March 2021

Balancing the Promise and the Peril of 5G:

The State of Play in the United States

Author
Melissa K. Griffith
Public Policy Fellow
Woodrow Wilson
International Center
for Scholars

5G BEYOND BORDERS

This series is a product of the 2020 5G Beyond Borders Workshop organized by:

Centre for International Governance Innovation

Wilson Center

Escuela de Gobierno y Transformación Pública
Tecnológico de Monterrey

Acknowledgments

This policy brief is a contribution to a workshop focusing on the future of 5G in North America. The 5G Beyond Borders workshop, organized by the Wilson Center, Centre for International Governance Innovation (CIGI), and Tecnológico de Monterrey, aimed to discuss how strategic cooperation at the North American level can directly shape the future of 5G and lay the groundwork for expanded North American competitiveness in a range of emerging technologies. One primary goal of the workshop was to help lay the foundations for a broader North American Technology Trust. Thank you to the Science and Technology Innovation Program (STIP), the Canada Institute, and the Mexico Institute at the Woodrow Wilson Center and to the Centre for International Governance Innovation and Tecnológico de Monterrey. I also owe a debt of gratitude to the individuals who shared their experiences, expertise, and insights with me in person and virtually over the course of this project. Special thanks go to Robert Fay, Sophie Goguichvil, Meg King, Elizabeth Newbury, and Spencer Stucky for their feedback and comments on the first draft and during the editing process.

Cover image: Shutterstock/ By Blue Planet Studio

Key Points:

1. While much of the public discussion is tinged with a sense of immediacy, the full potential, or promise, of 5G will not be realized in the short term. It is important to recognize that the next-generation of telecommunications – its architectures and applications – is still nascent and actively evolving.

2. 5G networks are a necessary but not a sufficient condition for the future many 5G proponents readily promise. That promise depends on an ecosystem of technologies including artificial intelligence, cloud computing, and robotics.

3. If we wish to see a diverse, innovative, and secure 5G ecosystem, the U.S. needs to widen its policy aperture and give the broader set of concerns the same political weight and voice given to Huawei and ZTE. Developing a more robust and comprehensive assessment of the U.S.'s 5G risk profile, one that is not predominantly focused on China and untrusted vendors, will help to set policy priorities and identify gaps in the current U.S. approach to national security concerns.

4. Current U.S. lines of effort remain deeply siloed and underdeveloped. At both the national and international level, shared concern needs be replaced by sustained and comprehensive policy action.

Table of Contents

1. Introduction

When you inquire into the current United States (U.S.) national security landscape for the fifth generation (5G) of cellular networks, a common story frequently emerges:

> 5G will power the fourth industrial revolution. Therefore, as a matter of national security, we cannot allow untrusted vendors (often used as a proxy for Chinese companies like Huawei and ZTE) to dominate or play a significant role within this critical infrastructure. And yet, concerningly, the U.S. is currently engaged in a 'race with China' over the development and deployment of 5G: a 'race' we are at risk of losing.

Sound familiar? Although most often presented as one cohesive 5G story by policy makers, industry leaders, and researchers alike, imbedded within this story are actually three related but distinct lines of argument about the promise and peril of 5G.

1. ***5G will power the fourth industrial revolution.*** In short, it will form the backbone of the new digital economy and drive economic growth over the first half of the twenty-first century.

2. ***Therefore, as a matter of national security, we cannot allow untrusted vendors to dominate or play a central role within this critical infrastructure.*** In other words, who builds, deploys, and maintains the 5G ecosystem will have unique opportunities for espionage through and disruption of this infrastructure and will, therefore, have a direct and negative impact on our national security going forward.

3. ***And yet, concerningly, the U.S. is currently engaged in a 'race' with China over the development and deployment of 5G: a 'race' we are at risk of losing.*** Put another way, if we want to benefit from 5G without significantly compromising our national security, our companies need to win, now and in the future (though the concept of winning and the specifics of the race itself remain poorly defined).

The distinctions between and the character of each of these lines of argument matter for policy. The first presents an argument about the promise of 5G; the second identifies an important peril associated with the specific development, deployment, and maintenance of 5G at home and abroad; and the third offers an assessment of the current state of play (framed as a race we are at risk of losing).

Rather than take each of these popular lines of argument as fact, we must instead take seriously the questions each of these statements implicitly seek to answer: (1) what benefits does 5G promise and (i.e. why the hype), (2) what types of national security concerns arise (i.e. why worry), and (3) where does the U.S. stand in terms of addressing those concerns while pursuing the promise (i.e. how far along is development and deployment in the U.S. and what steps has the U.S. taken so far to address the corresponding security concerns). Importantly, this approach illustrates how the common American refrain oversimplifies the issues at stake and, in so doing, overlooks core sets of national economic and security concerns and their corresponding policy options.

By breaking the American 5G story down into these constituent parts, four important, yet frequently underexamined, realities emerge.

First, 5G may power a fourth industrial revolution, but it will not and cannot do so alone. Companion technologies such as artificial intelligence (AI), cloud computing, robotics, and the further evolution of the Internet of Things (IoT) are equally as important for this transformation. As are questions of policy, such as the regulatory environments in which these technologies find themselves. In short, 5G networks are a necessary but not a sufficient condition for the future many 5G proponents readily promise.

Second, while it is true that 5G is already being deployed within the U.S., this statement can be misleading. We have not yet realized the full potential of 5G, nor are we likely to do so in the short term. Why? There remain significant unknowns about 5G in practice. We are currently in the process of developing and deploying core foundations and these foundations vary across vendors and locations. We are further off still from witnessing the emergence of the range of applications or use-cases 5G promises to make possible: such as the explosion of connected devices that would enable remote surgeries and fleets of driverless cars. Moreover, just as 4G led to the previously unimagined "app economy," 5G will lead to applications not yet understood.

Third, the U.S.'s 5G security focus has heavily leaned toward national security concerns that stem from 'untrusted vendors' in our networks at home and abroad, a term that has widely become shorthand for two Chinese companies in particular: Huawei and ZTE. To the U.S.'s detriment, this focus has not been accompanied by and has, in fact, drowned out the importance of a broader risk management strategy. Untrusted vendors represent a significant national security concern. But, equally important are the concerns for American security that extend beyond China's role in the development and deployment of 5G technology.

Fourth, the pressing policy question is not, 'are trusted vendors better than untrusted vendors?'. They are. Instead, the relevant question is two-fold: what are the range of national security concerns associated with 5G (of which untrusted vendors is only one concern) and what steps can the U.S. take, alone or cooperatively with other states, to mitigate this broader category of risk (of which banning untrusted vendors is only one option)? Ultimately, given the breadth and character of national security concerns that should inform the development of specific policy solutions in 5G, no single policy initiative will be adequate. In complex ecosystems, there are no geostrategic silver bullets. The 5G problem the U.S. faces will require a cohesive and multifaceted set of coordinated responses.

With these four takeaways in mind, this policy brief proceeds in four parts. First, I examine the promise of 5G, including its potential benefits and how it differs from cellular networks of today. Second, I examine the current state of 5G in the U.S., which includes infrastructure deployment, spectrum allocation, and use-cases. Third, I examine the peril of 5G, including the national security risks stemming from both untrusted vendors and the risks intrinsic to 5G networks regardless of specific vendors. Fourth, I conclude with an overview of three current strains of U.S. 5G security efforts before summarizing the main policy takeaways.

2. The Promise of 5G: Why the Hype?

5G, the "fifth generation" of mobile network technology, represents an important evolution and, in some respects, transformation of telecommunications networks and, as a consequence, will serve as an important foundation upon which industries compete and generate value, people communicate and interact, and militaries pursue security for their citizenry.

To illustrate the promise of 5G for the U.S., this section serves three purposes. First, it explains how 5G differs from prior telecommunications networks; second, it lays out the anatomy of a 5G network; and third, it illustrates how 5G is best understood as part of a broader technology ecosystem.

2.1. The Transformation of Telecommunications Networks

What is the benefit of developing and deploying 5G networks? In the most basic sense, 5G brings with it significant increases to bandwidth and the number of connections while decreasing latency. These changes are not trivial. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) estimates that 5G will support 100x faster download speeds, a 10x decrease in latency, and 100x the network capacity in comparison to existing 4G LTE networks.[1] In plain English, 5G means faster connections and larger capacity.

Yet, the promise of 5G lies not in what it is, but in what it enables. More specifically, and heading into some jargon heavy territory, there are three core functions of 5G that set it apart from the networks of today.

First, 5G facilitates **Enhanced Mobile Broadband (EMBB)**, which represents a marked improvement to the speed of existing mobile networks through significant increases in bandwidth. Fundamentally, however, EMBB is best understood as an improvement in functionality and not a transformation that enables novel use-cases in the future. For example, this shift will enable faster streaming of digital content, but it will not radically transform the types of digital content users are interacting with on their devices. Moreover, for most current use-cases, there is limited benefit to dramatically higher speeds.[2] Yet, EMBB will also be the first benefit users experience as 5G networks are deployed. Why? Unlike the subsequent two functionalities of 5G networks, it does not require similarly substantial investments in new telecommunications infrastructure.

Second, **Ultra-Reliable Low-Latency Communications (URLLC)** allows for near real-time interconnectivity (significantly reducing the lag between requesting and receiving information to seemingly instantaneous connections). This second functionality sets 5G networks fundamentally apart from today's mobile networks. Supported by the possibility of edge computing, which reduces latency by bringing compute capabilities closer to the end-user within the network,[a] URLLC is essential for many of the novel use-cases 5G promises. These include "full car automation, factory automation, and remote-controlled surgery where reliability and responsiveness are mandatory."[3]

Third, the increased network capacity of 5G networks will enable **Massive Machine Type Communications (MMTC).** 5G's MMTC lies at the heart of realizing the full potential of the Internet of Things (IoT) and, like URLLC, it is essential for many of the novel use-cases 5G promises. Driverless cars, automation and roboticization of factories and agriculture, remote-controlled surgeries, and commercial and military drone-swarms all rely on the ability to bring billions of end-user devices and sensors, which communicate amongst themselves and other parts of the network, online.

2.2. The Anatomy of a Telecommunications Network

If the aforementioned three core functions are what will set 5G functionally apart from the networks of today, what does a 5G network actually look like in practice?

[a] merging the "core" and the "periphery."

While it is important to note that 5G networks are deployed by operators and taken together these different networks comprise a broader 5G ecosystem, there are three commonly understood components of telecommunication networks in general and 5G networks in particular: (1) end-user devices, (2) the radio access network (RAN - sometimes referred to as the periphery), and (3) the core network.

In its simplest form,

1. end-user devices connect through
2. specialized antennas to modems in base stations (the RAN converts radio signals from end-user-devices through cells mounted on cell towers into data traversing terrestrial network cables and satellites) to other cell towers or to
3. the core network infrastructure (and vice versa). The core authenticates services, connects different parts of the access network, and routes data between end-user-devices and other components of the network.[4]

Notably, the specific deployments and configurations of 5G networks will impact all three components and their relationship to each other. For example, the New Radio (NR) standard for 5G can adapt to a wider range of use-cases than prior 4G LTE networks supported. This allows the number and type of connected devices to multiply to include not just mobile devices but vehicles, industrial robots, military drones, and virtual/augmented reality (VAR) devices. Other changes include the RAN transitioning to cloud-based radio processing; the RAN incorporating smaller cells atop a greater number of cell towers connected to each other and the core via satellite or fiber; and edge-based computing in telecommunications networks, which challenges the functional distinctions between the core and the periphery of the network.

2.3. Placing 5G within the Broader Technology Ecosystem

Taken together – EMBB, URLLC, and MMTC – represents an important transformation of telecommunications networks and represents a key enabler for a fourth industrial revolution/*Industrie 4.0* (i.e. the digitization of manufacturing and other production processes) as well as how states will pursue security for their citizenry in the future (i.e. the utility of 5G networks for national security purposes at the operational and tactical levels such as drones and command and control).

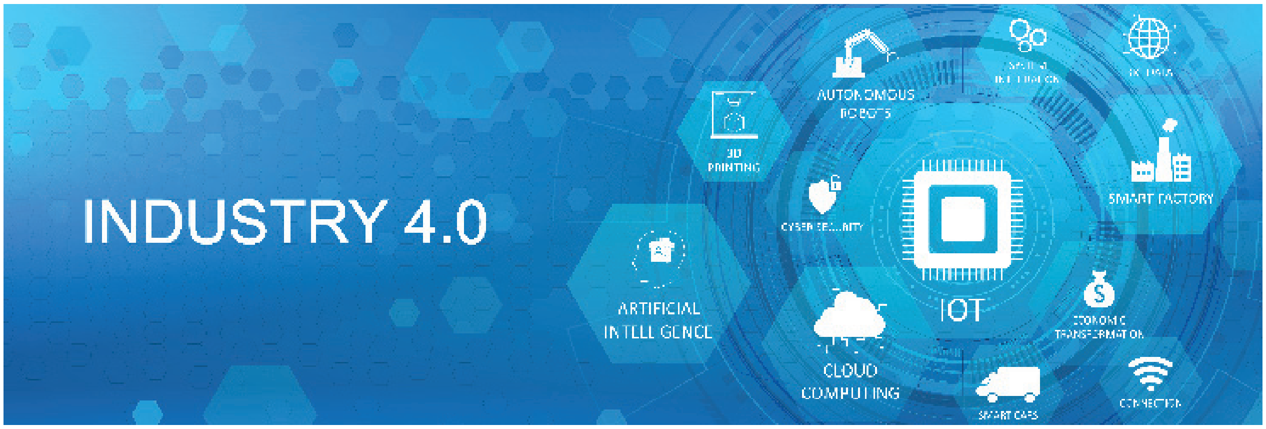

Image source: Shutterstock.com/ By Mari Kova

Notably, however, the use-cases 5G enables also rely on companion technologies such as cloud computing, machine learning (specific purpose AI), and robotics. The promise of 5G rests at the intersection of a series of technological advances and innovations, of which 5G forms a critical infrastructure backbone. Put another way, the wider promise of this ecosystem rests not just on the connectivity that 5G brings, but on the promise of intelligent connectivity, tools, and systems more broadly.[5]

Take AI, as just one example. As connected end-user devices proliferate and the functionality of the core and RAN become increasingly software-defined and customizable, AI will be an essential tool through which to manage that increasing complexity across the network. AI, however, will also benefit from the vast amounts of data (big data) that 5G networks create. Recall, data is one of the three foundations underpinning AI development and deployment alongside computational power and algorithms.

AI is not the only companion technology that will aid and benefit from 5G deployment. As Pat Gelsinger, the CEO of VMware, succinctly summarized, "[c]loud enables mobile connectivity; mobile connectivity creates more data; more data makes artificial intelligence better; AI enables more edge use-cases; and more edge needs more cloud for storage and compute."[6]

In conclusion, to realize the full promise – or hype – of 5G networks, each component of this broader ecosystem is necessary. Yet, this next-generation of telecommunications – its architectures and applications – is still nascent and actively evolving. 5G folds increasing virtualization, cloud computing, edge computing, machine learning, network slicing, and automation into not just a network that can support the Internet of Things, but a network that can support the Internet of Systems. This requires technical innovative solutions across the telecommunications stack - the Radio Access network, the core network, and end-user devices – but also innovative applications that are as of yet unknown. The promise of 5G will largely depend on how these systems are developed and deployed in practice, and not on what they could accomplish in theory.

3. The Current Status of 5G in the U.S.: Are We There Yet?

Given much of the recent coverage surrounding the buildout of 5G networks in the U.S. and around the world, it would be easy to assume that 5G is now fairly commonplace and widely used today. What is missing from this coverage, however, is a discussion about what counts as a 5G network. Notably, 5G remains a work in progress, both in terms of its development and in its deployments over time by various operators. Moreover, the novel use-cases 5G promises have not yet been realized while what may be the most novel of these use-cases remain largely unknown.

3.1. What Counts as 5G?

There are two different forms of 5G deployment: brownfield and greenfield. Brownfield deployments (also known as non-stand-alone (NSA (and no, not that NSA) networks) are built on top of existing networks. For incumbents in the market, brownfield deployments leverage prior investments and sunk costs as they transition to 5G. For most brownfield deployments in the U.S. and around the world, operators have focused their attention first on the RAN (primarily on radios, such as transitioning to the New Radio (NR) standard), while continuing to rely on the existing

4G LTE core.[7] This form of deployment is aided by technical standards, especially the widely implemented version of the Third Generation Partnership Project (3GPP)[b] standards known as Release 15 (R15).[8] R15 enabled brownfield deployments by focusing on interoperability between the new radio specifications for 5G and previous-generation networks.[9] In contrast to brownfield, greenfield deployments (also known as stand-alone (SA) networks) feature both a 5G RAN and a 5G core.[10] Here, standards remain in-progress. In fact, the awaited 2020 of Release 17 (R17) was delayed due to the realities of covid-19.[11]

So far, brownfield deployment has dominated rollout of 5G in the U.S. (i.e. operators have generally augmented existing infrastructure).[12] They have updated their radio interfaces but not, for example, broadly deployed or transitioned to cloud-based radio processing; small cell deployment, which places radios closer to end-users; or massive multiple-input multiple-out-put (MIMO), which would significantly increase the number of antennas at base stations and terminals.[13] In addition, these deployments have largely been centered on dense, urban areas while many rural carriers remain on legacies systems a generation behind 4G LTE (3G).[14]

However, not all operators are pursuing brownfield deployments. Dish - a relative newcomer to telecommunications unlike AT&T, T-Mobile, and Verizon - does not have an existing brownfield infrastructure from which to readily build. Instead, looking to replicate the early successes of Japan's Rakuten, Dish is investing in the development and then subsequent deployment of a SA (greenfield) network without relying on legacies systems to distribute the costs associated with the deployment of 5G.[15]

Functionally, why does the distinction between greenfield and brownfield matter? In the long-term, it will matter very little. In the short term, however, brownfield deployments have limited additional utility for end-users. While the brownfield deployments seen in the U.S. allow users to experience faster speeds (EMBB) promised by 5G, these deployments do not deliver on the full promise of 5G networks (URLLC and MMTC). Put another way, in order for the full potential of 5G to be unleashed, the current state of deployments will not be enough. A reality further cemented by the fact that few end-users across the U.S. currently have 5G-enabled devices.[16]

The availability of spectrum represents another potential constraint on the character and pace of deployment. Notably, while the Federal Communications Commission (FCC) has made significant gains in releasing mmWave spectrum, it has struggled to do the same for mid-band spectrum. Yet, it is "mid-band spectrum that offers the sweet spot between propagation and capacity" and, therefore, remains essential for the 5G future that proponents readily laud.[17] While the FCC is currently moving forward with efforts to free up this spectrum, considerable challenges remain while demand only increases.

Encouragingly, evidence does point to the necessary transition toward fully 5G networks. According to a 2020 survey by 5G technology provider Enea, one third of global mobile operators plan to deploy such networks within two years.[18] While promising, it is also the case that the full concepts and designs for the architectures (from the end-user devices to the core network) as well as the applications necessary to unleash the full potential and promise of 5G are still developing and are very much in a state of flux. As Doug Brake, the Director of Broadband and Spectrum Policy at the Information Technology and Innovation Foundation (ITIF), argued: it is important to remember that "5G is not a

[b] The 3GPP consortium is the *de facto* leader in mobile network standards.

monolith. […] different versions of it will be deployed in different areas over time."[19] Notably, even within the U.S., some current deployments of 5G are not much faster than the 4G LTE networks they are slowly replacing, while others are, in fact, slower.[20]

3.2. The Universe of Use-Cases

Just as the infrastructure and end-user devices remain a work in progress, we are also not currently living in the commonly heralded 5G future in terms of use-cases.

A series of familiar use-cases frequently accompany most 5G conversations: e.g. driverless cars, smart manufacturing, smart cities, and remote surgeries. Yet, these promised use-cases remain under development and currently lack widespread adoption. Moreover, fully automated, fleets of driverless cars and remote surgeries in our hospitals depend as much on the regulatory and policy ecosystem they find themselves in as they do on technological maturity.

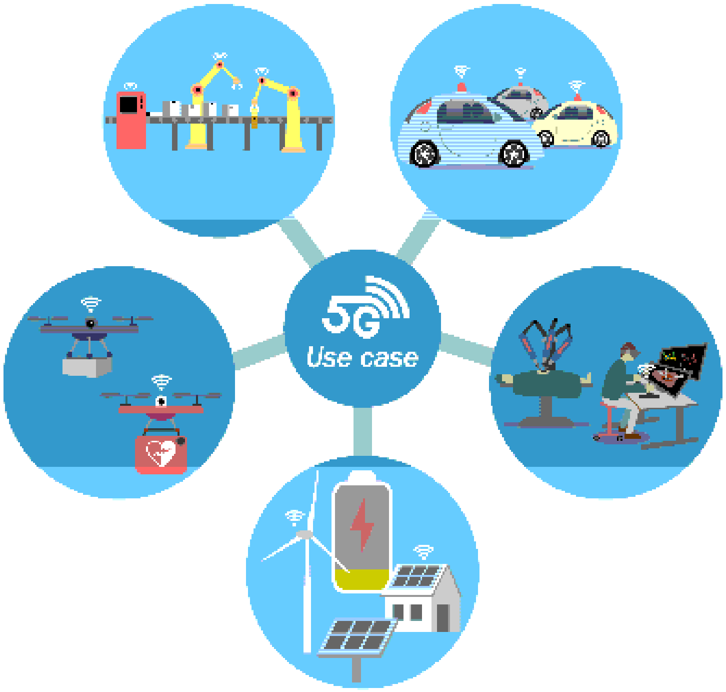

Image source: Shutterstock.com/ By Solveig Been

Additionally, many of the use-cases that will emerge from this fifth generation of mobile networks remain unknown. Take, for example, one portion of the "app economy": ride-share applications such as Lyft and Uber. They were enabled by advances in three areas of technology: smartphones, navigation systems (GPS), and telecommunications (4G LTE). Together, these three areas gave rise to the necessary conditions for a business model based around providing personal transportation options for users on the move. 4G alone did not give rise to the "app economy." An ecosystem, of which 4G was part, did. Similarly, many of the most impactful and innovative use-cases to emerge out of 5G have not yet been conceived of. In other word, these novel use-cases have not made it into the present 5G 'hype'.

3.3. A Work in Progress

In the long term, the promise of 5G is significant and may, in fact, be underhyped though often poorly understood. In the short term, however, that promise has been the victim of far too much hype. While much of the public discussion is tinged with a sense of immediacy, the full potential of 5G has not been realized nor will it be realized within the next few years.[21] Moreover, the promise of 5G will largely depend on how these systems are developed and deployed in practice, and not on what they could accomplish in theory. It is important to recognize that the next-generation of telecommunications – its architectures and applications – is still nascent and actively evolving.

4. The Peril of 5G: Why Worry?

5G promises to serve as the principal foundation upon which modern societies – their economies and their militaries alike – will rest. As a consequence, it is potentially one of the most important networks of the 21st century. 5G is the very definition of critical infrastructure, but also a potentially catastrophic single point of failure and a one-stop shop for intelligence gathering.[22]

In this section, I answer two related but distinct questions. First, why should the U.S. worry about the security of telecommunications networks? Second, what are the national security risks associated with 5G networks in particular?

4.1. 5G is Critical Infrastructure

Why should the U.S. care about the reliability and security of 5G networks? The strategic importance of communications networks, including prior generations and the 5th generation of cellular technology, have been officially recognized at the federal level for nearing on a decade. Established as critical by Presidential Policy Directive 21 in 2013,[23] communications are one of sixteen critical infrastructure sectors in the U.S.[24] As such, it has been deemed essential to the effective functioning of society. More specifically, its "assets, systems, and networks" are so critical to the daily functioning of the U.S. that "their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[25]

This criticality stems from the reality that communications serve an "enabling function" across all critical infrastructure sectors. According to CISA, communications networks underpin "the operations of all businesses, public safety organizations, and government"[26] through a "diverse, competitive, and interconnected industry using terrestrial, satellite, and wireless transmission systems."[27]

Notably, 5G only increases the scale and character of that "enabling function." Given the transformative functions of 5G networks and the use-cases these functions will enable, telecommunications will become even more foundational to the daily operations of government, companies, and society. A similar, though not identical, "enabling function" can be found in other critical infrastructure such as the energy sector, upon which the daily functioning of all other sectors heavily depend. As Federal Communications Commission (FCC) Chairman Ajit Pai summarized in 2019, "[w]hen 5G is embedded in almost every aspect of our society and economy, from businesses to homes, hospitals to transportation networks, manufacturing to the electrical grid, that means securing our networks will become much more important, and much more difficult."[28]

Threats to critical infrastructure in general, and communications in particular, are not merely theoretical. From the vantage of national security, these sectors can fall victim to two broad categories of malicious operations: espionage operations and disruptive or destructive operations. Espionage operations focus on the gathering of intelligence but not the interruption or destruction of infrastructure. In other words, these types of operations undermine the confidentiality of data within systems but not the integrity or availability of those systems. Espionage operations have long targeted communications networks as a treasure trove of information.[29] Looking to 5G in particular, big data found traversing these networks represents an appealing opportunity for intelligence gathering and intellectual property (IP) theft.

In contrast, disruptive operations seek to undermine the integrity and availability by either temporarily incapacitating systems or destroying them altogether. Disruptions of 5G networks have the potential not only to cripple a hospital's traditional communications systems, but also terminate or introduce potentially deadly lag times into a remote-access surgery in the middle of an operation. Factory floors, leveraging a myriad of connected devices and sensors for manufacturing, could grind to a halt and their corresponding safety-critical systems (e.g. safety instrumented systems (SIS)) could be manipulated into unsafe states. In a world of fully automated cars, sudden increases in latency can lead to physical crashes. Ultimately, given the importance of reliability, speed, low latency, and IoT for 5G use-cases, small disruptions in 5G networks could have outsized impacts on the cyber-physical systems they support.

In conclusion, while communications have served a critical "enabling function" within the U.S. historically, 5G amplifies both the scale and character of these dependencies further cementing its place as a potentially catastrophic "single point of failure" for critical functions more broadly. The explosion of data these networks facilitate and transport, will also make 5G a prime intelligence gathering target.

4.2. National Security Concerns with 5G Networks

The confidentiality, integrity, and reliability of data (at-rest, in-motion, and in-use) across 5G networks as well as the networks' resilience as a whole are clearly pressing national security concerns. However, how might malicious actors carry out espionage and disruptive or destructive operations against 5G networks in practice? Put another way: what are the specific security concerns associated with the development, deployment, and maintenance of these networks?

As I have previously discussed in detail in a Wilson Center policy brief,[30] there are two broad categories of security concerns surrounding the development, deployment, and maintenance of 5G: (1) those shaped by the specific actors developing, deploying, and maintaining 5G in practice and (2) those that are points of concern with 5G networks regardless of the specific actors involved in these networks.

4.2.1. Specific Actors: The Risks Associated with Untrusted Vendors

Security concerns associated with 5G can be amplified depending on who is developing and operating the technology in question. Why? Because these vendors have greater access to and inside knowledge of their portions of the ecosystem. To illustrate the potential impact of untrusted vendors within our 5G networks, many of us frequently liken this problem to an untrustworthy company being tasked to build your house. They may retain a copy of the key, but even if they do not, the company is intimately familiar with the layout and security of your home and can use that knowledge to more effectively and efficiently gain access. Ultimately, the 'who' of it all, takes on greater significance given China's domestic political environment and its place as a rising, geopolitical competitor to the U.S. and other like-minded states.

Notably, this first category of risk has also dominated discussions of U.S. national security imperatives around 5G networks. If you were to read recent coverage and policy initiatives surrounding security and the fifth generation of cellular networks, you would logically assume that national security concerns are primarily limited to China in general and Huawei and ZTE in particular. While this is not the case, there are real security concerns associated with untrusted vendors within or as the primary vendors of critical systems.

Image source: of Shutterstock.com/ By Alberto Garcia Guillen

Why is the U.S. so deeply concerned about the presence of untrusted vendors, specifically Chinese vendors, within our 5G networks? Recall, the three components of telecommunication networks: (1) end-user devices, (2) the radio access network (RAN), and (3) the core network. Today, there are a handful of vendors that can offer an integrated end-to-end network at scale, from user devices to the core. Of that handful, two are Nordic (Sweden's Ericsson and Finland's Nokia) and one is Chinese (Huawei). None are American.

Though concerning, this reality should not be interpreted as a lack of U.S. leadership in 5G. In fact, U.S. vendors are among the market leaders in end-user devices (Cisco, Qualcomm, and Apple) and the core network (Cisco and Juniper). In addition, U.S. companies dominate the market for chips, an area where Chinese companies are currently absent (Broadcomm, Texas Instruments, Analogue Devices, Qualcomm, Intel, and Cavium).[31]

Yet, when it comes to the RAN, the U.S. does not have an equipment vendor that can manufacture radios at the scale necessary to meet the needs of the U.S. market.[32] There are radio manufacturers in the U.S. (e.g. Mavenir, JMA, Blue Danube, and Parallel Wireless) but, so far, the capacity for "low-cost US-managed volume manufacture" of radios has been missing.[33] Significantly, this is not a problem for the U.S. alone. The RAN is, in fact, the least vendor-diverse part of the network. It is also considered to be the most expensive: "60-65% of total cost of ownership[c] of a network is in the RAN."[34]

In short, it is not accurate to claim that the U.S. is not a leader in 5G, or that U.S. vendors do not hold dominate market positions across most of the 5G stack. It is accurate to point out, however, that the U.S. does not have a viable end-to-end provider or even a set of providers that together cover the network end-to-end.

Historically, end-to-end providers made up a significant portion of U.S. deployments and dominated the early stages of 5G deployment. As a consequence, incumbent vendors already have a presence in today's mobile networks, a presence that has the potential to persist in emerging brownfield 5G deployments unless components are ripped-and-replaced. Even if the U.S. were able to disaggregate the stack today, leveraging the diversity of U.S. manufacturing expertise and capacity for end-user devices and the core, the RAN would remain a vendor chokepoint.

As a consequence, Huawei as an end-to-end provider and ZTE as a market leader in RAN equipment and the core network appeared poised to play a leading role in the development and deployment of 5G infrastructure within the U.S. but also abroad. A role that raised national security concerns given the criticality of these networks.

4.2.2. More Broadly: Security Challenges for 5G Networks

Even before China enters the conversation, however, here are numerous cybersecurity challenges baked into 5G. Keeping to the house analogy, malicious actors do not require a key if your home was designed without security in mind (just open door, it isn't locked) or security has been poorly tacked on later (the lock is poorly fitted to the doorframe, so just jiggle the door to compromise the lock and then walk on in). With or without untrusted vendors such as Huawei and ZTE, national security concerns - the confidentiality of data and the reliability and integrity of 5G networks – must be addressed.

These include:

1. the challenge of telecommunication infrastructure protection given trends toward increasing cyber-physical systems and the potential for a single point of failure given the expansive "enabling function" 5G will play for other critical infrastructure;

2. the inherited cybersecurity concerns related to prior generations of mobile networks such as 4G LTE, which underpin current brownfield deployment in the U.S.;

3. the amplification of cybersecurity concerns as 5G networks transition core functions even further away from hardware to software as well as the introduction of additional software (AI) to manage the growing complexity of these networks;

4. increased network speed, which allows malicious activity to move or proliferate through a network more rapidly;

5. the explosion of IoT devices, which are notorious for poor security and also radically expand the attack surface of telecommunications networks;

[c] Note: this figure captures the total cost of ownership, which includes building, operating, and maintaining the RAN over time. Total cost of ownership of a network is not synonymous with equipment costs, though equipment costs are included in the broader assessment.

6. fewer hardware chokepoints where cyber hygiene could be traditionally practiced, given that 5G architecture moves away from a hub-and-spoke design toward distributed, software-defined digital routing; and

7. supply chain security risks as development, deployment, operation, and maintenance of network infrastructure, services, and devices all introduce new potential sources of vulnerabilities and opportunities for malicious activity, intentionally or otherwise.

While there are important network defense opportunities that begin to address each of these concerns (such as end-to-end encryption, network segmentation, security standards for IoT devices, and zero-trust architectures), this second category of national security risk has been largely overlooked within national rhetoric and subsequent policy initiatives in favor of the former.

5. The Current U.S. Approach to Security: What is Missing?

To the detriment of broader infrastructure security priorities and initiatives, the dominant focus of recent American rhetoric and policy has been on addressing the problems associated with untrusted vendors within 5G networks at home and abroad. The thrust of the strategy overall is perhaps best described as 'just say no' to Huawei and ZTE.[35]

What steps has the U.S. taken so far to mitigate these risks in the development and deployment of 5G networks? To achieve this goal at home, the U.S. has been deploying a three-pronged approach featuring warnings and formal restrictions, financial incentives, and discussions of technology standards to muscle Chinese telecommunications vendors out of the U.S. 5G ecosystem.

Are those steps adequate? No, for two reasons. First, these efforts have been largely China-centric to the detriment of developing a broader security strategy for 5G networks. Second, a cohesive and uniform national 5G strategy has remained largely elusive. As Jessica Rosenworcel, an FCC Commissioner, noted: "[w]e have yet to coordinate our 5G strategy across the government."[36] A concern echoed by a bipartisan group of eight U.S. Senators in a letter to Robert O' Brien, the Assistant to the President for National Security Affairs, when they warned that "[i]n our view, the current national level approach to 5G is comprised of a dispersed coalition of common concern, rather than a coordinated, interagency activity."[37]

5.1. Warnings and Formal Restrictions

The first and longest standing strain of U.S. policy consists of formal warnings about the risks associated with relying on Chinese vendors and the implementation of formal restrictions. These efforts include government statements, documents, and hearings (a brief sample of which is presented here).

While tensions between the U.S. and Chinese companies significantly heated up in the past two years, the U.S. government blocked Huawei from building out specific wireless networks citing national security concerns as early as 2011.[d38] By 2016, the heads of the FBI, CIA, and NSA all warned against using Chinese vendors (specifically Huawei

[d] In this particular instance, Huawei had bid to build a national U.S. wireless network for emergency services.

and ZTE)[39] and the U.S. Department of Commerce had placed ZTE on the Entity List, which limits exports, re-exports, or transfers to specific persons or companies.[40] By May of 2019, the U.S. Department of Commerce had placed Huawei on the Entity List as well.[41] In that same year, President Trump had issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain, which specifically addressed "information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary."[42] This Executive Order was followed by a second in 2020 extending the ban until 2021.[43] Also in 2020, the FCC officially designated Huawei and ZTE as national security threats.[44] On the legislative front, the National Defense Authorization Act, which prohibited the use of federal money to purchase telecommunications equipment and services from companies like Huawei, went into effect and the Secure and Trusted Communications Network Act of 2019 (HR 4998), which prohibited the use of and creating a reimbursement program from rip-and-replace of components by companies that pose a national security threat, was signed into law.[45]

While there had been some early debate over whether formally restricting Huawei and ZTE from the core of 5G networks would be sufficient,[46] this option was ultimately rejected due to concerns over edge computing in 5G networks, which blurs distinctions between core and peripheral functionalities. In the words of Robert Strayer, Deputy Assistant Secretary of State for Cyber and International Communications Policy at the U.S. State Department, "[t]here is no way that we can effectively mitigate the risk to having an untrustworthy vendor in the edge of the network."[47]

The U.S. has not been alone in this approach. As of August 2020, all five of the Five Eyes countries (members of a long-standing intelligence-sharing alliance) – the U.S., the U.K., Canada, Australia, and New Zealand – had, for the time being, excluded Huawei equipment from their 5G networks.[48] In Belgium, home to both the North Atlantic Treaty Organization (NATO) and the European Union (EU), Orange and Proximus elected to use Nordic network equipment rather than Chinese equipment in their 5G rollouts given persisting security concerns.[49] Taking restrictions a step further, Denmark indicated that it "wants to be able to exclude 5G technology suppliers from providing critical infrastructure in Denmark if they are not from countries considered security allies."[50]

Yet, this formal warnings and restrictions approach to addressing national security concerns has four persisting limitations. First, it fails to address the broader set of risks stemming from non-Chinese vendors and cybersecurity challenges in favor of tackling Huawei and ZTE in particular. Second, while the U.S. has currently excluded Huawei and ZTE from the development and deployment of 5G within the U.S., formal restrictions do not address a lack of alternative American vendors in the market, particularly in regard to radio manufacturing. Third, Huawei and ZTE components exist within prior generations of cellular networks. Replacing these components can be costly, especially for rural vendors where the majority of these components are located within the U.S. In September of 2020, the FCC estimated that it would cost small carriers as much as $1.8 billion to replace Huawei and ZTE across their existing telecommunications networks.[51] Formal restrictions, without corresponding financial incentives, do not address these rip-and-replace costs. Fourth, and finally, while this approach clearly specifies which vendors are untrusted, it does not adequately address what qualifies as a trusted vendor in this space other than using American or other allied countries as political shorthand.

5.2. Financial Incentives

The second strain of American policy has focused on leveraging financial incentives – positive and negative – to exclude Chinese companies within the present and future U.S. telecommunications ecosystem. This approach has the advantage of addressing some of the costs associated with excluding Huawei and ZTE, but, in practice, these efforts remains limited in scope or are currently aspirational.

There are five financial initiatives of particular note that fall under this policy umbrella.

The first of these five initiatives was signed into law in 2020. As previously mentioned, the Secure and Trusted Communications Network Act of 2019 (HR 4998) prohibits the use of and creates a reimbursement program for the rip-and-replace of components by companies that pose a national security threat. But to qualify for the reimbursement program, telecommunications providers must have fewer than two million customers.[52] HR 4998 also prohibits the FCC from "subsidizing the acquisition or maintenance of telecommunications equipment or services from untrusted suppliers."[53] As such, HR 4998 directly built upon the FCC's 2019 Supply Chain Order, which had previously prohibited the use of "Universal Service Fund (USF) subsidies by carriers to purchase or obtain equipment or services produced or provided by a covered company" such as Huawei and ZTE.[54]

There are also three initiatives in progress that, if passed, would provide further financial incentives. First, the CHIPS For America Act (HR 7178) would strengthen American semiconductor manufacturing, a core component of 5G networks as well as other emerging technology.[55] Notably, while the U.S. leads the world in chip design, most chips are manufactured outside the U.S.. Second, the 5G Fund for Rural America proposes to make up to $9 billion in USF support available to carriers to aid in their deployment of advanced 5G mobile wireless services in rural America (including up to $680 million for deployment on Tribal lands).[56] Third, the Utilizing Strategic Allied (USA) Telecommunications Act put forth by six senators proposes that the U.S. government spend at least $1.25 billion "to invest in Western-based alternatives to Chinese equipment providers Huawei and ZTE."[57] Though all three of these initiatives are currently propositions, taken together they illustrate a recognition that 'just say no' is not a viable 5G strategy given the existing vendor landscape and the broader geo-economic and market forces that led to the current 'China Challenge' now dominating security conversations.

In conclusion, despite recognition that financial incentives and support will be necessary to address national security concerns related to 5G networks, efforts in this space remain narrowly defined to Huawei and ZTE and/or remain currently aspirational/in progress. Notably, while there have been some suggestions that the U.S. government needs to invest in or incentivize American radio manufacturing, given the lack of American options in this portion of the stack, this has not yet taken place.

5.3. Technology Standards

The most recent strand of 5G national security debates within the U.S. centers on technology standards, specifically, open radio access networks (RAN). Open RAN has been heralded as the newest means through which the U.S. can achieve a diverse, innovative, and secure 5G ecosystem.

Since I have discussed the range of national security implications of Open RAN in a prior Wilson Center publication in detail, I will only briefly address the potential national security solutions Open RAN offers and the potential pitfalls here. "Open RAN and 5G: Looking Beyond the National Security Hype" offers readers a more in-depth discussion of whether Open RAN can live up to the national security promise.[58]

The "open" in Open RAN, a generic industry term for open radio access network (RAN) architecture, promises to move 5G away from proprietary, vertically integrated networks dominated by a handful of vendors to a diversity of hardware and software players across the 5G stack. Put simply, it would give operators the option to shop around and then, in theory, plug and play. In the broadest sense, advocates of Open RAN claim that, when given the opportunity, operators will avoid Chinese vendors when building and maintaining their 5G networks. As a consequence, Open RAN has found itself as the latest geopolitical tool, heralded by the FCC's Chairman Ajit Pai and Secretary of State Mike Pompeo alike, for removing untrusted vendors from 5G networks at home and abroad.

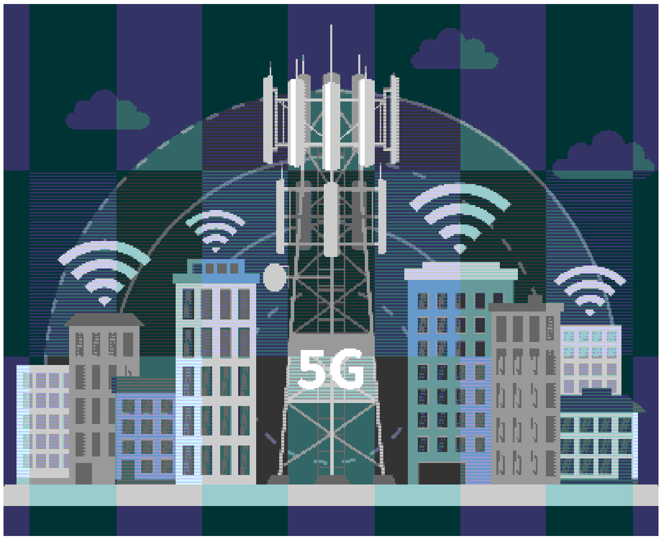

Image source: of Shutterstock.com/ By kanvictory

The potential benefits of Open RAN for the U.S. 5G ecosystem are largely fivefold: (1) lower component prices due to market competition across the stack, (2) improved cybersecurity by increasing the number of eyes on each component and allowing operators to shop around for components with higher standards of security throughout the stack, (3) allowing the U.S. to play to its industry strengths (software, the platform economy, and an increasingly service-based economy), and (4) a diverse set of vendors to replicate current incumbent end-to-end solutions by the likes of Huawei. It also has one final, particularly clever benefit. (5) It forces incumbent players to spend resources on Open RAN when they have already expended significant resources on the development and deployment of proprietary end-to-end solutions.

Yet, Open RAN is not the geopolitical silver bullet it is frequently portrayed to be in popular accountings. There are three limitations of particular note related to the utility of Open RAN as a solution for national security concerns, specifically untrusted vendors.

First, Huawei is not the only vendor whose relative advantage lies in providing proprietary, vertically integrated 5G networks. Recall, both Ericsson and Nokia provide proprietary, vertically integrated 5G networks within the U.S. market. Moreover, both Ericsson and Nokia are also two of the only other major players in the radio space alongside Huawei. As a tool for addressing untrusted vendors, the impact of Open RAN will also be felt by these two Nordic companies as well as Huawei. In short, Open RAN is more anti-establishment than it is anti-Chinese. This type of market disruption may yield positive outcomes in the long term. But in the short term, we risk undermining the few potentially trusted vendors we have for radios as well as the two vendors who are currently building nearly all the 5G networks in the US market and employ about 24,000 people in North America.[59]

Second, Open RAN is not currently as mature as the proprietary, vertically integrated network vendors it is meant to muscle out. This raises three sets of concerns. First, integrated 5G vendors have a market advantage both in terms of existing infrastructure deployment but also given the level of performance at scale that customers have grown to expect from their telecommunications networks. In other words, Open RAN must still contend with more mature incumbent players in the U.S. and global market. Second, given that operators in the U.S. are currently facing increasing pressure to rip-and-replace untrusted vendors from within their stack, they also now face the dilemma of delaying, hedging their bets on Open RAN, or selecting existing vendors with a proven track record. Third, while Open RAN advocates argue that it will improve cybersecurity, it also introduces a series of new concerns. While there are security advantages to open code (more eyes are better than less), there are also disadvantages (more eyes also means more malicious eyes on code). Moreover, new is not better given that time aids in discovering latent vulnerabilities in software and integrating a diversity of vendors, in practice, introduces potentially unanticipated failures and bugs into an already complex system.

Third, in contrast to cloud platform providers (an inspiration behind Open RAN), market dynamics in telecommunications differ in fairly significant ways. In telecommunications, there are a limited number of service providers (3-5) competing not over global ecosystems but within nationally bounded territories. In this market, to compensate for costs that must be "amortized over a relatively narrow customer base," service providers "are tightly-coupled to vendors who build products – not platforms – with little incentive for ecosystem involvement."[60] The elephant in the Open RAN room is the degree to which service providers are genuinely willing to take on the costs of leveraging a wide diversity of suppliers across a network, which is easier said than done and deeply costly to pull off in practice. To solve this problem, system's integrators could take on the costs of developing and testing a disaggregated stack to ensure reliability and quality performance. Yet, a fundamental question remains; will the telecommunications market support the cost of a fully disaggregated stack? The answer likely lies not at either extreme, but on a balance between vendor-integrated and disaggregated networks where service providers incorporate a broader but still fairly limited number of vendors for each section of the stack rather than the diverse and numerous vendors cloud platforms boast.

In conclusion, while Open RAN does offer important benefits for the development and deployment of 5G and presents some leverage for addressing national security concerns, it is no geopolitical silver bullet. The scale and scope of its impact remains an open question. Moreover, while the FCC, CISA, and the State Department in particular have been keen to publicly promote Open RAN, so far, the U.S. has been hesitant to officially champion, invest in, or aid in its widespread adoption.

5.4. Persisting Shortcomings

The national level policy discourse in the U.S. has unduly focused its efforts on just one half of the national security landscape – risks shaped by the specific actors developing, deploying, and maintaining 5G in practice – leaving the second, more foundational half – cybersecurity challenges with 5G networks – largely under-discussed and under-addressed.

Perhaps this disparity in focus stems from the appeal of the geopolitical flavor of national security arguments centering on China. Clearly, these so-called Chinese national champions feel more pressing given the larger geopolitical environment and competition with China the U.S. now finds itself in. The solutions feel more manageable and imaginable, at least in the short term. The policy narrative: China is a threat and, therefore, we must remove Chinese vendors from our 5G networks and those of likeminded countries. Though, even here, efforts largely rest on 'just say no' without addressing the broader forces that led to the rise of Chinese telecommunications vendors such as Huawei and ZTE and the absence of American end-to-end vendors.

In contrast, conversations over critical infrastructure protection more broadly feel more technical; bureaucratically complex, and intractable with fewer easily imagined and deployed solution-sets in the short and long term. As a consequence, many of the efforts here, such as cybersecurity efforts led by the U.S. Department of Commerce's National Institute of Standards and Technology (NIST),[61] lack the national attention and political weight given to Huawei and ZTE.

Whatever the reason, the U.S. has neither adequately grappled with the broader realities of risk associated with 5G networks nor developed, cohesive government and industry approaches for mitigating that risk in practice.

6. Concluding Thoughts and Policy Takeaways

With 5G, the U.S. faces a pressing national security challenge. However, the relevant question for policy is not where the U.S. is in relation to China on some metaphorical racetrack. Instead, the relevant question is how the U.S. can put itself in the best possible position to reap the current and future economic benefits of 5G while also addressing the security concerns associated with this fifth generation of cellular networks.

To that end, there are four observations of particular relevance to the policy moment the U.S. now finds itself in.

First, security, in its simplest form, is a risk management problem. However, solving that problem first requires a clear understanding of the risks. The national security implications of 5G are not limited to high-risk vendors in general and/or Chinese companies in particular. Equally important are the security concerns that extend beyond any single company's role in the development, deployment, and maintenance of 5G networks. Therefore, the U.S. needs to build out a more robust and comprehensive assessment of the country's risk profile, one that is not dominated by a focus on China and untrusted vendors.

Second, policy solutions must be as diverse as the problems they need to solve. The recent narrowing of focus to one specific problem provides a distorted picture of the potential perils associated with this future critical infrastructure and will not adequately address the broader category of risks the U.S. faces. This requires three recognitions. First, in complex systems, there are no geostrategic silver bullets. No, not even the currently popular Open RAN. Second, if we wish to see a diverse, innovative, and secure 5G ecosystem, the U.S. needs to widen the policy aperture and give the broader set of concerns the same political weight and voice given to Huawei and ZTE. Third, even when focused on Chinese vendors, solutions cannot afford to be primarily reactionary and tailored to specific companies. This approach will not adequately address the root causes that have led to the 5G vendor market the U.S. now faces.

Third, in developing and implementing these solutions, the U.S. must move beyond "a dispersed coalition of common concern" and build out "a coordinated, interagency" national security effort. 5G is the very definition of critical infrastructure, representing a potentially catastrophic single point of failure and a one-stop shop for intelligence gathering. It is also the foundation upon which economies will continue to generate value. The stakes are incredibly high and the security concerns complex, yet U.S. lines of effort remain deeply siloed and underdeveloped. In the same vein, we can, and should, leverage alliances, trade agreements, and other forms of cooperation that have long been the backbone of U.S. foreign policy. At both the national and international level, it is past time for common concern to be replaced by sustained policy action.

Fourth, and finally, while much of the public discussion is tinged with a sense of immediacy, the full promise of 5G will not be realized in the short term. 5G is a work in progress and much remains unknown, both in terms of the potential network permutations that will emerge and the universe of use-cases those foundations will one day support.

Yet, because the next-generation of telecommunications – its architectures and applications – is still nascent and actively evolving, the present moment provides the U.S. with a unique window of opportunity. Here, the final few lines of a 5G policy brief I wrote last year continue to capture the current moment: "[i]n the race for 5G supremacy, security is no less important than speed. As the U.S. wades into this policy space, they have an opportunity to design policy in a manner that proactively addresses the wider, complex realities of risk rather than pursuing reactionary policy out of sole concern for one multinational company. As this critical infrastructure of the future materializes, now is the time to seize that opportunity." If the U.S. waits too long, this window of opportunity will close.[62]

Endnotes

[1] Cybersecurity and Infrastructure Security Agency U.S. Department of Homeland Security, “CISA 5G STRATEGY Ensuring the Security and Resilience of 5G Infrastructure In Our Nation 2020,” 2020, https://www.cisa.gov/sites/default/files/publications/cisa_5g_strategy_508.pdf.

[2] Doug Brake and Alexandra Bruer, “Broadband Myths: Is It a National Imperative to Achieve Ultra-Fast Download Speeds?,” *ITIF* , November 16, 2020, https://itif.org/publications/2020/11/16/broadband-myths-it-national-imperative-achieve-ultra-fast-download-speeds.

[3] Jeremy Horwitz, “Decoding 5G: A Cheat Sheet for next-Gen Cellular Concepts and Jargon ,” VentureBeat, December 12, 2018, https://venturebeat.com/2018/12/12/decoding-5g-a-cheat-sheet-for-next-gen-cellular-concepts-and-jargon/

[4] James Andrew Lewis, “How 5G Will Shape Innovation and Security | Center for Strategic and International Studies,” CSIS, December 2018, https://www.csis.org/analysis/how-5g-will-shape-innovation-and-security.

[5] For a more in-depth discussion of the importance of this ecosystem refer to Dafna Bearson, Martin Kenney, and John Zysman, “Labor in the Platform Economy: New Work Created, Old Work Reorganized and Value Reconfigured,” BRIE Working Paper Series. 2019; Martin Kenney, Dafna Bearson, and John Zysman, “The Platform Economy Matures: Pervasive Power, Private Regulation, and Dependent Entrepreneurs,” BRIE Working Paper Series. 2019; and John Zysman and Mark Nitzberg “Governing AI: Understanding the Limits, Possibility, and Risks of AI in an Era of Intelligent Tools and Systems” Woodrow Wilson Center White Paper. 2020, https://www.wilsoncenter.org/publication/governing-ai-understanding-limits-possibilities-and-risks-ai-era-intelligent-tools-and.

[6] “Exploring the Links between AI, 5G and IoT – and How Cloud Computing Underpins Them All,” Cloud Computing News, February 12, 2019, https://cloudcomputing-news.net/news/2019/feb/12/exploring-links-between-ai-5g-and-iot-and-how-cloud-computing-underpins-them-all/.

[7] Hannes Ekström, “Non-Standalone and Standalone: Two Paths to 5G,” Ericsson, July 11, 2019, https://www.ericsson.com/en/blog/2019/7/standalone-and-non-standalone-5g-nr-two-5g-tracks.

[8] Monica Alleven, “3GPP Declares First 5G NR Spec Complete ,” FierceWireless, December 20, 2017, https://www.fiercewireless.com/wireless/3gpp-declares-first-5g-nr-spec-complete.

[9] “Release 15,” 3GPP, April 26, 2019, https://www.3gpp.org/release-15.

[10] Mehmet Turunc, “What Is 5G, SA, NSA?,” iBASIS, February 27, 2020, https://ibasis.com/what-is-5g-sa-nsa/.

[11] “Release 17,” 3GPP, September 22, 2020, https://www.3gpp.org/release-17.

[12] Monica Alleven, “‘Real’ 5G Relies on 5G NR, Standalone Architecture: Special Report ,” FierceWireless, March 24, 2020, https://www.fiercewireless.com/wireless/real-5g-relies-5g-nr-standalone-architecture-special-report.

[13] Rajiv Shah, “Ensuring a Trusted 5G Ecosystem of Vendors and Technology,” Australian Strategic Policy Institute (ASPI), September 17, 2020, https://www.aspi.org.au/report/ensuring-trusted-5g-ecosystem-vendors-and-technology and Brian Lavallée, “5G Wireless Needs Fiber, and Lots of It,” *Ciena*, 2020, https://www.ciena.com/insights/articles/5G-wireless-needs-fiber-and-lots-of-it_prx.html#:~:text=global%20responsibility%20for%20Ciena’s%205G,and%20Submarine%20networking%20solutions.&text=In%20fact%2C%205G’s%20formidable%20network,of%20it%2C%20to%20cell%20sites.

[14] Brian Greenberg et al., “5G in Government: The Future of Hyperconnected Public Services,” Deloitte Insights, 2020, https://www2.deloitte.com/xe/en/insights/industry/public-sector/future-of-5g-government.html#endnote-5.

15 Linda Hardesty, “Dish Picks Nokia for Containerized 5G SA Core ,” FierceWireless, September 14, 2020, https://www.fiercewireless.com/5g/dish-picks-nokia-for-containerized-5g-sa-core and “Rakuten Mobile and NEC Agree to Jointly Develop Containerized Standalone 5G Core Network ,” Business Wire, June 2, 2020, https://www.businesswire.com/news/home/20200602005999/en/Rakuten-Mobile-NEC-Agree-Jointly-Develop-Containerized.

16 Greenberg et al., “5G in Government: The Future of Hyperconnected Public Services.”

17 Doug Brake, “A U.S. National Strategy for 5G and Future Wireless Innovation” (Information Technology and Innovation Foundation, 2020), https://itif.org/publications/2020/04/27/us-national-strategy-5g-and-future-wireless-innovation.

18 Enea, “Survey: One Third of Mobile Operators will Deploy 5G Standalone withing Two Years,” accessed October 11, 2020, https://www.enea.com/press-releases/item/?pressrelease=914951D566B65F37.

19 Brake, “A U.S. National Strategy for 5G and Future Wireless Innovation.”

20 Geoffrey A. Fowler, “The 5G Lie: The Network of the Future Is Still Slow,” *The Washington Post*, September 8, 2020, https://www.washingtonpost.com/technology/2020/09/08/5g-speed/.

21 Mohanbir Sawhney, “5G Tech Won’t Be Here as Soon as You Think (Opinion),” CNN, December 30, 2019, https://www.cnn.com/2019/12/10/perspectives/5g-technology-t-mobile-att-verizon/index.html.

22 Melissa K Griffith, “5G and Security: There Is More to Worry About than Huawei,” *Wilson Center Policy Brief*, 2019, https://www.wilsoncenter.org/publication/5g-and-security-there-more-to-worry-about-huawei.

23 “Presidential Policy Directive -- Critical Infrastructure Security and Resilience,” The White House, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

24 “Critical Infrastructure Sectors,” CISA, March 24, 2020, https://www.cisa.gov/critical-infrastructure-sectors.

25 “Critical Infrastructure Sectors.”

26 “Critical Infrastructure Sectors.”

27 “Communications Sector,” CISA. accessed October 12, 2020, https://www.cisa.gov/communications-sector.

28 Alfred Ng, “5G Brings up Questions of Cybersecurity Vulnerabilities ,” CNET, November 12, 2019, https://www.cnet.com/news/5g-security-means-fcc-getting-tough-on-wireless-carriers-senator-says/.

29 Ben Buchanan, *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Kindle Edition (Harvard University Press, 2020).

30 Griffith, “5G and Security : There Is More to Worry About than Huawei.”

31 Lewis, “How 5G Will Shape Innovation and Security | Center for Strategic and International Studies.”

32 Melissa K. Griffith, “Open RAN and 5G: Looking Beyond the National Security Hype,” *Wilson Center*, November 2, 2020, https://www.wilsoncenter.org/article/open-ran-and-5g-looking-beyond-national-security-hype.

33 Morris Lore, “Open RAN Won’t Stop China, Dotards,” Light Reading, January 30, 2020, https://www.lightreading.com/mobile/5g/open-ran-wont-stop-china-dotards/a/d-id/757193.

[34] Samsung, "The Open Road to 5G," https://image-us.samsung.com/SamsungUS/samsungbusiness/pdfs/Open-RAN-The-Open-Road-to-5G.pdf.

[35] David Forscey and Herb Lin, "'Just Say No' Is Not a Strategy for Supply Chain Security ," *Lawfare*, March 25, 2020, https://www.lawfareblog.com/just-say-no-not-strategy-supply-chain-security.

[36] Margaret Harding McGill, "Barr Scoffs at White House's Anti-Huawei 5G Approach," Axios, February 6, 2020, https://www.axios.com/barr-scoffs-at-white-houses-anti-huawei-5g-proposal-e3afb2c2-7f21-4609-a02e-ae3753f514f5.html/.

[37] Joseph Marks, "The Cybersecurity 202: The White House Needs a 5G Czar to Win the Race to Secure next-Generation Networks, Senators Warn ," *The Washington Post*, November 20, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/11/20/the-cybersecurity-202-the-white-house-needs-a-5g-czar-to-win-the-race-to-secure-next-generation-networks-senators-warn/5dd4505788e0fa10ffd2103f/.

[38] Joe Hindy, "The Huawei Controversy Timeline: Everything You Need to Know!," Android Authority , May 29, 2019, https://www.androidauthority.com/huawei-vs-united-states-990007/.

[39] James Vincent, "Don't Use Huawei Phones, Say Heads of FBI, CIA, and NSA," The Verge, February 14, 2018, https://www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears.

[40] "Additions to the Entity List," Federal Register , March 8, 2016, https://www.federalregister.gov/documents/2016/03/08/2016-05104/additions-to-the-entity-list.

[41] "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies ," U.S. Department of Commerce Press Release , May 15, 2020, https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts.

[42] The White House, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019, https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

[43] Chaim Gartenberg, "Donald Trump Extends Huawei Ban through May 2021," The Verge, May 13, 2020, https://www.theverge.com/2020/5/13/21257675/trump-extends-huawei-ban-may-2021-china-us-android-google-telecom.

[44] "FCC Designates Huawei and ZTE as National Security Threats," Federal Communications Commission, June 30, 2020, https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats.

[45] Brake, "A U.S. National Strategy for 5G and Future Wireless Innovation."

[46] "NCSC advice on the use of equipment from high risk vendors in UK telecoms networks version 1.0" National Cyber Security Centre (January 2020), https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks.

[47] U.S. Department of State, "LiveAtState With Economic and Business Affairs Bureau Deputy Assistant Secretary Robert Strayer" (transcript), April 29, 2019, https://2017-2021.state.gov/liveatstate-with-economic-and-business-affairs-bureau-deputy-assistant-secretary-robert-strayer/index.html.

[48] Tom Jowitt, "Canada Final 'Five Eyes' Member Exclude Huawei," Silicon UK Tech News, August 26, 2020, https://www.silicon.co.uk/5g/canada-exclude-huawei-347312.

49 Campbell Kwan, “Belgian Telcos Leave Huawei out in the Cold for 5G Rollouts,” *ZDNet*, October 12, 2020, https://www.zdnet.com/article/belgian-telcos-leave-huawei-out-in-the-cold-for-5g-rollouts/#:~:text=Orange%20and%20Proximus%20have%20both,of%20the%20telcos’%204G%20networks.

50 “Denmark Wants 5G Suppliers from Closely Allied Countries, Says Defence Minister,” *Reuters*, June 8, 2020, https://www.reuters.com/article/us-telecoms-5g-denmark/denmark-wants-5g-suppliers-from-closely-allied-countries-says-defence-minister-idUSKBN23F1IT.

51 Russell Brandon, “It Will Cost $1.8 Billion to Pull Huawei and ZTE out of US Networks, FCC Says ,” The Verge, September 4, 2020, https://www.theverge.com/2020/9/4/21422939/huawei-zte-us-phone-networks-fcc-congress-reimbursement-cost.

52 Brake, “A U.S. National Strategy for 5G and Future Wireless Innovation.”

53 “Wicker Statement on Senate Passage of Secure and Trusted Communications Networks Act,” Press Release, U.S. Senate Committee on Commerce, Science, and Technology, 2020, https://www.commerce.senate.gov/2020/2/wicker-statement-on-senate-passage-of-secure-and-trusted-communications-networks-act.

54 Wiley Reports That Bill Rejecting the ‘Rip and Replace’ of Huawei and ZTE Equipment Heads to the President”, Satellite Evolution Group, March 2, 2020. https://www.satellite-evolution.com/post/2020/03/03/wiley-reports-that-bill-requiring-the-rip-and-replace-of-huawei-and-zte-equipment-heads.

55 “CHIPS for America Act Would Strengthen U.S. Semiconductor Manufacturing, Innovation,” Semiconductor Industry Association, June 10, 2020, https://www.semiconductors.org/chips-for-america-act-would-strengthen-u-s-semiconductor-manufacturing-innovation/.

56 Wicker, Walden Release Broadband Connectivity and Digital Equity Framework” Press Release, U.S. Senate Committee on Commerce, Science, and Transportation. June 18, 2020. https://www.commerce.senate.gov/2020/6/wicker-walden-release-broadband-connectivity-and-digital-equity-framework.

57 Jon Brodkin, “US May Subsidize Huawei Alternatives with Proposed $1.25 Billion Fund ,” Ars Technica, January 15, 2020, https://arstechnica.com/tech-policy/2020/01/us-may-subsidize-huawei-alternatives-with-proposed-1-25-billion-fund/.

58 Griffith, “Open RAN and 5G: Looking Beyond the National Security Hype.”

59 Morris Lore, “The Political Hijacking of Open RAN,” Light Reading, May 6, 2020, https://www.lightreading.com/5g/the-political-hijacking-of-open-ran/a/d-id/759454.

60 Frank Rayal, “A Perspective on Open RAN ,” 2020, https://frankrayal.com/2020/07/18/a-perspective-on-open-ran/.

61 “5G Cybersecurity | NCCoE,” NIST, accessed November 22, 2020, https://www.nccoe.nist.gov/projects/building-blocks/5g-cybersecurity.

62 Griffith, “5G and Security : There Is More to Worry About than Huawei.”

About the Author

Melissa K. Griffith is a Public Policy Fellow with the Science and Technology Innovation Program (STIP) at the Woodrow Wilson International Center for Scholars; a Non-Resident Research Fellow at the University of California, Berkeley's Center for Long-Term Cybersecurity (CLTC); and an Adjunct Professor at Georgetown's Center for Security Studies (CSS).

She works at the intersection between technology and national security with a specialization in cybersecurity. Ongoing research projects include (1) the national security implications of and policy opportunities for the development and deployment of 5G networks, (2) collective defense and resilience as national defense strategies in cyberspace, (3) transatlantic cybersecurity and technology cooperation, and (4) the role of emerging technologies in great power competition. Her work sheds important light on the components and dynamics of cyber power and cyber conflict, as well as the vital role that public-private cooperation and both security and economic policy play in national defense.

Griffith holds a Ph.D. and a M.A. in Political Science from the University of California, Berkeley and a B.A. in International Relations from Agnes Scott College.

About the Project: 5G Beyond Borders

5g.wilsoncenter.org

The **Wilson Center's 5G Beyond Borders** project explores how the U.S., Canada, and Mexico can work together to maximize the benefits of 5G and related technology through informed policy solutions. The project offers an overview of the landscape of 5G technology around the globe, while also focusing on the impact of 5G on North American business, and smart manufacturing. Cross-border collaboration between the U.S., Canada, and Mexico is essential to a secure transition. 5G Beyond Borders explores not only 5G security, but how North American cooperation can reduce risks, maximize economic gains, and ensure an efficient 5G rollout.

Workshop Partners

The Wilson Center was chartered by Congress in 1968 as the official memorial to President Woodrow Wilson. It serves as the nation's key non-partisan policy forum for tackling global issues through independent research and open dialogue to inform actionable ideas for the policy community. The workshop is part of the Wilson Center's **5G Beyond Borders** project, which is a larger collaboration between the Wilson Center's Mexico Institute, Canada Institute, and Science and Technology Innovation Program (STIP).

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

Tecnológico de Monterrey is a private, non-profit, and independent institution with no political and religious affiliations, founded in September of 1943. Since then, the university has enrolled more than 65,000 undergraduate and graduate students in Monterrey, Mexico City, Guadalajara and 26 other cities in Mexico. The work of Tecnológico de Monterrey is supported by civil associations made up of a numerous group of outstanding leaders from all over the country who are committed to quality in higher education. It is the only non-US university in the Princeton Review of Top Schools for Entrepreneurship Studies (2020).

Woodrow Wilson International Center for Scholars
One Woodrow Wilson Plaza
1300 Pennsylvania Avenue NW
Washington, DC 20004-3027

The Wilson Center

www.wilsoncenter.org
wwics@wilsoncenter.org
facebook.com/woodrowwilsoncenter
@thewilsoncenter
202.691.4000

Wilson Center