averages at around seven defects per KLOC.[71] The US Defence Innovation Board noted that poor software development is a 'universal problem'.[72] Meanwhile, the EU Coordinated Risk Assessment concluded that unidentified vulnerabilities are 'a leading cause of potentially undetected, long-lasting intrusions into networks'.[73]

There are a variety of malicious threat actors that could enter the supply chain. Government officials have publicly stated concerns about other states' ability to insert agents into technology companies.[74] The EU Coordinated Risk Assessment argues that capable and well-resourced actors could infiltrate any level of any vendor's 5G supply chain.[75] The attacker could be a state or organised crime actor, or a hacktivist.[76] The earlier in the stage of a product's lifecycle that a malicious actor alters a component, the greater the multiplier effect of the alteration.[77] And malware or backdoors can be installed at various layers of 5G infrastructure.[78]

Banning Huawei as a 5G vendor would not prevent Chinese presence and influence in supply chains.[79] As of 2018, the most recent year for which data was available, China controlled 35% of the market share for telecommunications equipment and was the home of half of the world's electronics-manufacturing capacity.[80] Chinese companies are an inevitable participant in 5G supply chains,[81] and most 5G vendors – including Nokia, Cisco and Ericsson – have factories

[71] Syed Muhammad Ali Shah, Maurizio Morisio and Marco Torchiano, 'An Overview of Software Defect Density: A Scoping Study', *APSECW 2012: Proceedings of the 19th Asia-Pacific Software Engineering Conference* (Washington, DC: IEEE Computing Society, 2013).

[72] Milo Medin and Gilman Louie, 'The 5G Ecosystem: Risks and Opportunities for DoD', Defense Innovation Board, 3 April 2019, p. 24.

[73] NIS Cooperation Group, 'EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks', p. 26.

[74] Ciaran Martin, 'Ciaran Martin's CyberSec Speech in Brussels', 20 February 2019, <https://www.ncsc.gov.uk/speech/ciaran-martins-cybersec-speech-brussels>, accessed 3 August 2019.

[75] NIS Cooperation Group, 'EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks', p. 22: 'While a threat actor's direct access to or influence on the telecom supply chain may significantly facilitate its exploitation for malicious actions … it should also be noted that actors with a high level of intent and capabilities, such as State actor [sic], would seek to exploit vulnerabilities at any stage of the product lifecycle provided by any supplier'; author's interview with T1, member of the telecommunications sector, 27 September 2019.

[76] NIS Cooperation Group, 'EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks', p. 13.

[77] Author's interview with T1, member of the telecommunications sector, 27 September 2019; DCMS, *UK Telecoms Supply Chain Review Report*, p. 26.

[78] DCMS, *UK Telecoms Supply Chain Review Report*; Levite, 'ICT Supply Chain Integrity'.

[79] Author's interview with A1, academic expert, 15 October 2019.

[80] *The Economist*, 'Supply Chains for Different Industries Are Fragmenting in Different Ways', 11 July 2019.

[81] Author's interview with A1, academic expert, 15 October 2019.

in China.[82] The number of possible points of entry into the 5G supply chain makes it almost impossible to verify the origin of all of the components that comprise any given product.

Patches or updates to the network also derive from a complex supply chain. Each software update or patch provides an opportunity to insert backdoors or accidentally introduce vulnerabilities into the source code.[83] With current technology, it is impossible to exhaustively test every patch owing to time constraints,[84] and actually proving that there are no defects is nearly impossible.

Risk 2: Increased Attack Surface and Attack Opportunities

Even if a vendor could provide full confidence in its equipment, 5G networks present new risks compared to previous generations.[85] These risks include: larger physical and virtual attack surfaces, particularly in the RAN; the physical disaggregation of network components;[86] the number of devices connected to the network; and the frequency of software patching.[87] For non-stand-alone 5G networks, vulnerabilities in legacy networks add to the number of risks.[88]

5G-related antennae are a low-level risk. Antennae that support 5G networks have a much shorter range and, consequently, there will be more antennae distributed over the same geographic area than there were in 4G.[89] These components could become more vulnerable as they could process more sensitive information.[90] However, while it is technically possible to push data processing capabilities to individual antenna, it is highly unlikely. There is no use case currently anticipated that would require it and there would be significant issues with achieving the necessary security.[91] Until then, attacks on individual antennae will only achieve highly localised impact.

[82] Murray Scot Tanner, 'Beijing's New National Intelligence Law: From Defense to Offense', *Lawfare*, 20 July 2017; author's interview with UK G1, UK government official, 29 October 2019; *The Economist*, 'Supply Chains for Different Industries Are Fragmenting in Different Ways'.

[83] Medin and Louie, 'The 5G Ecosystem', p. 24.

[84] Author's interview with T1, member of the telecommunications sector, 27 September 2019; author's interview with T5, member of the telecommunications sector, 29 October 2019.

[85] Schneier, 'Every Part of the Supply Chain Can Be Attacked'.

[86] Author's interview with T1, member of the telecommunications sector, 27 September 2019; author's interview with T3, member of the telecommunications sector, 3 October 2019.

[87] Author's interview with T3, member of the telecommunications sector, 3 October 2019.

[88] Author's notes from a roundtable event at Stiftung Neue Verantwortung, Berlin, 4 September 2019.

[89] Colin Blackman and Simon Force, *5G Deployment: State of Play in Europe, USA and Asia* (Luxembourg: European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies, Directorate-General for Internal Policies, 2019), p. 7. This report estimates the range to be in the hundreds of metres and perhaps in the tens of metres. In interviews, most individuals cited ranges in the tens of metres.

[90] Author's interview with UK G4, UK government official, 11 November 2019.

[91] Levy, 'Security, Complexity and Huawei'.

Of much more concern will be a larger number of devices connected to 5G networks.[92] This increases the number of opportunities for attackers to sabotage a system or exfiltrate data using the weakness of a single device.[93] For example, the increased number of devices connected to 5G networks will make it easier to launch a distributed denial of service (DDoS) attack.[94] Most of these devices, which will range from mobile phones to industrial shipping containers, are likely to lack robust security and authentication measures.[95] Further, the same technical supply chain risks that apply to network infrastructure will apply to devices that connect to the network.[96]

All networks, old and new, run using software. 5G will be reliant on software updates and patches, just like previous generations of telecommunications networks, and the scale of patching could increase.[97] If so, frequent updates could increase the number of instances at which the network might be vulnerable to attack and misuse.[98] At present, operators find it difficult to conduct in-house oversight of networks, and they employ subcontractors (often including the original 5G vendor) to repair and maintain the network.[99] Much like legacy networks, there is a risk that vendors could be granted unsupervised access without a time limit.[100]

Risk 3: Lack of Vendor Diversity

The 5G market has a very small number of vendors who can provide for the entire network.[101] Huawei, Ericsson, Nokia and ZTE are the only providers of RAN equipment in mainland Europe. Consequently, there is a risk of a single point of failure, and these vendors may have too much leverage.[102] This lack of diversity is an enduring challenge for 5G networks.

[92] Author’s interview with T3, member of the telecommunications sector, 3 October 2019.

[93] NIS Cooperation Group, ‘EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks’, p. 29.

[94] Ano Serrano Mamolar et al., ‘Towards the Detection of Mobile DDoS Attacks in 5G Multi-Tenant Networks’, *IEEE Xplore*, 15 August 2019, <https://ieeexplore.ieee.org/abstract/document/8801975>, accessed 29 January 2020.

[95] NIS Cooperation Group, ‘EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks’, p. 29.

[96] Levite, ‘ICT Supply Chain Integrity’.

[97] Author’s interview with T1, member of the telecommunications sector, 27 September 2019; NIS Cooperation Group, ‘EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks’, p. 29.

[98] Author’s interview with UK G1, UK government official, 29 October 2019; NIS Cooperation Group, ‘EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks’, p. 20.

[99] Author’s interview with T1, member of the telecommunications sector, 27 September 2019; author’s interview with UK G1, UK government official, 29 October 2019.

[100] Author’s interview with UK G1, UK government official, 29 October 2019; author’s interview with UK G3, UK government official, 8 November 2019; author’s interview with UK G4, UK government official, 11 November 2019.

[101] Author’s interview with UK G4, UK government official, 11 November 2019.

[102] Author’s notes from roundtable event at Stiftung Neue Verantwortung, Berlin, 4 September 2019.

A lack of vendor diversity could increase the risk of systemic failures or hostile exploitation of the network.[103] There is a risk that vendor-specific vulnerabilities could easily spread across the whole network.[104] Likewise, an over-reliance on components from a single vendor would leave the network exposed in the event of a problem.[105] Arguably, as there are only three suppliers that provide RAN equipment in the UK, a blanket ban on one could actually end up increasing the cyber risk to 5G networks. A complete ban on Huawei in the UK would have left only Nokia and Ericsson as 5G vendors, reducing vendor competition.

Measures to Mitigate 5G Risk

5G networks will never be completely secure, no matter what the risk-management approach. However, there are ways to make it difficult for cyber threat actors to exploit the network's vulnerabilities.[106] Research identified various measures that could help mitigate risks to 5G infrastructure:

- Measure 1: Resilient network architecture.
- Measure 2: Access management.
- Measure 3: Testing and monitoring.
- Measure 4: Strong cyber security standards.
- Measure 5: Banning of certain components in certain parts of the infrastructure.

Measure 1: Resilient Network Architecture

Operators and regulators must assume that any piece of equipment can fail or become vulnerable to cyber attack.[107] Safeguarding 5G networks is about ensuring that the failure of one component – or several components from a single vendor – does not impact the entire network.[108] 5G networks should be designed with defence in depth and an emphasis on resilience.[109] Network segmentation and redundancy are two important considerations.

[103] DCMS, *UK Telecoms Supply Chain Review Report*.

[104] Author's interview with UK G3, UK government official, 8 November 2019.

[105] Author's interview with UK G1, UK government official, 29 October 2019.

[106] Author's interview with UK G3, UK government official, 8 November 2019.

[107] Medin and Louie, 'The 5G Ecosystem', p. 29; author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019.

[108] Author's interview with T3, member of the telecommunications sector, 3 October 2019; author's interview with T5, member of the telecommunications sector, 29 October 2019; author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G3, UK government official, 8 November 2019.

[109] Medin and Louie, 'The 5G Ecosystem', p. 29.

Network segmentation (or segregation) is an accepted measure for ensuring resilience in existing networks.[110] This paper has highlighted the work done by standards bodies to support the separation of different layers of the network.[111] While operators cannot guarantee that they have prevented attackers from moving between layers, they can make it much more difficult, time-consuming and resource-intensive.[112] Further, the more hurdles an attacker has to surpass to move between layers, the more likely it is that the attacker will eventually be found.[113]

Redundancy ensures that no function relies on a single component or set of components. If a part of the network fails, another portion of the network can perform the intended task.[114] For example, if a malicious actor were able to shut down all of one vendor's base stations within an urban area, base stations from another vendor would be able to pick up that traffic.[115] Redundancy ensures the network's consistent availability. Vendor diversity also increases redundancy,[116] as a range of equipment is less likely to fail in the same way at the same time.[117] Interviewees emphasised that operators should never rely on a single vendor.[118] In fact, using diverse equipment makes it easier to spot unusual behaviour from one particular vendor.[119] Interoperable equipment that can work with similar equipment from other vendors also creates an extra layer of security.[120]

As mentioned, the current lack of 5G vendor diversity creates further difficulties for countries planning to introduce a blanket ban on the participation of specific vendors. If regulation requires operators to use at least two different vendors in their RAN, as the UK has proposed for 5G (and

[110] 5G Americas, 'The Evolution of Security in 5G', July 2019, <https://www.5gamericas.org/wp-content/uploads/2019/07/5G_Americas_5G_Security_White_Paper_Final.pdf>, accessed 29 January 2020; author's interview with T1, member of the telecommunications sector, 27 September 2019.

[111] 3GPP, 'Release 15'.

[112] Author's interview with UK G3, UK government official, 8 November 2019.

[113] Author's interview with T3, member of the telecommunications sector, 3 October 2019.

[114] Author's interview with UK G1, UK government official, 29 October 2019; author's interview with T3, member of the telecommunications sector, 3 October 2019; author's interview with T5, member of the telecommunications sector, 29 October 2019.

[115] Author's interview with UK G3, UK government official, 8 November 2019.

[116] DCMS, *UK Telecoms Supply Chain Review Report*, p. 26; author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019.

[117] Author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019.

[118] DCMS, *UK Telecoms Supply Chain Review Report*, p. 26; author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019.

[119] Author's interview with UK G3, UK government official, 8 November 2019.

[120] Author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G4, UK government official, 11 November 2019.

as is already the case for 4G), Ericsson and Nokia would automatically have guaranteed market shares for 5G components.[121] This could remove incentives for either company to increase product quality and security, increasing the risk to 5G networks.[122]

In the longer term, governments should think about how they might cultivate more vendors to increase network diversity.[123] This may require governments to develop targeted investment schemes to enable diversification or leverage its procurement power.[124] Initiatives promoting interoperability, such as OpenRAN, may also help lower barriers to market entry. OpenRAN is a group of companies trying to make it technically possible for different vendors' equipment to interoperate in the RAN.[125] However, such initiatives face serious challenges. Even if interoperability is feasible, it may not yet be economically viable.[126] While creating long-term market diversity is an important aim, it will take a long time to achieve.[127]

Measure 2: Access Management

To secure 5G networks, operators must closely regulate and supervise vendor access to the network.[128] Software update mechanisms, particularly when vendors have remote access, are a prime attack vector.[129] In some cases, the companies providing maintenance or patching support are the original product vendors. Alternatively, the operator might perform the maintenance itself or outsource it to a subcontractor. A concern is that operator facilities could be staffed with insiders working at the behest of hostile state actors.[130] The location of the facility could be in China, the UK or elsewhere. The threat still remains.[131]

Access controls could include supervising vendors while they are in the network and limiting the amount of time that vendors have access to it.[132] Some interviewees argued this should

[121] Author's interview with UK G7, UK government official, 21 November 2019.

[122] Author's interview with UK G3, UK government official, 8 November 2019.

[123] Author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019.

[124] DCMS, *UK Telecoms Supply Chain Review Report,* pp. 41–42.

[125] Telecom Infra Project, 'OpenRAN', 2019, <https://telecominfraproject.com/openran/>, accessed 13 December 2019.

[126] Author's interview with UK G7, UK government official, 21 November 2019.

[127] Author's interview with T5, member of the telecommunications sector, 29 October 2019.

[128] Author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019; author's interview with UK G3, UK government official, 8 November 2019; author's interview with T5, member of the telecommunications sector, 29 October 2019.

[129] Levite, 'ICT Supply Chain Integrity'.

[130] Author's interview with UK G3, UK government official, 8 November 2019.

[131] *Ibid.*; author's interview with UK G1, UK government official, 29 October 2019.

[132] Author's interview with UK G4, UK government official, 11 November 2019.

include the tracking of outsourcing to ensure confidence in a vendor's equipment.[133] For many, network access is the strongest justification for banning vendors where confidence is low in their equipment.[134]

Other experts argue that any risk of vendors accessing the network is manageable.[135] If operators keep close control over the process and use the proper protocols and procedures, anyone should be able to provide this support without jeopardising the network.[136] As one government official pointed out, an operator's inability to monitor any vendor's access to the network would be a significant problem for security.[137] Certainly, the supply chain vulnerabilities discussed above apply both to vendors and individuals performing maintenance and patching functions.[138]

In either case, some level of access management and monitoring is a critical component of 5G network security. Such control should significantly decrease the risk of a vendor abusing authorised access to either exploit existing vulnerabilities or insert backdoors.

Measure 3: Testing and Monitoring

Testing and monitoring are critical 5G safeguards.[139] They create yet another hurdle for anyone looking to install a backdoor or leave a bug door.[140] Because of the frequent patching in software-based networks, testing must persist throughout the full lifecycle of components. This guards against backdoors or accidental vulnerabilities. Because it is impossible to exhaustively test every piece of equipment, particularly as patches are issued, testing must be random and continuous.[141]

[133] Author's interview with UK G1, UK government official, 29 October 2019.

[134] Gilding, '5G Choices'.

[135] Author's interview with T5, member of the telecommunications sector, 29 October 2019; author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019; author's interview with UK G6, UK government official, 30 October 2019; author's interview with UK G7, UK government official, 21 November 2019.

[136] Author's interview with T5, member of the telecommunications sector, 29 October 2019.

[137] Author's interview with UK G4, UK government official, 11 November 2019.

[138] Author's interview with UK G3, UK government official, 8 November 2019.

[139] Author's interview with UK G1, UK government official, 29 October 2019; author's interview with UK G7, UK government official, 21 November 2019; author's interview with T5, member of the telecommunications sector, 29 October 2019.

[140] Author's interview with T1, member of the telecommunications sector, 27 September 2019; author's interview with T3, member of the telecommunications sector, 3 October 2019.

[141] Author's interview with T3, member of the telecommunications sector, 3 October 2019; author's interview with A1, academic expert, 15 October 2019.

In addition to testing, operators must monitor network activity.[142] Though technically challenging, monitoring helps pinpoint unusual behaviour that may indicate malicious activity. Governments and operators are continuing to work on better methods to monitor network traffic.[143]

Some argue that the tools for monitoring and managing 5G systems have not kept pace with the advancements in the technology itself.[144] However, one of the benefits of 5G is that as it is virtualised, it can leverage superior testing and monitoring tools from other sectors, rather than being limited to an inferior single proprietary product.[145] Regardless, operators should continue to invest in improving the tools available to monitor, test and manage 5G networks, in the knowledge that technology will continue to evolve at pace.

Measure 4: Strong Cyber Security Standards

Although obvious, it is important to clearly state that a strong approach to cyber security policy and practice is a fundamental component of the protection of 5G networks. This applies to companies producing 5G technology as well as to cyber security professionals operating it. A number of the measures identified elsewhere in this section contribute to strong cyber security, but in addition, basic cyber security principles – like effective IT asset management, keeping patching up to date, deploying effective firewalls and other protection and detection measures, and employing staff with the right skills to implement cyber security – need to be implemented effectively. These are the fundamentals of security protection.

Measure 5: Banning Certain Components in Certain Parts of the Network

In certain circumstances, banning technology from a source where there is not the highest degree of confidence in security from inclusion in the most sensitive parts of a network is a legitimate risk-mitigation approach. In the UK, the NCSC has stated that using Huawei's equipment in the core of a 5G network creates unacceptable risks to the network.[146] In some countries, such as France, the government must authorise the vendors used in certain sensitive geographic areas, including the capital.[147] Some states' criteria may include a company's technical performance, while others may be based on economic or geopolitical factors. The Prague Proposal is one effort to standardise these criteria.[148]

[142] Author's interview with T5, member of the telecommunications sector, 29 October 2019.

[143] Author's interview with T1, member of the telecommunications sector, 27 September 2019.

[144] Author's notes from a techUK event, 30 September 2019.

[145] Author's interview with UK G3, UK government official, 8 November 2019.

[146] Martin, 'Ciaran Martin's CyberSec Speech in Brussels'.

[147] Raphaël Balenieri, 'Sécurité des réseaux : la France hésite face à Huawei', *Les Echos*, 25 November 2018, <https://www.lesechos.fr/tech-medias/hightech/securite-des-reseaux-la-france-hesite-face-a-huawei-150171>, accessed 5 September 2019.

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

Standard cyber risk management requires the identification of ‘crown jewels’: that data or those parts of an operational capability that must be protected at all costs, and where the least level of risk can be accepted. In a communications context, for example, a country could decide that the core technology in its systems to provide top-secret intelligence or military communications should not come from a supplier based in a country with a track record of hostile cyber action and where the links between the technology provider and its government are opaque. As discussed elsewhere in this paper, the conclusion that the integrity of the entire network would be unacceptably compromised, even if a single component is derived from a particular Chinese company, is highly unlikely from a technical risk-management perspective. However, banning technology from a certain vendor from sensitive parts of a network is a realistic risk-management measure.

Interviews raised four factors that could impact a country’s decision on whether to use a certain vendor’s 5G infrastructure: geographic location; cyber security experience; vendor availability; and cost. In some countries, geography and population density mean that more critical layers of the network may need to be more spread out. This would make these layers more vulnerable.[149] There are also questions of cyber security knowledge and experience – the UK has unique experience working with vendors and operators to test equipment.[150] Vendor availability also varies between countries: Samsung is a fourth viable RAN vendor in much of North America and the Asia-Pacific, but not in Europe.[151] For the UK, a pragmatic risk-management approach makes most sense because of its experience in understanding Huawei equipment, the geographical spread of its infrastructure and its level of risk tolerance at this present time.

National contexts and risk tolerance matter when making this decision. Ultimately, risk management using technical measures is the most appropriate policy to mitigate most cyber risks to 5G networks. As this paper demonstrates, there are multiple ways to localise and isolate cyber risk. These methods were used for previous generations of telecommunications equipment, and, as 5G is evolutionary, not revolutionary, past approaches remain applicable. However, for some states, political and economic factors may ultimately supersede technical risk-management assessments. In this context, states must be clear about the extent to which political or economic, rather than technical, factors inform their decision-making relating to 5G. Otherwise, the credibility of technical authorities will be seriously undermined.

[149] Author’s interview with UK G1, UK government official, 29 October 2019; author’s interview with UK G3, UK government official, 8 November 2019. If a base station has a range of 30 km, you are going to need many more to cover rural Wyoming, for example, than you would for a densely populated area like London.

[150] Huawei Cyber Security Evaluation Centre (HCSEC), ‘Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board: Annual Report 2019’, March 2019.

[151] Author’s interview with UK G7, UK government official, 21 November 2019.

UK and EU 5G Risk-Management Measures

On 28 January 2020, the UK announced its approach to HRVs in 5G networks (see Measure 5).[152] The policy decision was to exclude HRV components from sensitive parts of all UK 5G networks. It is important to note that this is just one of the suggested cyber security measures listed in this paper – it is not the golden ticket to securing 5G networks. There is a lot more work to do to strengthen measures relating to network architecture, access management, testing and monitoring, and cyber standards (see Measures 1–4).[153] This will require robust guidance or regulations for telecommunications operators, backed up by strong technical and regulatory oversight. The UK's final decision relating to Huawei's role in 5G infrastructure is merely one step towards addressing the cyber security of its 5G networks.

Meanwhile, the EU has released its toolbox to mitigate risks to 5G networks. It includes guidance on a wide range of solutions for member states to implement. They relate to: supplier diversity and secure network architecture (Measure 1); strict access controls (Measure 2); continuous testing and auditing for operators (Measure 3); baseline security requirements (Measure 4) and assessing vendors' risk profiles (Measure 5).[154] The toolbox also underlines the importance of sharing best practices when implementing these measures and how approaches to 5G cyber security should depend on national context.[155] Furthermore, it is indicative of the growing role of governments in 5G network security.

Huawei and Cyber Security

Much of the public debate on the cyber security of 5G networks relates to the implications of the continued provision of 5G infrastructure components by Huawei. Research demonstrated that confidence in Huawei, both technical and political, is low. This section explains why.

Huawei has previously been accused of producing poor-quality equipment. The UK's Huawei Cyber Security Evaluation Centre (HCSEC), which has examined all of Huawei's equipment deployed in the UK for several years, concluded that the 'general software engineering and cyber security quality of the product continues to demonstrate a significant number of major defects'.[156] The report attributed this to poor processes, including a 'software component lifecycle management [which] revealed flaws that cause significant cyber security and availability risks'.[157] A cyber security firm, Finite State, also found that both Huawei hardware and software

[152] NCSC, 'NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks', 28 January 2020, <https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks>, accessed 31 January 2020.

[153] DCMS, *UK Telecoms Supply Chain Review Report*.

[154] NIS Cooperation Group, 'Cybersecurity of 5G Networks: EU Toolbox of Risk Mitigating Measures', January 2020, pp. 12–13.

[155] *Ibid.*, p. 13.

[156] HCSEC, 'Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board', p. 17.

[157] *Ibid.*, p. 16.

were significantly more likely to have flaws than other vendors' equipment.[158] Many of these vulnerabilities introduced a security threat.[159]

Experts worry that either backdoors or bug doors would allow Huawei to access user data or seriously affect the functionality of the network.[160] However, despite serious doubts about Huawei, no one has presented clear evidence that the company is deliberately installing backdoors or leaving bug doors in its equipment.[161] In the case of vulnerabilities found by HCSEC and Finite State, it is almost impossible to prove whether or not vulnerabilities arise from poor engineering or malicious actions. However, the NCSC has stated it does not believe the defects found are a result of Chinese state interference.[162]

In addition to questions about whether Huawei's equipment is technically sound, public discourse has considered the connections between Huawei and the Chinese government. There is no question that the Chinese government has a history of perpetrating hostile cyber acts, including espionage against its adversaries, including the US and the UK.[163]

Numerous reports have alleged that Huawei shares a close relationship with the Chinese government. Critics point to the company's financial and trading practices, which many believe to be unfair, as well as its personnel.[164] Huawei denies links with the Chinese government; however, its governance structure is extremely opaque.[165] Many of its employees, including its founder, also have close, long-term links with Chinese military and intelligence.[166] While Huawei is not the only technology company with links to its home government, it is the only major telecommunications infrastructure vendor with such close ties.[167]

[158] Finite State, 'Finite State Supply Chain Assessment: Huawei Technologies Co., Ltd.', FS-SCA1, July 2019, <https://finitestate.io/wp-content/uploads/2019/06/Finite-State-SCA1-Final.pdf>, accessed 23 July 2019, p. 2.

[159] *Ibid*.

[160] Author's interview with A1, academic expert, 15 October 2019.

[161] Atlantic Council, 'My Way or the Huawei: 5G at the Center of US–China Strategic Competition', 23 July 2019, <https://www.atlanticcouncil.org/blogs/econographics/my-way-or-the-huawei-5g-at-the-center-of-us-china-strategic-competition/>, accessed 11 December 2019.

[162] HCSEC, 'Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board'.

[163] Author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019; Levy, 'Security, Complexity, and Huawei'.

[164] There are many sources on this topic, which fall outside of the remit of this paper, including: Christopher Balding, 'Huawei Technologies' Links to Chinese State Security Services', SSRN, 5 July 2019, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3415726>, accessed 24 July 2019; Kania, 'Securing Our 5G Future'.

[165] Kania, 'Securing Our 5G Future'.

[166] Balding, 'Huawei Technologies' Links to Chinese State Security Services'.

[167] Levy, 'Security, Complexity, and Huawei'.

The legal environment in China also suggests that the Chinese government could share any access Huawei has to telecommunications networks. The Chinese 2017 National Intelligence and Cybersecurity Laws require firms to comply with demands from military or intelligence personnel and prohibit companies from disclosing any cooperation.[168] This legal regime is a broad-based framework enabling the Chinese authorities to make open-ended demands on companies like Huawei, potentially to include access to data or even that the company takes more active measures in relation to its operations.[169] The laws appear to lack the balancing measures such as independent judicial oversight or right of appeal that are a feature of Western, democratic legal regimes.[170]

While all the above evidence is open to interpretation, the pattern is clear. Huawei claims it is a normal, private company concerned about profit and respects the laws of the countries in which it operates.[171] It also denies that it is subject to the National Intelligence and Cybersecurity Laws.[172] However, Huawei's alleged behaviour to date leaves ample room for doubt.

In the UK, Huawei has been classified as a HRV. UK criteria to identify a HRV include: the vendor's strategic position in the UK and in other telecommunications networks; the quality and transparency of the vendor's engineering and cyber security; past behaviour and practices; the vendor's resilience; and the domestic state apparatus, laws and offensive cyber capabilities of the vendor's country of origin.[173] The associated risk-management framework states that any HRV will have a limited role in all UK networks (not just 5G), meaning that there are specified network functions where a HRV cannot have any presence. This includes all core functions such as security, operational support, management and authentication, virtualisation infrastructure, network monitoring, lawful intercept and any future 5G core functions.[174] Meanwhile, the proportion of HRV components in peripheral parts of UK 5G infrastructure should have a hard cap of 35% to allow for effective cyber security risk management.

Huawei is the only HRV in the UK that has a bespoke risk-management strategy.[175] For the recent UK National Security Council decision relating to Huawei and the overall 5G risk-management strategy to be effective over the next decade and beyond, the NCSC (and its partners) should: constantly review, monitor and update 5G cyber security measures where appropriate; continue to restrict HRV presence in CNI, government, military and intelligence

[168] Tanner, 'Beijing's New National Intelligence Law'.

[169] *Ibid.*

[170] Kania, 'Securing Our 5G Future'.

[171] Huawei, 'Who Owns Huawei', <https://www.huawei.com/en/facts/question-answer/who-owns-huawei>, accessed 28 January 2020.

[172] Tara Francis Chan, 'Huawei Hits Back at "Uninformed" Claims that China Can Force It to Spy on Other Countries', *Business Insider*, 27 June 2018.

[173] NCSC, 'NCSC Advice on the Use of Equipment from High Risk Vendors in UK Telecoms Networks'.

[174] As specified by 3GPP TS 23.501.

[175] Ian Levy, 'The Future of Telecoms in the UK', NCSC, 28 January 2020, <https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk>, accessed 31 January 2020.

systems; continue to work closely with operators who use components from HRVs; maintain a close working relationship with the HRV and test their equipment; and promote a robust regulatory environment. Finally, the UK government should develop a long-term strategy to increase vendor diversity, which would in turn allow operators to decrease reliance on HRVs in 5G infrastructure, and for other emerging technology. The UK's approach to managing risk from Huawei is unique. It will be judged on the number of cyber security incidents relating to 5G and the UK's ability to adapt to new 5G use cases and advancements without compromising cyber security.

The Role of Governments in 5G Cyber Security

Some experts believe that commercial incentives have failed to convince operators to take the necessary cyber security measures to protect 5G networks from the threats and risks discussed in this paper.[176] Governments have a vital role to play in safeguarding 5G networks.

Research indicated that organisation-level risk management is unlikely to change despite the widening reach of 5G. Mitigation measures such as redundancy and segregation are costly and require significant up-front expenditure.[177] And there are few financial incentives to prioritise security.[178] Cyber security measures are often very expensive and delay network deployment, potentially creating conflicting interests for the operators.[179] As private companies, telecommunications operators are worried about their profit margins and fiduciary responsibilities, but lax 5G cyber security is an increasing reputational risk.

For end users, the cyber security of 5G networks is not a pressing concern and the public does not seem willing to pay extra for a more secure cellular network.[180] Public cyber education and awareness is an enduring challenge.

This raises the questions as to what extent governments should take on a more interventionist approach to secure 5G networks. In the UK, the government has taken on an advisory role but to date has largely allowed telecommunications companies to make their own decisions

[176] Author's interview with UK G3, UK government official, 8 November 2019; author's interview with UK G4, UK government official, 11 November 2019.

[177] Author's interview with T1, member of the telecommunications sector, 27 September 2019; author's interview with UK G3, UK government official, 8 November 2019.

[178] DCMS, *UK Telecoms Supply Chain Review Report*, p. 4; author's interview with T3, member of the telecommunications sector, 3 October 2019.

[179] DCMS, *UK Telecoms Supply Chain Review Report*, p. 12.

[180] Levy, 'Security, Complexity, and Huawei'; Harris Interactive, 'Consumer Internet of Things Security Labelling Survey Research Findings', March 2019, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798543/Harris_Interactive_Consumer_IoT_Security_Labelling_Survey_Report.pdf>, accessed 29 January 2020, p. 7. According to this report, only half of consumers consider security features to be important when buying smart end user devices.

about which vendors to use and how to design 5G networks. This approach should change. The UK Supply Chain Review identified a lack of supply chain diversity and recommended that regulations enforcing telecommunications cyber security must be strengthened.[181] This would represent a shift in approach if acted upon, and could lead to more prescriptive and rigorous guidance for operators. Meanwhile, as previously mentioned, the EU has recommended a toolbox of measures that member states can implement to secure their networks.[182] These types of measures should go a long way to creating better incentives for the private operators to prioritise national security and take the necessary measures to protect this critical national infrastructure.[183]

This paper has highlighted the challenges around the lack of sovereign technology options in certain cases, and also the lack of vendor diversity more generally. Both these issues raise significant challenges that go well beyond the narrow confines of cyber risk management. Rather, they are issues of industrial strategy. Governments are currently seeking ways to incentivise or influence industry to address these gaps. Many, including the UK, are starting to look hard at whether there are technology areas where a sovereign capability is essential, and if so, how to enable that.[184] In addition, there is increasing enthusiasm for governments to look more broadly at how to encourage greater vendor diversity. Both these issues go well beyond 5G.

Finally, the 5G debate is not just about cyber security – this has implications for the role of governments in technology. Companies have become embroiled in a geopolitical debate that undoubtedly requires state intervention. Some research interviewees were hesitant to discuss 5G or declined to speak specifically about Huawei. Even governments are finding the issue difficult to navigate. Relations between the US and China are strained and, consequently, many states have delayed decisions on their approaches to 5G security.[185] National approaches to

[181] DCMS, NCSC and Jeremy Wright, 'Government Plans to Safeguard the Future Security of UK Telecoms', press release, 22 July 2019, <https://www.gov.uk/government/news/government-plans-to-safeguard-the-future-security-of-uk-telecoms>, accessed 28 January 2020.

[182] European Commission, 'Secure 5G Networks: Questions and Answers on the EU Toolbox', 29 January 2020, <https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127>, accessed 31 January 2020.

[183] Author's interview with T1, member of the telecommunications sector, 27 September 2019; author's interview with T4, member of the telecommunications sector, 7 October 2019.

[184] The need for the UK to pursue sovereign capabilities in cyberspace is discussed in greater detail in the following publications: Cabinet Office, 'National Cyber Security Strategy 2016–2021', 13 September 2016, <https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf>, accessed 29 January 2020, p. 47; Cabinet Office, 'National Security Capability Review', March 2018, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/705347/6.4391_CO_National-Security-Review_web.pdf>, accessed 29 January 2020, p. 16; Sam Jones, 'Ministry of Defence Steps Up Cyber Security Operations', *Financial Times,* 1 April 2016.

[185] Written evidence submitted by RUSI for the Joint Committee on the National Security Strategy's inquiry, 'Ensuring Access to "Safe" Technology'.

5G security and other emerging technologies will continue to be geopolitical in nature for the foreseeable future, even if that does not necessarily make networks any safer.[186]

[186] Wheeler and Williams, 'Keeping Huawei Hardware Out of the US Is Not Enough to Secure 5G'.

III. Conclusions

RECENTLY, THERE HAS been considerable debate on national approaches to 5G cyber security. Research conducted for this paper has evidenced that:

- 5G networks have inherent vulnerabilities. As a policy priority, **governments should implement appropriate technical cyber risk-management measures that protect against most risks**. In doing so, it must be noted that no network will ever be 100% secure and no vendor can guarantee 'trustworthy' equipment. Instead, all equipment should be assessed on a scale of confidence. Banning any particular vendor, such as Huawei, will not fully address the issue of cyber risk in 5G networks and does not automatically make 5G networks safer. And the financial costs associated with such a ban may be significant.
- **Approaches to 5G security should depend on national context, including the geographic location of equipment, national cyber security experience, vendor availability and cost**. In some instances, this may result in a ban in sensitive parts of 5G networks, but this should depend on the risk tolerance of the state at the time.
- **Governments should explore how to better incentivise operators and private companies to prioritise the cyber security of 5G networks** over their commercial considerations and explore ways to improve public education and awareness about cyber security and 5G, and other emerging technology. Regulation, backed up by suitably skilled and resourced regulators, is likely to be a critical part of this.
- **Policymakers and practitioners should seek to maintain the distinction between sensitive and non-sensitive parts of a 5G network when assessing approaches to 5G cyber security**, even if this division is slightly blurred. 5G is not a technology where every component is of instrumental importance to network security and there are multiple ways to isolate and localise the risk.
- Political and economic considerations may be the overriding factors that lead to the decision to ban a particular vendor for some governments. This may be an entirely legitimate policy approach. **But governments must be clear about the extent to which political, rather than technical, factors inform their decision-making relating to 5G**. They should not seek to mask these political considerations with weak assertions about technical risk management.
- 5G is one instance of a much wider set of issues around the globalisation of technology and the pivot of technology innovation from western countries to Asia. This raises significant questions around national strategy in relation to vendor diversity and sovereign technology. **Governments should rapidly identify those advanced technology areas where greater vendor diversity and/or sovereign technology is required and develop an industrial strategy approach to address these gaps**.
- To safeguard telecommunications networks and other critical national infrastructure, **states should invest in further developing, supporting and implementing agreed-upon international cyber security standards**. This should include supporting global standards bodies and following secure-by-design principles.

About the Authors

Rebecca Lucas is a Research Analyst in Cyber Threats and Cyber Security. Her current research focuses on cyber security policy, including the globalisation of technology and associated national security risks. Her research interests also include the intersection of technological innovation, including cyber, and defence policy. Prior to this, Rebecca spent several years at Booz Allen Hamilton supporting clients in the defence science and technology sector. She holds an MA in Security Studies from Georgetown University and a BA in Political Science from Wellesley College. Rebecca is pursuing a MPhil/PhD in Defence Studies at King's College London.

James Sullivan is the Head of Cyber Research at RUSI. James joined RUSI from Deloitte's Cyber Risk team where he provided analysis on the cyber threat landscape and advised clients on cyber risk management strategies. Prior to this, James worked at the National Crime Agency as an Intelligence Analyst specialising in cybercrime threats. His research interests include cyber security, the spread of terrorism and violent extremism in cyberspace, online disinformation campaigns and the role of emerging technology in defence and security. He holds an MSc in Security Studies from University College London.

The authors would like to thank Conrad Prince CB for his valued advice on this paper. Conrad is a RUSI Distinguished Fellow and RUSI's senior adviser on cyber. Now an independent adviser on cyber security to a range of organisations in the private sector, from 2008–15 he was the Director General responsible for the intelligence and cyber operations conducted by Britain's signals intelligence and cyber security agency, the Government Communications Headquarters (GCHQ).

In March 2015, Conrad was appointed as the first UK Cyber Ambassador, a post he held until February 2018, when he left government service. He has an MPhil in International Relations and a BA (Hons) in History from Cambridge University.