

MARCH 2020



NSI

THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

THE RACE TO 5G: Securing the Win

By Andy Keiser*

NSI LAW AND POLICY PAPER

THE RACE TO 5G:

Securing the Win



THIS NSI LAW AND POLICY PAPER:

1

Describes the path and promise of 5G, the potential security implications therein, and United States and international policy responses as networks get deployed globally.

2

Evaluates the key issues at stake for U.S. national security and innovation in 5G.

3

Argues that the free market will provide better 5G security, and that the threat of Huawei and ZTE in the supply chain cannot be mitigated.

4

Proposes actionable recommendations to enhance 5G security, while promoting U.S. and Western-valued leadership in the telecommunications infrastructure needed to power transformative technologies key to America's economic and national security.



CONTENTS

02 EXECUTIVE SUMMARY

06 BACKGROUND ON 5G

13 KEY ISSUES AT STAKE

15 AUTHOR'S VIEWS

16 ACTIONABLE RECOMMENDATIONS

18 CONCLUSION

19 ENDNOTES

EXECUTIVE SUMMARY



Background On 5G

PATH & PROMISE OF 5G

- The advent of 5G will enable the digital economy of the future by connecting billions of devices as part of the internet of things (IoT) and enabling transformative technologies like autonomous vehicles and telemedicine, while bringing unforeseen innovations as well for adjacent discoveries.
 - China, Estonia, Japan, South Korea, Sweden, Turkey, and the United States are furthest along in deployment of 5G, although with limited service available. 25% of the mobile subscriptions in North America, and 10% in the Asia-Pacific region, are expected to be using 5G by 2022.
 - Huawei, Nokia, Ericsson, ZTE, and Samsung are leading 5G infrastructure providers in contracts awarded, patents, and R&D.

5G SECURITY

- 5G networks hold the promise for improved security through built-in standards and design, as well as improved use of encryption. We can also expect to see machine learning capabilities deployed to monitor and respond to threats, and the enhanced role of software solutions that allow for network operators, and therefore security threats, to be isolated through network slicing or virtualization.
 - 5G will undoubtedly pose new and expanded security risks due to dramatic increases in network devices and traffic, the accessibility of small cell infrastructure, and the growing reliance of devices and applications of all kinds that will be exposed at the network's edge.



U.S. & INTERNATIONAL POLICY RESPONSES

- The U.S. has embraced the “race to 5G” by aiming to push spectrum into the marketplace and help standardize small cell infrastructure deployment across the country.
 - Starting with a 2012 Congressional Report, the U.S. government has also been making clear its concerns regarding U.S. companies and allies working with Huawei and ZTE when it comes to 5G. In the last two years, the U.S. has banned the government’s use of Huawei and ZTE technology, added Huawei to the export controls Entity List, secured criminal indictments against Huawei, and conducted a diplomatic campaign to restrict Huawei from global 5G infrastructure.
 - While there is broad acceptance of the risks posed by Huawei, the international response has been mixed. U.S. allies Australia, New Zealand, and Japan have imposed effective bans on Huawei technology, while the UK will only restrict Huawei from “core” 5G infrastructure.



Key Issues At Stake

HOSTILE STATE THREATS

- In a 5G network relied on for critical economic and security functions, the integrity of the network and thus its supply chain becomes critical—highlighting the risk that could accompany the integration of Chinese national champions into critical 5G infrastructure.

THE STANDARDS RACE

- There is a threat that Huawei- and ZTE-manufactured gear could achieve a “first-mover” advantage and become a de facto international standard for 5G interoperability—a clear advantage to the Chinese government. China also aggressively worked to try to shape international 5G standards in their favor through standards bodies like 3GPP.



NATIONALIZATION OF THE 5G NETWORK

- In light of China's success and ambitions in developing global 5G infrastructure, and the importance of 5G to the U.S. economy and security, some have proposed either a government owned or operated network, or stringent regulation of security standards.

WHETHER HUAWEI AND ZTE RISKS CAN BE MITIGATED

- As the U.S. has demanded that Huawei be restricted from 5G infrastructure, some allies, most notably the UK, have considered different approaches to "mitigate" any security risks rather than fully banning Huawei's involvement.



Author's Views

FREE MARKET WILL PROVIDE BETTER SECURITY IN 5G

- Upending private sector-led efforts to deploy 5G would not only disrupt network developments well underway, but would likely cause significant delay while government policy, technical capabilities, and operational capacity was developed to manage an increased role in 5G infrastructure. Such a delayed effort, even if successful, would risk Chinese dominance in the 5G deployment and standards race.

THREAT OF HUAWEI & ZTE CANNOT BE MITIGATED

- Huawei and ZTE are part of China's strategic vision to dominate key sectors of the global economy including telecommunications and are beholden to the Chinese military and security services. While mitigation efforts may give some comfort to those host nations that employ untrustworthy vendor networks, they are not sufficient and are of limited effectiveness in a 5G environment.



**"HUAWEI AND ZTE ARE PART OF
CHINA'S STRATEGIC VISION TO
DOMINATE KEY SECTORS OF
THE GLOBAL ECONOMY..."**



Actionable Recommendations

ENSURE U.S. AND ALLIED 5G SUPPLY CHAIN SECURITY

- **Fully implement the communications technology supply chain Executive Order**, which should lead to the Commerce Department formally banning the import of Huawei and ZTE products into the United States.
- **Condition intelligence sharing** on U.S. allies fully securing their telecommunications supply chain from Huawei and ZTE—making clear that mitigation centers are not sufficient to protect from the threat.
- **Incent alternative 5G vendors** by maintaining export controls and promoting the use of vendors domiciled in allied nations utilizing diplomatic pressure, public relations support, and U.S. financial incentives.

ESTABLISH SUPPORTIVE FEDERAL ROLE

- **Adopt a national strategy for 5G security** to ensure the resiliency of the infrastructure that will enable and become a dependency for many other critical infrastructure functions.
- **Secure the necessary spectrum** to ensure the United States has the right mix available to build out a viable, robust 5G network to allow the U.S. to win the race to 5G and reap the security benefits therein.
- **Share threat information** with private sector telecommunications companies from dedicated monitoring of 5G networks to ensure security concerns are being addressed.
- **Promote security internationally** through promoting a policy of security and quality of the 5G network ahead of merely a rush to be first.

SUPPORT PRIVATE SECTOR-LED EFFORT

- **Reject 5G nationalization** proposals such as those considered at the National Security Council to have the federal government seize and manage large swaths of federal spectrum.
- **Accelerate O-RAN R&D** funding into open radio access network (O-RAN) technology to promote a more secure, software-based virtualized platform, where Western companies currently have an advantage.

EXPAND THE DEFENSE INDUSTRIAL BASE TO TELECOMMUNICATIONS INFRASTRUCTURE

- **Issue a Presidential Determination on telecommunications infrastructure** to expand Defense Industrial Base authorities and provide a range of financial tools to support the maintenance of domestic telecommunications technology essential to 5G and subsequent generations.

BACKGROUND ON 5G



» The Path & Promise Of 5G

ROUTING TO 5G

- **Zero Generation (0G)** refers to the first, early wireless technology that included push-to-talk technology.¹ 0G technology was primarily used in cars beginning in Chicago in 1946 through the early 1980's.² Its use required an operator to make connections.³
- **First Generation (1G)** mobile wireless communications were launched in Japan in 1979, and later in Nordic countries and the United States.⁴ This mobile technology was analog and supported voice calls only but no longer required an operator.⁵
- **Second Generation (2G)** mobile launched in the 1990's and was a digital technology that supported text messaging.⁶ It was first launched with a Global System for Mobile Communications (GSM) standard in Finland in 1991.⁷
- **Third Generation (3G)** mobile technology was first launched in Japan in 2001 following 15 years of standards development by the International Telecommunications Union (ITU).⁸ Though slow in adoption, 3G created the first mobile internet.⁹
- **Fourth Generation (4G)** mobile technology and 4G Long Term Evolution (LTE) and LTE Advanced networks were first introduced commercially in Sweden and Norway in 2009.¹⁰ With its higher download and upload speeds, 4G created an environment that allowed things such as the application and gig economy to flourish.¹¹
- **Fifth Generation (5G)** mobile technology will revolutionize the economy with the fastest ever network speed and throughput—as high as 100 times faster than 4G, and even as fast or faster than broadband.¹²
 - It is said that 1G brought the world the cell phone, 2G brought text messaging, 3G created the mobile internet and 4G enabled the application economy and mobile video streaming to flourish.
 - The advent of 5G will enable the digital economy of the future by providing lightning-fast internet connections, connecting billions of devices as part of the internet of things (IoT),¹³ and enabling transformative technologies like autonomous vehicles and telemedicine, while bringing unforeseen innovations as well for adjacent discoveries.¹⁴



5G DEPLOYMENT

- All four major United States mobile wireless carriers have deployed full 5G services in specific cities.¹⁵
- According to Ericsson, 74% of the mobile subscriptions in North America will be using 5G by 2025, and 56% in the North East Asia region.¹⁶
- Countries furthest along in broad deployment of 5G include China, Estonia, Japan, South Korea, Sweden, Turkey, and the United States.¹⁷ Despite certain question marks for each, all of these nations currently have limited service available, but plan for broad deployment later this year.¹⁸

PROVIDER COMPETITION

- **Infrastructure Deployment.** Huawei has claimed to have won at least 90 commercial 5G contracts,¹⁹ though skeptics claim this number could include advanced LTE buildouts. Nokia has announced 68 commercial 5G deals,²⁰ while ZTE claims 25,²¹ Ericsson has announced 81,²² and Samsung has six.²³
- **Patents and R&D.** Patents and research and development of course represent, at least in part, the core building blocks for securing the innovation that leads to key market share in a critical technology.
 - Among infrastructure providers, Huawei has the most patents for 5G technologies at 1,554, followed by Nokia at 1,427, Samsung at 1,316, ZTE at 1,208, and Ericsson with 819.²⁴
 - Huawei spent \$15.3 billion on total research and development (R&D) in 2018,²⁵ while Nokia and Ericsson spent \$4.6 billion and \$4.1 billion respectively.²⁶ Samsung plans to invest \$22 billion in 5G technology and other tech fields over three years.²⁷ ZTE plans to spend \$2.1 billion on 5G R&D.²⁸



**“5G WILL ENABLE
THE DIGITAL ECONOMY
OF THE FUTURE.”**

» 5G & Security

SECURITY BENEFITS OF 5G

- **Security In Design.** Commercial 5G networks in the U.S. are the first mobile network to have security built in from the beginning as part of the standards process.²⁹ 5G networks will integrate layers of security from the centralized core out to the radio access network and to virtual networks.
 - 5G will be the most secure wireless network infrastructure built to date, though the vast amount of newly-connected devices brings its own security challenges not seen in previous generations of networks.³⁰ In recent surveys, mobile operations have ranked security as nearly as important as increased network capacity and throughput in their 5G network planning.³¹
- **Improved Encryption.** 5G will utilize Public Key Infrastructure (PKI) for encryption more readily than 4G network operators.³² PKI refers to the foundation of security principles that include encryption, signatures, authentication, and certificates.³³
 - 5G will also utilize International Mobile Subscriber Identity (IMSI) encryption to mask a cellphone's unique user identifier before it is sent to the 5G mobile network—protecting against cyber criminals and other malicious actors.³⁴
- **Reduced Latency.** The fact that 5G will lower latency also presents security opportunities.³⁵ Encryption tools generally lower access speed by introducing an additional step, so parties often forgo using encryption in the interest of maintaining faster systems. The reduction in latency then should mean the increased use of encryption and overall improved security.

EMERGING SECURITY SOLUTIONS IN 5G

- **Artificial Intelligence.** Machine learning is likely to play an important role in the cybersecurity of the 5G network as threats become more complicated and the amount of data overwhelms the capacity for humans to protect against them. Numerous companies are promoting proprietary machine learning software to deal with cyber threats in 5G.³⁶
- **Network Slicing.** Network slicing refers to isolating operators from one another while using one piece of infrastructure.³⁷ Network slicing, or network virtualization, will also be prominent in 5G, providing primarily software companies a greater potential role than they had in previous generations of mobile networks. Software-based 5G network slice-as-a-service would necessarily rely on artificial intelligence to monitor for anomalies.³⁸
 - Breaking up the networks into smaller, manageable slices will allow operators to isolate threats through compartmentalization, remove infected portions from the rest of the network, and give operators more visibility and control over network traffic and threats.³⁹

- **Diameter protocol?** While aspirational, some security experts hope that the move to 5G will promote the use of the Diameter protocol, which is an international standard used to authenticate and authorize communications and the exchange of data between internet-based software applications on mobile networks and is more resilient to attacks.⁴⁰ It contains more reliable, secure, and flexible options for the movement of data on mobile networks.⁴¹

SECURITY RISKS FROM 5G

- **Volume.** Security threats are expected to increase exponentially as 5G technology is more widely adopted.⁴² AT&T, for example, currently sees 11 billion security incidents per day and expects such incidents to increase to five billion every 10 minutes with the adoption of 5G as hundreds of millions of more connected devices come onto the network.⁴³
- **Internet of Things (IoT) and DDoS Attacks.** By 2022, companies are expected to spend \$5 trillion on IoT devices, infrastructure, and adoption.⁴⁴ In 2021, there will be a projected 22.5 billion IoT devices,⁴⁵ up from 6.6 billion in 2016.⁴⁶ This influx of new devices creates the potential for massive bots being banded together to launch nefarious global cyber-attacks.⁴⁷ Another risk is increased potential to direct a disruptive surge in network traffic.⁴⁸
 - Distributed denial-of-service (DDoS) attacks are not problems inherent with 5G technology as such attacks are already occurring.⁴⁹ However, with increased bandwidth and available targets (IoT devices), the efficacy of DDoS attacks may increase with the adoption of 5G technology.⁵⁰
- **Small Cell Accessibility.** What sets 5G small cells apart from traditional infrastructure is not just their size. 5G technology relies, in part at least, on high frequency spectrum that can't travel as far as low frequency spectrum that is used for 3G/4G/LTE data.⁵¹ This requires persistent repeaters to relay information. The accessibility of small cell devices raises its own threats.
 - For example, the ultra-portability of small cells means they could be placed on top of light poles and other similar fixtures, making it easier for hackers to place fake small cells across a city just as they place fake traditional antennas which can harvest and access user data.
 - Small cell technology may also lower the barrier to entry for adversaries because of cost and accessibility.
 - Cisco, however, believes that the potential to drive up adoption of encryption/decryption in 5G will ameliorate the risk from rogue cell sites.⁵²
- **Reliance On Connectivity.** The increase in connected devices will inevitably create increased dependencies on this infrastructure, and poorly secured devices may be prone to exploitation. For instance, a power outage could cause devices such as cars to be inoperable because of network connectivity errors if they rely completely on cloud-based operations.
 - Additionally, due to the large amounts of personal and potentially sensitive data being transmitted, transmission of this information out at the network's edge presents a whole new potential opportunity for hackers. Many have noted that stringent data privacy regulations and compliance will be required both in the U.S. and globally to ensure protections for consumer data.⁵³

» U.S. Policy Responses


SECURING 5G

- **Curtailing Huawei & ZTE.** A 2012 Congressional report singled out Huawei as a national security threat⁵⁴ and the United States government has made clear its concerns regarding U.S. companies working with certain foreign companies, including Huawei and ZTE, when it comes to 5G.⁵⁵
 - In 2018, President Trump signed a bill banning the government's use of Huawei and ZTE technology, as well as certain additional telecommunications and video surveillance equipment from Chinese telecommunications companies.⁵⁶
 - The Commerce Department also added Huawei to its Entity List, which, despite a series of waivers to the restriction being granted, has significantly restricted U.S. exports to Huawei.⁵⁷
 - The U.S. has also been warning allies about using Huawei in 5G,⁵⁸ and has briefed many other countries including India, which is currently grappling with ways to restrict Huawei from their 5G network.⁵⁹
 - The Department of Justice (DOJ) unsealed two cases of criminal charges against Huawei in early 2019.⁶⁰ One indictment dealt with Huawei allegedly stealing intellectual property from T-Mobile while the other detailed Huawei's alleged sanctions violations with Iran.⁶¹
 - In February 2020, DOJ indicted Huawei and four subsidiaries with 16 counts of racketeering and theft of trade secrets.⁶²
 - These cases are being used to buttress the case with allies that using Huawei for 5G is unwise.⁶³
- **Supply Chain Security.** In May 2019, President Trump issued an Executive Order on "Securing the Information and Communications Technology and Services Supply Chain"⁶⁴ that was followed in November by a rule proposed by the Department of Commerce to effectively prohibit imports that pose a security risk from "foreign adversaries."⁶⁵ It is expected this framework may eventually lead to the ban of all imports of Huawei and ZTE products into the U.S.⁶⁶
 - These authorities would go beyond 2018 reforms to CFIUS via the Foreign Investment Risk Review Modernization Act (FIRRMA), which allowed for the review of national security risks posed by foreign investments in new areas such as real estate acquisitions in sensitive areas, private equity investments, and joint ventures acquiring sensitive technologies.⁶⁷
 - Congress is putting its own pressure on the Administration when it comes to 5G security with the Secure 5G and Beyond Act of 2019, which requires the President to develop a strategy to ensure the security of the 5G network.⁶⁸
 - The legislation, which moved through committee in the House and Senate in late 2019, has a domestic component in seeking to protect the supply chain of U.S. 5G networks and a foreign component of seeking to promote secure solutions with U.S. allies and partners as they build out their own 5G networks.⁶⁹

- Congress also recently passed legislation to fund a \$1 billion “rip and replace” effort to remove legacy Huawei and ZTE infrastructure from small telecommunications networks in the U.S. and replace them with trusted equipment. The legislation was signed into law by the President in March of 2020.⁷⁰

PROMOTING 5G DEPLOYMENT

- **Presidential Memorandum.** President Trump has adopted a self-described “America First” approach to 5G wireless—directing his administration to develop a “sustainable spectrum strategy” to become the leading innovator in 5G wireless technologies.⁷¹ Trump signed a presidential memorandum on October 25, 2018 which created the White House Spectrum Strategy Task Force to coordinate an assessment of federal spectrum needs and the development of a National Spectrum Strategy that includes recommendations to improve spectrum management and spectrum access for federal and private users.⁷²
 - The goal of this task force is ultimately to ensure both that there is enough spectrum to handle the growing amount of internet data and that it can be shared and stored safely. 5G cannot be brought to reality in the U.S. or anywhere else unless proper spectrum is made available.⁷³
 - In remarks from April 2019, President Trump stated, “The race to 5G is a race America must win, and it’s a race, frankly, that our great companies are now involved in. We’ve given them the incentive they need. It’s a race that we will win.”⁷⁴
- **Spectrum Policy.** The FCC is pursuing a plan called FAST (Facilitate America’s Superiority in 5G Technology).⁷⁵ This strategy’s goal is to push more spectrum into the marketplace—including high-frequency mmWAVE, midband, and lowband—update infrastructure policy, and modernize outdated regulation to enable the U.S. to have the best chance of “winning the race to 5G.”⁷⁶
 - This oft-cited goal has the security benefit of first-mover advantage. If the U.S. deploys 5G more quickly and broadly than China or Russia, it will be in a better position to benefit Western suppliers, dictate standards and write the rules of the road. Should China achieve broad adoption first, the converse is true.⁷⁷
 - In a September 2018 declaratory ruling, *Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Investment*,⁷⁸ the FCC set out “federal standards for small cell deployment regulation that aim to streamline the roll-out of 5G services across state and local governments” meant to address the rapid proliferation of municipal and state measures governing 5G infrastructure deployment.⁷⁹
 - On April 12, 2019, President Trump and FCC Chairman Ajit Pai announced plans to further 5G adoption through its third 5G spectrum auction on December 10th, and a Rural Digital Opportunity Fund meant to accelerate the deployment of gigabit-speed rural broadband infrastructure.⁸⁰
 - On February 6, 2020, FCC Chairman Pai announced a plan for a public auction of a large swatch of valuable midband spectrum for the purpose of 5G.⁸¹ The plan was approved on a 3-2 vote by the FCC on February 28 and the auction is planned for December.⁸²



» International Response

- **Australia** effectively blocked Huawei and ZTE from providing equipment for its 5G network under 2018 security guidelines, citing security concerns with entities “likely to be subject to extrajudicial directions from a foreign government.”⁸³

- **The European Parliament**, in a non-binding shot at Chinese telecommunications providers, adopted a resolution in early 2019 calling on member states and European Union agencies to ensure that European 5G networks meet strict security standards.⁸⁴

- **Germany** is continuing to wrestle with how to shape its regulatory framework and whether to establish insurmountable hurdles for firms such as Huawei and ZTE from being selected to build out Germany’s 5G networks.⁸⁵

- **Japan** has effectively banned purchases of Huawei and ZTE products.⁸⁶

- **The Netherlands** has not explicitly prevented the participation by Huawei in its coming 5G network,⁸⁷ but security concerns are at the forefront of the process and the government is reportedly investigating hidden backdoors built in telecommunications networks by Huawei.⁸⁸

- **New Zealand** blocked Huawei from that country’s 5G build out, apparently citing “serious national security risks.”⁸⁹

- **NATO** began looking seriously at 5G security when “representatives from Canada, France, Germany, the Netherlands, Sweden, the United States, and the United Kingdom participated in an Exploratory Team investigating national interest in researching Fifth Generation (5G) COMMS and MIMO Challenges in Electronic Warfare.”⁹⁰ This exploratory team created a Research Task Group to follow developments and investigate the impact of key 5G technologies on NATO cyber systems.⁹¹
 - American officials have recently pleaded to key members of NATO about refusing to work with Huawei over security concerns,⁹² and Poland has been calling for a joint EU-NATO stance on Huawei after a spying arrest in January 2019.⁹³

- **The United Kingdom** announced that it would prohibit “high risk vendors” Huawei and ZTE from its country’s 5G “core,” but would allow it in its “edge” of the network at the radio.⁹⁴ This was a blow to U.S. diplomatic efforts at the highest levels that had sought an outright ban. U.K. officials point to cybersecurity operations centers to mitigate Huawei or ZTE cybersecurity threats.⁹⁵

KEY ISSUES AT STAKE



» Hostile State Threats

- **Network Integrity.** In a 5G network relied on for critical economic and security functions, and where vast amounts of data are traveling at lightning-speed, one needs to be able to trust the integrity of the network, and thus trust the supply chain used to develop and operate that network infrastructure.
 - The core of the debate about potential limits to Huawei and ZTE building out 5G networks internationally lies with a concern that they, like all companies domiciled in China, are beholden to the Chinese military and intelligence services upon request under Chinese law and that the expected U.S. reliance on 5G networks for critical functions therefore creates unacceptable levels of risk.
 - The Defense Innovation Board issued a report on “5G Risks and Opportunities for DoD,” which stated: “The 5G ecosystem will especially run the risk of including security vulnerabilities if China becomes the global leader supplying 5G infrastructure...”⁹⁶ It went on to state: “...even if the United States limits sales of Chinese products into the United States, DoD will still have to operate on foreign networks overseas that will likely be built with a Chinese supply chain.”⁹⁷
- **Economic Retaliation And Coercion.** China’s practiced policy of economic coercion—the promise of economic benefits and their denial—is being deployed to influence the outcome of this global debate.
 - As nations limit Huawei and ZTE’s participation in their 5G networks, the Chinese government is exerting massive pressure on countries that are considering vendor restrictions, including by threatening to withdraw from unrelated economic opportunities or close off market access.⁹⁸
 - This highlights China’s willingness to use economic leverage and the heightened risk that could accompany the integration of these national champions into critical 5G infrastructure.

» The Standards Race

- **First-Mover Advantage.** As Chinese manufacturers are furthest along in deployment, and given the Chinese Government has prioritized 5G, there is a threat that Huawei and ZTE manufactured gear could become a de facto international standard for 5G interoperability—a clear advantage to the Chinese government.⁹⁹
 - This “first-mover” advantage would be a clear disadvantage to Western interests as core telecommunications infrastructure is not compatible across different companies. Once Chinese, or Western telecommunications infrastructure for that matter, is imbedded in a network it becomes difficult and cost prohibit to remove.¹⁰⁰

- **Standards Bodies.** The Chinese have also aggressively worked to try to shape international 5G standards in their favor.¹⁰¹
 - The first official governance standard for 5G was released by 3GPP, which consists of seven national telecommunications standard development organizations, and is known as 5G NR.¹⁰²
 - Though there is debate about the efficacy of Chinese involvement in this international standards-making body, there is no question that they have placed a high level of priority on shaping 5G standards, which could present security challenges if they are successful.

» Nationalization of the 5G Network

- Some argue for a 5G network to be owned, operated and managed by the federal government. Under this construct, the government, primarily the Department of Defense, would lease existing spectrum that it holds to private sector telecommunications companies.¹⁰³
 - An alternative would call for stringent regulation of private sector telecommunications companies to meet and maintain robust and prescriptive cybersecurity requirements.
 - These proposals arise from concerns that the market-driven approach has left the U.S. behind competitors like China on 5G deployment,¹⁰⁴ or that the 5G network is too important to our economy and security to be managed by the private sector.¹⁰⁵
- In contrast, others believe the private sector will build a better, more resilient, more secure, and more cost-effective 5G network than the government could maintain—that the government lacks the expertise of the private sector to manage security across a complex network, or the right incentives to ensure continued investment in innovation and cyber security solutions.¹⁰⁶

» Whether Huawei & ZTE Risks Can Be Mitigated

- Canada, the United Kingdom and others have argued that the risk of Huawei and ZTE on their networks can be mitigated through the use of cyber security centers to monitor the traffic coming off of Huawei and ZTE gear in an effort to contain any nefarious activity.¹⁰⁷
- This approach is made more challenging in light of finding that Huawei technology is tainted by sloppy coding providing increased threat opportunities even if there was no mal intent.¹⁰⁸
- Given the technical challenges involved in ensuring security via an off-premise center testing questionable gear supporting a highly dynamic and remotely updated network such as 5G, vendor trust has become a critical factor.¹⁰⁹

AUTHOR'S VIEWS



Free Market Will Provide Better Security in 5G

- A government-run or even managed 5G network would delay deployment of 5G and dilute security.
- Upending private sector-led efforts to deploy 5G would not only disrupt network developments well underway, but would likely cause significant delay while government policy, technical capabilities, and operational capacity was developed to manage an increased role in 5G infrastructure. Such a delayed effort, even if successful, would risk Chinese dominance in the 5G deployment and standards race.
- It would also be plagued by similar problems to what has faced other government-run efforts in technology including the use of outdated technology and security, lack of innovation, duplication of effort, overlapping requirements, and a compliance rather than security-focused mindset.
- In a free-market driven network, security becomes a competitive imperative, giving advantage to providers that can demonstrate resilient and sustainable security sufficient for the range of critical economic and security activities expected to rely on 5G.
- There is clearly a role for the federal government in regulating the 5G network, including potential minimum-security requirements, as it does for all previous generations of mobile networks. However, room must be left for private sector innovation to meet rapidly developing technology solutions and a dynamic and expanding threat environment.



Threat of Huawei & ZTE Cannot Be Mitigated

- Huawei and ZTE are part of China's strategic vision to dominate key sectors of the global economy including telecommunications. Beholden to the Chinese military and security services, Huawei and ZTE are key enablers for Chinese influence and intelligence collection.
- Following a 2012 House Intelligence Report citing Huawei and ZTE as a national security threat,¹¹⁰ 23 federal criminal charges filed against Huawei by the Department of Justice last year for violating Iran sanctions and theft of trade secrets,¹¹¹ arrests in Poland of Huawei executives for espionage,¹¹² a 16 count racketeering and trade secret theft indictment earlier this year, a reported hacking of the African Union by Chinese telecommunications providers,¹¹¹ and reports that the Chinese military and intelligence services fund Huawei,¹¹³ there is little reason left to trust Huawei and ZTE in the 5G ecosystem despite their proclamations of independence from government control.
- While mitigation efforts may give some comfort to those host nations that employ untrustworthy vendor networks, they are not sufficient and are of limited effectiveness in a 5G environment.

ACTIONABLE RECOMMENDATIONS



1

ENSURE U.S. AND ALLIED 5G SUPPLY CHAIN SECURITY

- **Fully Implement Supply Chain EO.** Fully implement the May 15, 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain. This should lead to the Commerce Department formally declaring Huawei and ZTE products as a national security threat to the United States under the International Emergency Economic Powers Act (IEEPA) and ban their import into the United States.
- **Condition Intelligence Sharing.** Encourage U.S. allies around the world to fully secure their telecommunications supply chain from Huawei and ZTE. Make clear that cybersecurity mitigation centers are not sufficient to protect from the threat and that the U.S. will condition intelligence sharing on the trustworthiness of a country's telecommunications supply chain.
- **Incent Alternative Vendors.** Maintain Huawei on the export controls Entity List and promote the use of 5G vendors domiciled in allied nations that have strong democratic values and rule of law as alternatives to Huawei/ZTE with diplomatic pressure, public relations support, and U.S. financial incentives consistent with World Trade Organization obligations. Financing options from the Export-Import Bank of the United States, the Development Finance Corporation and other U.S.-government backed financing options should be made available to foreign countries looking to build secure 5G networks using Western-allied, secure vendors.

2

ESTABLISH SUPPORTIVE FEDERAL ROLE

- **Adopt A National Strategy.** The President should establish a national strategy for 5G security as called for in the Secure 5G and Beyond Act. As 5G will become the critical infrastructure that enables and becomes a dependency for many other critical infrastructure functions, its security requires a dedicated national strategy.
- **Secure Necessary Spectrum.** The FCC should ensure the United States has the right mix of spectrum available to build out a viable, robust 5G network to give the U.S. a chance to win the race to 5G and reap the security benefits therein. The FCC, for example, should move expeditiously to auction off the "C band" midband spectrum essential to having a 5G national network.

- 
- **Share Threat Information.** The Department of Homeland Security and the Federal Communications Commission, informed by the Intelligence Community, should closely monitor the deployment of 5G networks in the United States to ensure security concerns are being addressed. Threat information sharing from the government to private sector telecommunications companies should be enhanced in advance of deployment of this critical, national network.
 - **Promote Security Internationally.** Prioritize security in international fora and standards bodies through promoting a policy of security and quality of the 5G network ahead of merely a rush to be first. Governments that relegate security to the back burner can put broader international networks at risk.

3

SUPPORT PRIVATE SECTOR-LED EFFORT

- **Reject USG 5G.** Avoid the security temptation of to have the U.S. government run or manage the 5G network, and reject proposals such as those considered at the National Security Council to have the federal government seize and manage large swaths of federal spectrum in an effort to kick-start and secure 5G.
 - Protect and support the market-based, private sector led approach which will lead to a better, faster, safer network.
- **Accelerate O-RAN R&D.** Fund new research and development into open radio access network (O-RAN) technology at the U.S. National Laboratories and Technology Centers. Acceleration of this technology would help negate reliance on telecommunications hardware and promote a more secure, software-based virtualized platform, where U.S. and Western allied technology companies currently have an advantage.

4

EXPAND THE DEFENSE INDUSTRIAL BASE TO TELECOMMUNICATIONS INFRASTRUCTURE

- Expanding Defense Industrial Base authorities to address telecommunications infrastructure would help U.S. or allied manufacturers of telecommunications hardware to keep a Western or Western-allied manufacturing base in place similar to the how the U.S. Defense Industrial Base protects ship, tank and airplane manufacturing lines.
- Doing so via the Industrial Base Fund and the Defense Production Act's Title III would provide a range of financial tools to support the maintenance of domestic production capacity and supply of telecommunications technology essential to 5G and subsequent generations.
- Such a reform would create a government-ensured backstop to maintain critical private-sector production lines of things like 5G routers, switches and base stations.

CONCLUSION



- Broad deployment of a 5G network in the United States and around the globe will unleash transformative innovations and potentially improved cybersecurity if done correctly. The additional billions more of connected devices transmitting data at rates we haven't before seen presents tremendous opportunity to bring new innovations like automated vehicles to market.
- 5G also presents major cybersecurity challenges and creates new opportunities for hostile nation-state, terrorist and other hackers to conduct crippling cyber-enabled attacks if not properly protected.
- 5G also presents significant national security challenges if the standards and architecture is shaped or owned by hostile governments.
- A trusted supply chain is integral to providing a secure 5G network.



BROAD DEPLOYMENT
OF A 5G NETWORK IN
THE UNITED STATES
AND AROUND THE
GLOBE WILL **UNLEASH
TRANSFORMATIVE
INNOVATIONS AND
POTENTIALLY IMPROVED
CYBERSECURITY IF
DONE CORRECTLY.**

ENDNOTES

*Andy Keiser is a Fellow at the National Security Institute at the Antonin Scalia Law School at George Mason University and previously served, among other positions, as a Senior Advisor to the House Permanent Select Committee on Intelligence. Mr. Keiser also conducts cybersecurity consulting and federal lobbying for several companies, including in the telecommunications sector. This paper is solely the work of the author and does not necessarily represent the views of the National Security Institute or any other entity or individual.

- 1 *The Mobile Wireless Communication Technology Journey – 0G, 1G, 2G, 3G, 4G, 5G*, PROTEI (March 18, 2019), <http://protei.me/blog/telecom-news/the-mobile-wireless-communication-technology-journey/>.
- 2 *Id.*
- 3 Jean Gabriel Remy & Charlotte Letamendia, *LTE SERVICES* at xix (Pierre-Noël Favennec ed., John Wiley & Sons 2014).
- 4 Ai Sin Chan, *A brief history of 1G mobile communication technology*, Xoxzo (July 24, 2018), <https://blog.xoxzo.com/en/2018/07/24/history-of-1g/>.
- 5 *Id.*
- 6 Ai Sin Chan, *A brief history of 2G mobile communication technology*, Xoxzo (Aug. 1, 2018), <https://blog.xoxzo.com/en/2018/08/01/history-of-2g/>.
- 7 *Id.*
- 8 *The Evolution to 3G Mobile – Status Report*, ITU NEWS (Sept. 3, 2003), <https://www.itu.int/itunews/issue/2003/06/thirdgeneration.html>.
- 9 Ai Sin Chan, *A brief history of 3G mobile communication technology*, Xoxzo (Aug. 10, 2018), <https://blog.xoxzo.com/en/2018/08/10/history-of-3g/>.
- 10 David Meyer, *First '4G' services go live in Norway, Sweden*, ZDNET (Dec. 14, 2009), <https://www.zdnet.com/article/first-4g-services-go-live-in-norway-sweden/>.
- 11 DELOITTE, *THE IMPACT OF 4G TECHNOLOGY ON COMMERCIAL INTERACTIONS, ECONOMIC GROWTH, AND U.S. COMPETITIVENESS* 4 (2011); see also Brad Reed, *Better, faster, stronger: 4G's impact on app development*, Network World (Mar. 5, 2010), <https://www.networkworld.com/article/2203767/better-faster-stronger-4g-s-impact-on-app-development.html>.
- 12 Chris Hoffman, *What is 5G, and How Fast Will It Be?*, HOW-TO GEEK (Jan. 3, 2018), <https://www.howtogeek.com/340002/what-is-5g-and-how-fast-will-it-be/>.
- 13 PHILLIPPA BIGGS & YOLIA LOZANOVA, *BROADBAND COMM'N FOR SUSTAINABLE DEV., THE STATE OF BROADBAND: BROADBAND CATALYZING SUSTAINABLE DEVELOPMENT* (2017).
- 14 Eric Zeman, *What is 5G? A Guide to the Transformative Wireless Tech That's Being Hyped to Change Everything*, FORTUNE (Oct. 8, 2018), <https://fortune.com/2018/10/08/what-is-5g/>.
- 15 See Dan Jones, *5G in the USA: Going Mobile*, LIGHT READING (Feb. 23, 2019), <https://www.lightreading.com/mobile/5g/5g-in-the-usa-going-mobile/d-d-id/749627>.
- 16 Richard Möller, *Forecasts*, in ERICSSON, *ERICSSON MOBILITY REPORT 10* (Patrik Cerwall ed., Nov. 2019).
- 17 Jennifer Wills, *5G Technology: Which Country Will Be the First to Adapt?*, INVESTOPEDIA (Mar. 27, 2019), <https://www.investopedia.com/articles/markets-economy/090916/5g-technology-which-country-will-be-first-adapt.asp>.
- 18 *Id.*
- 19 Lauly Li and Cheng Ting-Feng, *HUAWEI CLAIMS OVER 90 CONTRACTS FOR 5G, LEADING ERICSSON, NIKKEI ASIAN REVIEW* (Feb. 21, 2020, 12:33 AM), <https://asia.nikkei.com/Business/China-tech/Huawei-claims-over-90-contracts-for-5G-leading-Ericsson>.
- 20 *5G in action*, Nokia, <https://www.nokia.com/networks/5g/5g-in-action/> (last visited Mar. 12, 2020).
- 21 *ZTE secures 25 5G commercial contracts*, ZTE (June 25, 2019), <https://www.zte.com.cn/global/about/news/20190625e2.html>.
- 22 *Ericsson 5G*, Ericsson, <https://www.ericsson.com/en/5g> (last visited Mar. 12, 2020).
- 23 Martha De Grasse, *Which vendor leads in 5G contracts?*, FIERCEWIRELESS (Sept. 13, 2019), <https://www.fiercewireless.com/5g/which-vendor-leads-5g-contracts>.
- 24 Tim Pohlmann, *Who is leading the 5G patent race?*, PREMIER CERCLE (May 28, 2019), <https://premiercercle.com/news/who-is-leading-the-5g-patent-race>.
- 25 *No Pay, No Gain: Huawei Outspends Apple on R&D for a 5G Edge*, BLOOMBERG (April 26, 2019, 5:35 AM), <https://www.bloomberg.com/news/articles/2019-04-25/huawei-s-r-d-spending-balloons-as-u-s-tensions-flare-over-5g>.
- 26 Iain Morris, *Huawei's \$800M 5G Budget Piles Pressure on Ericsson, Nokia*, LIGHT READING (Feb. 8, 2018), <https://www.lightreading.com/mobile/5g/huawei-s-800m-5g-budget-piles-pressure-on-ericsson-nokia/d-d-id/740427>.
- 27 Saheli Roy Choudhury, *Samsung to invest \$22 billion into new growth areas like A.I. and 5G*, CNBC (Aug. 8, 2018, 2:43 AM), <https://www.cnbc.com/2018/08/08/samsung-to-spend-22-billion-in-new-growth-areas-including-ai-and-5g.html>.
- 28 Kavitha Majithia, *ZTE aims to bag \$2B for 5G R&D*, MOBILE WORLD LIVE (Jan. 31, 2018), <https://www.mobileworldlive.com/featured-content/top-three/zte-aims-to-bag-2b-for-5g-rd/>.
- 29 See generally NAT'L RISK MGMT. CTR., *CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, OVERVIEW OF RISKS INTRODUCED BY 5G ADOPTION IN THE UNITED STATES* 7 (2019).
- 30 CTIA, *PROTECTING AMERICA'S NEXT-GENERATION NETWORKS* 3 (2018).
- 31 Monica Allevén, *With new 5G revenues come security concerns: survey*, FIERCEWIRELESS (May 6, 2019, 9:49 AM), <https://www.fiercewireless.com/wireless/new-5g-revenues-come-security-concerns-survey>.
- 32 PATRICK DONEGAN, *HEAVY READING, EVOLVING THE MOBILE SECURITY ARCHITECTURE TOWARD 5G* 9-10 (2017), <https://www.cisco.com/c/en/us/solutions/collateral/service-provider/mobile-internet/mobile-security-architecture-wp.pdf>.
- 33 *What is Public Key Infrastructure (PKI)?*, THALES, <https://www.thalesecurity.com/faq/public-key-infrastructure-pki/what-public-key-infrastructure-pki> (last visited Feb. 20, 2019).
- 34 John Marinho, *What's New in 5G Security? A Brief Explainer*, CTIA (June 12, 2019), <https://www.ctia.org/news/whats-new-in-5g-security-a-brief-explainer>.
- 35 It is expected that latency will drop a ping time of 50 to 80 milliseconds with today's 4G technology to a potential of a few milliseconds. DARRELL M. WEST, *THE FUTURE OF WORK: ROBOTS, AI, AND AUTOMATION* 44 (2018).
- 36 Adrian Jakobsson, *The 5G Future Will Be Powered By AI*, NETWORK COMPUTING (Mar. 14, 2019), <https://www.networkcomputing.com/wireless-infrastructure/5g-future-will-be-powered-ai>.
- 37 See Sacha Kavanagh, *What is Network Slicing? How Fast is 5G - 5G Speeds and Performance*, 5G.CO.UK (Aug. 28, 2018), <https://5g.co.uk/guides/what-is-network-slicing/>. The difference between future 5G tenancy and the current system with MVNOs can be described with the analogy of a pie. Tenancy slices the pie and each tenant may do as they wish with their slice. The current system takes the entire pie and without slicing it, allows each operator to take a bite from the pie.

- 38 VED P. KAFLE ET AL., NAT'L INST. OF INFO. AND COMM'C'N TECH., CONSIDERATION ON AUTOMATION OF 5G NETWORK SLICING WITH MACHINE LEARNING (2018); see also Emmanuel Dotaro, *5G Network Slicing and Security*, IEEE (Jan. 2018), <https://sdn.ieee.org/newsletter/january-2018/5g-network-slicing-and-security>.
- 39 See Phil Goldstein, *The Benefits of 5G Network Slicing in Public Safety*, STATETECH (Mar. 28, 2019), <https://statetechmagazine.com/article/2019/03/benefits-5g-network-slicing-public-safety-perfcon>.
- 40 For the past three decades, Signaling System 7 has been the standard for public switched telephony. Researchers at the European Union Agency for Network and Information Security (ENISA) stated (in 2016) that SS7 is still used as a legacy network when falling back to 2G/3G technologies while hoping that 5G technology adopts a new standard. EUR. UNION AGENCY FOR NETWORK AND INFO. SEC., SIGNALING SECURITY IN TELECOM SS7/DIAMETER/5G: EU LEVEL ASSESSMENT OF THE CURRENT SITUATION 4 (2018); see also Elad Yoran & Edward G. Amoroso, *The Role of Commercial End-to-End Secure Mobile Voice in Cyberspace*, 3 THE CYBER DEF. REV. 57, 60 (2018).
- 41 *What is Diameter Protocol?*, RIBBON, <https://ribboncommunications.com/company/get-help/glossary/diameter-protocol> (last visited Feb. 20, 2020).
- 42 NAT'L RISK MGMT. CTR., CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, OVERVIEW OF RISKS INTRODUCED BY 5G ADOPTION IN THE UNITED STATES 1 (2019).
- 43 5 key requirements for a secure 5G network, CISCO, https://www.cisco.com/c/m/en_us/network-intelligence/service-provider/digital-transformation/secure-5g-network.html (last visited Feb. 20, 2020).
- 44 IDC Forecasts Worldwide Spending on the Internet of Things to Reach \$745 Billion in 2019, Led by the Manufacturing, Consumer, Transportation, and Utilities Sectors, INTERNATIONAL DATA CORPORATION (Jan. 3, 2019), <https://www.idc.com/getdoc.jsp?containerId=prUS44596319>; Louis Columbus, 2018 Roundup Of Internet Of Things Forecasts And Market Estimates, FORBES (Dec. 13, 2018, 11:49 AM), <https://www.forbes.com/sites/louiscolumnbus/2018/12/13/2018-roundup-of-internet-of-things-forecasts-and-market-estimates/#560386327d83>.
- 45 Press Release, Gartner Inc., Gartner Identifies Top 10 Strategic IoT Technologies and Trends (Nov. 7, 2018) (on file with author).
- 46 Amy Nordrum, *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated*, IEEE SPECTRUM (Aug. 18, 2016), <https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated>.
- 47 Nicholas Shields, *Here's how 5G will revolutionize the Internet of Things*, BUSINESS INSIDER (Jun. 15, 2017, 10:15 AM), <https://www.businessinsider.com/how-5g-will-revolutionize-the-internet-of-things-2017-6>.
- 48 NGMN, 5G SECURITY RECOMMENDATIONS 7 (Remy Harel & Steve Babbage eds., 2016), <https://bit.ly/2TAQxRv>.
- 49 See generally *What is a Distributed Denial-of-Service (DDoS) Attack?*, CLOUDFLARE, <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/> (last visited Feb. 20, 2020) ("A distributed denial-of-service (DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. DDoS attacks achieve effectiveness by utilizing multiple compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. From a high level, a DDoS attack is like a traffic jam clogging up with highway, preventing regular traffic from arriving at its desired destination").
- 50 Michael Schachter, *DDoS & 5G: The Bigger the Pipe, the Stronger the Threat*, ALLOT (June 26, 2018), <https://www.allot.com/blog/ddos-5g-the-bigger-the-pipe-the-stronger-the-threat/>.
- 51 5G – A Few Frequency Facts, IDG COMMUNICATIONS, <https://www.cio.com/article/3226451/5g-a-few-frequency-facts.html>.
- 52 Donegan, *supra* note 24, at 10.
- 53 *Id.* at 7.
- 54 CHAIRMAN AND RANKING MEMBER OF THE PERMANENT SELECT COMM. ON INTELLIGENCE, 112TH CONG., INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE (2012).
- 55 Dean DeChiaro, Trump order clears path to ban Huawei 5G equipment from United States, ROLL CALL (May 16, 2019, 10:50 AM), <https://www.rollcall.com/2019/05/16/trump-order-clears-path-to-ban-huawei-5g-equipment-from-united-states/>.
- 56 Jacob Kastrenakes, Trump Signs Bill Banning Government use of Huawei and ZTE Tech, THE VERGE (Aug. 13, 2018, 6:33 PM), <https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump>.
- 57 Addition of Entities to the Entity List, 84 Fed. Reg. 22,961 (May 21, 2019) (to be codified at 15 C.F.R. § Pt. 744, Supp. 4).
- 58 Stu Woo & Kate O'Keeffe, *Washington Asks Allies to Drop Huawei*, THE WALL STREET JOURNAL (Nov. 23, 2018, 4:56 AM), <https://www.wsj.com/articles/washington-asks-allies-to-drop-huawei-1542965105>.
- 59 Rahul Satija, *India searching for a way to restrict Huawei in 5G*, NIKKEI ASIAN REVIEW (Mar. 7, 2019), <https://asia.nikkei.com/Spotlight/5G-networks/India-searching-for-a-way-to-restrict-Huawei>.
- 60 Julia Horowitz, *US Unveils Its Criminal Case Against Huawei, Alleging China Giant Stole Trade Secrets and Violated Iran Sanctions*, CNN (last updated Jan. 29, 2019, 4:33 PM), <https://www.cnn.com/2019/01/28/business/huawei-charges/index.html>.
- 61 *Id.*
- 62 Press Release, Dept. of Justice, Off. of Public Affairs, Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets (Feb. 13, 2020) (on file with author).
- 63 David McCabe et. al, *U.S. Charges Huawei With Racketeering, Adding Pressure On China*, THE NEW YORK TIMES (Feb. 13, 2020), <https://www.nytimes.com/2020/02/13/technology/huawei-racketeering-wire-fraud.html>.
- 64 Executive Order on Securing the Information and Communications Technology and Services Supply Chain, 2019 DAILY COMP. PRES. DOC. 310 (May 5, 2019).
- 65 Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65,316 (proposed Nov. 27, 2019) (to be codified at 15 C.F.R. § Pt. 7).
- 66 Stephanie Zable, *Huawei Technologies v. U.S.: Summary and Context*, LAWFARE (Apr. 9, 2019, 8:03 AM), <https://www.lawfareblog.com/huawei-technologies-v-us-summary-and-context>.
- 67 Stephanie Zable, *The Foreign Investment Risk Review Modernization Act of 2018*, LAWFARE (Aug. 2, 2018, 3:39 PM), <https://www.lawfareblog.com/foreign-investment-risk-review-modernization-act-2018>.
- 68 Secure 5G and Beyond Act of 2020, H.R. 2881, 116th Cong. (2019).
- 69 Secure 5G and Beyond Act, S. 893, 116th Cong. (2019). Available at <https://bit.ly/2T0nHLj>.
- 70 Secure and Trusted Communications Networks Act of 2019, H.R. 4998, 116th Cong. (2020).
- 71 Lucas Laursen, *Trump Sets Out to Apply His 'America First' Approach to 5G Wireless*, FORTUNE (Oct. 26, 2018, 6:46 AM), <https://fortune.com/2018/10/26/federal-government-wireless-spectrum-strategy-5g/>.
- 72 Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future, 2018 DAILY COMP. PRES. DOC. 730 (Oct. 25, 2018).
- 73 See *Trump Signs Order to Set US Spectrum Strategy as 5G Race Looms*, REUTERS (Oct. 25, 2018, 12:17 PM), <https://www.cnn.com/2018/10/25/trump-signs-order-to-set-us-spectrum-strategy-as-5g-race-looms.html>.
- 74 Remarks by President Trump on United States 5G Deployment, 2019 DAILY COMP. PRES. DOC. 223 (April 12, 2019).
- 75 The FCC's 5G FAST Plan, FCC, <https://www.fcc.gov/5G> (last visited Feb. 21, 2020).
- 76 *Id.*
- 77 Michael Chertoff et al., National Security and Winning the Race to 5G, REALCLEAR DEFENSE (May 2, 2019), https://www.realcleardefense.com/articles/2019/05/02/national_security_and_winning_the_race_to_5g_114386.html.

78 In the Matter of Accelerating Wireless Broadband Deployment by Removing Barriers to Infrastructure Inv., 33 F.C.C. Rcd. 9088 (2018).

79 Kendra Chamberlain, *5G Small Cell Deployment: Every Current State Laws*, BROADBAND NOW (Dec. 3, 2018), <https://broadbandnow.com/report/5g-small-cell-deployment-state-laws/>.

80 Fact Sheet from the Fed. Commc'ns Comm'n, FCC Chairman Pai Announces Major Initiatives to Promote U.S. Leadership on 5G and Connect Rural Americans to High-Speed Internet at White House Event (Apr. 12, 2019) (on file with the author).

81 Memorandum from the Fed. Commc'ns Comm'n, THE C-BAND: Repurposing Mid-Band Spectrum for 5G (Feb. 6, 2020) (on file with the author).

82 Press Release, FCC, FCC Acts to Free Up C-Band Spectrum for 5G Services (Feb. 28, 2020) (on file with author).

83 Joint Media Release, Dept. of Commc'ns and the Arts & Dept. of Home Affairs, Government Provides 5G Security Guidance To Australian Carriers (Aug. 23, 2018) (Austl.).

84 Emanuele Scimia, *EU Parliament wary of Huawei's 5G technology*, ASIA TIMES (Mar. 13, 2019), <https://asiatimes.com/2019/03/eu-parliament-wary-of-huawei-5g-technology/>.

85 Andreas Rinke & Holger Hansen, *With or without Huawei? German coalition delays decision on 5G rollout*, REUTERS (Dec. 17, 2019, 12:27 PM), <https://www.reuters.com/article/us-germany-china-huawei/with-or-without-huawei-german-coalition-delays-decision-on-5g-rollout-idUSKBN1YL22Z>.

86 *Japan to ban Huawei, ZTE from govt contracts-Yomiuri*, REUTERS (Dec. 6, 2018, 7:22 PM), <https://www.reuters.com/article/japan-china-huawei/japan-to-ban-huawei-zte-from-govt-contracts-yomiuri-idUSL4N1YB6JJ>.

87 *Netherlands to raise at least 900 million euros in first 5G auction*, REUTERS (Dec. 5, 2019, 4:52 AM), <https://www.reuters.com/article/us-netherlands-5g/netherlands-to-raise-at-least-900-million-euros-in-first-5g-auction-idUSKBN1Y90Z7>.

88 *Dutch spy agency investigating alleged Huawei 'backdoor': Volkskrant*, REUTERS (May 16, 2019, 5:14 AM), <https://www.reuters.com/article/us-netherlands-huawei-tech/dutch-spy-agency-investigating-alleged-huawei-backdoor-volkskrant-idUSKCN1SM0UY>.

89 Vicky Xiuzhong Xu, *New Zealand Blocks Huawei, in Blow to Chinese Telecom Giant*, THE NEW YORK TIMES (Nov. 28, 2018), <https://www.nytimes.com/2018/11/28/business/huawei-new-zealand-papua-new-guinea.html>.

90 *Fifth Generation (5G) COMMS and MIMO Challenges in Electronics Warfare*, NATO (Oct. 18, 2016), <https://www.sto.nato.int/SitePages/newsitem.aspx?ID=3475>.

91 *Id.*

92 *U.S. to discuss challenges posed by China, 5G with NATO allies*, REUTERS (Nov. 29, 2019, 1:16 PM), <https://www.reuters.com/article/us-nato-summit-usa-china/u-s-to-discuss-challenges-posed-by-china-5g-with-nato-allies-idUSKBN1Y326C>.

93 *Poland calls for 'joint' EU-Nato stance on Huawei after spying arrest*, THE GUARDIAN (Jan. 12, 2019, 8:50 AM), <https://www.theguardian.com/world/2019/jan/12/huawei-sacks-chinese-worker-accused-of-spying-in-poland-wang-weijing>.

94 *New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity*, GOV.UK (Jan. 28, 2020), <https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity>.

95 Demetri Sevastopulo & David Bond, *UK says Huawei is manageable risk to 5G*, FINANCIAL TIMES (Feb. 17, 2019), <https://www.ft.com/content/619f9df4-32c2-11e9-bd3a-8b2a21d90d5>.

96 MILO MEDIN & GILMAN LOUIE, DEF. INNOVATION BD., THE 5G ECOSYSTEM: RISKS & OPPORTUNITIES FOR DoD 23 (2019).

97 *Id.*

98 Sanjeev Miglani & Neha Dasgupta, *Exclusive: China warns India of 'reverse sanctions' if Huawei is blocked – sources*, REUTERS (Aug. 6, 2019, 9:10 AM), <https://www.reuters.com/article/us-huawei-india-exclusive/exclusive-china-warns-india-of-reverse-sanctions-if-huawei-is-blocked-sources-idUSKCN1UW1FF>.

99 Henny Sender, *US-China contest centres on race for 5G domination*, FINANCIAL TIMES (June 18, 2019), <https://www.ft.com/content/d3072b76-90e9-11e9-aea1-2b1d33ac3271>.

100 CTIA, THE GLOBAL RACE TO 5G 5 (2018), <https://api.ctia.org/wp-content/uploads/2018/04/Race-to-5G-Report.pdf>; Jeremy Hsu, *How the U.S. Can Prepare to Live in China's 5G World*, IEEE SPECTRUM (Apr. 23, 2019, 8:30 PM), <https://spectrum.ieee.org/tech-talk/telecom/standards/how-america-can-prepare-to-live-in-chinas-5g-world>.

101 Todd Shields and Alyza Sebenius, *Huawei's Clout Is So Strong It's Helping Shape Global 5G Rules*, BLOOMBERG (Feb. 1, 2019, 4:00 AM), <https://www.bloomberg.com/news/articles/2019-02-01/huawei-s-clout-is-so-strong-it-s-helping-shape-global-5g-rules>.

102 Ryan Whitwam, *The first real 5G wireless standard is official*, ANDROID POLICE (Dec. 21, 2017), <https://www.androidpolice.com/2017/12/21/first-real-5g-wireless-standard-official/>.

103 Jonathan Swan et al., *Scoop: Trump team considers nationalizing 5G network*, AXIOS (Jan. 28, 2018), <https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html>.

104 Newt Gingrich, *If China Dominates 5G, It Will Control The Future*, NEWSWEEK (Feb. 22, 2019, 5:19 PM), <https://www.newsweek.com/newt-gingrich-if-china-dominates-5g-they-will-control-future-opinion-1335767>.

105 Rebecca Kheel & Ellen Mitchell, *Pentagon fears losing race for 5G to China*, THE HILL (Sept. 25, 2018, 6:00 AM), <https://thehill.com/policy/defense/408181-pentagon-fears-losing-race-for-5g-to-china>.

106 Jim Baker, *5G Networks Must Be Secure and Reliable*, LAWFARE (Mar. 13, 2019, 10:31 AM), <https://www.lawfareblog.com/5g-networks-must-be-secure-and-reliable>; Mike Rogers, *Getting real about Huawei*, THE HILL (Mar. 12, 2019, 3:00 PM), <https://thehill.com/opinion/technology/433696-getting-real-about-huawei>; Brendan Carr, *Nationalizing 5G Is Not the Way to Beat China*, NATIONAL REVIEW (Mar. 5, 2019, 3:10 PM), <https://www.nationalreview.com/2019/03/nationalizing-5g-is-not-the-way-to-beat-china/>.

107 See Rory Cellan-Jones, *Huawei risk can be managed, say UK cyber-security chiefs*, BBC NEWS (Feb. 18, 2019), <https://www.bbc.com/news/business-47274643>.

108 HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD, ANNUAL REPORT TO THE NATIONAL SECURITY ADVISER, AT 3, 25 (UK); Raymond Zhong, *China's Huawei Is at Center of Fight Over 5G's Future*, THE NEW YORK TIMES (Mar. 7, 2018), <https://www.nytimes.com/2018/03/07/technology/china-huawei-5g-standards.html>.

109 Nadarajah Sethurupan, *5G security a 'positive step forward': U.S. official*, NORWAY NEWS (Apr. 10, 2019, 10:20 PM), <http://www.norwaynews.com/5g-security-a-positive-step-forward-u-s-official/>.

119 Chairman, *supra* note 46.

111 Rachel Brown & Preston Lim, *Department of Justice Unseals Two Indictments Against Huawei*, LAWFARE (Feb. 6, 2019, 1:59 PM), <https://www.lawfareblog.com/sinotech-department-justice-unseals-two-indictments-against-huawei>.

112 Charles Reilly & Antonia Mortensen, *Huawei fires employee arrested in Poland on spying charges*, CNN BUSINESS (Jan. 12, 2019, 10:34 AM), <https://www.cnn.com/2019/01/11/tech/poland-huawei-exec-arrest/index.html>.

113 John Aglionby et al., *African Union accuses China of hacking headquarters*, FINANCIAL TIMES (Jan. 29, 2018), <https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5>.

114 John Fingas, *CIA claims Huawei is funded by Chinese state security*, ENGADGET (Apr. 20, 2019), <https://www.engadget.com/2019/04/20/cia-claims-huawei-funded-by-chinese-state-security/>.



NSI

THE NATIONAL SECURITY INSTITUTE
At George Mason University's Antonin Scalia Law School

THE NATIONAL SECURITY INSTITUTE

Antonin Scalia Law School | George Mason University
3301 Fairfax Dr. Arlington, VA 22201 | 703-993-5620

NATIONALSECURITY.GMU.EDU

