2021

A

Melissa K. Gri□th

Public Policy Fellow
Woodrow Wilson
International Center
for Scholars

Ba a c e
P ea d e
Pe 5G:

The State of Play in the United States

5G BEYOND BORDERS

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

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

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 prom-

Table of Contents

1.

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***

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

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 [illegible], which represents a marked improvement to the speed of existing mobile networks through significant increases in bandwidth. Fundamentally, however, EMBB is best under

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).

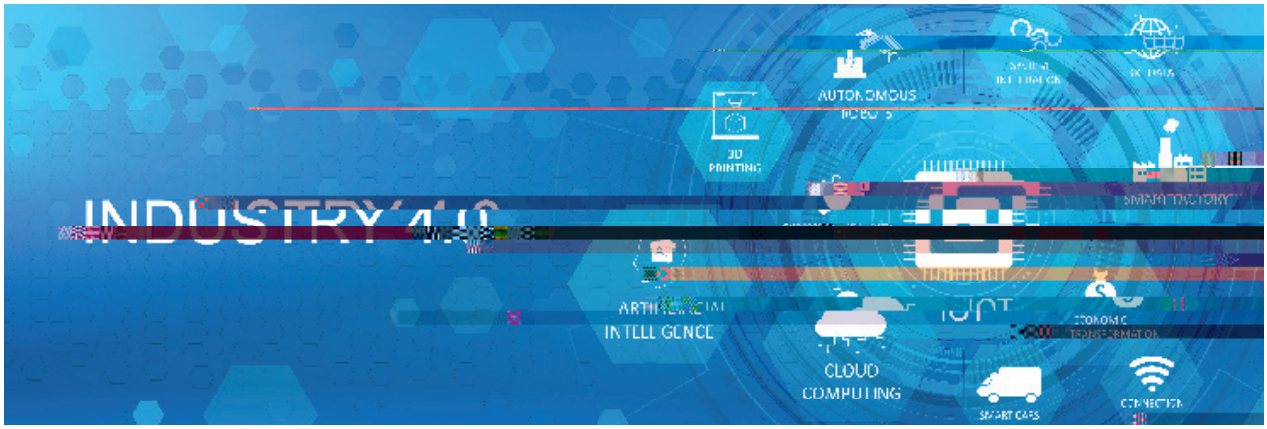

Image source: Shutterstock.com/ By Mari Kova

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

4G LTE core.[7] This form of deployment is aided by technical standards, especially the widely implemented version

monolith. […] different versions of it will be deployed in different areas over time."

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.

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 e aEMCccorenera aEMC5 (a un(v)p2 ()4ecuri.5 (inc op the 5th)0)0 busine

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]

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]

5.2. Financial Incentives

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

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

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.

, 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]

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,

49

A • A •

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.

A

5 .

The 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.

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 5 project, which is a larger collaboration between the Wilson Center's Mexico Institute, Canada Institute, and Science and Technology Innovation Program (STIP).

( ) 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.

is a private, non-profit, and independent institution ihanada0nalyr thiID 1206 BDC BT0 0 0 0.8 k/T1