MITRE | The MITRE Center for Technology & National Security

5G AND THE FRONT LINES OF THE U.S.-CHINA GREAT POWER COMPETITION

By T. Charles Clancy, PhD

©2019 The MITRE Corporation. All rights reserved. Approved for Public Release. Distribution unlimited. Case number 19-02806-1

This page intentionally left blank.

Introduction

Roughly every decade, a new generation of wireless technology emerges that fundamentally disrupts how we access the Internet and how it impacts our daily life. For example, 3G was the first network technology to provide ubiquitous access to the web from any mobile device. Then increased throughput from 4G fueled the social-mobile Internet that enabled real-time social media and multimedia content sharing. And now we have 5G, which promises to unlock the Internet of Things (IoT), connecting everything from home appliances to critical infrastructure to the cloud, enabling accelerated data analytics and advanced automation.

5G seeks to enable three broad use cases. Enhanced Mobile Broadband (EMB) will have the capacity to simultaneously deliver 4K HD video to every smartphone in a dense, congested area like Manhattan. Massive Machine-Type Communications (MMTC) will support densities as large as one million connected IoT devices in a square-kilometer area to enable things like smart-city deployments. Ultra-Reliable Low Latency Communications (URLLC) brings network delay to under one millisecond so, for example, autonomous vehicles can exchange safety-critical messages nearly instantly. The combination of these technologies is expected to transform virtual reality, fundamentally change robotic process autonomation, and create an environment where thousands of drones can be safely controlled from the cloud.

Along the way, however, a new player disrupted the telecommunications vendor community. Once led by North American companies like Motorola, Lucent, and Nortel, today's global telecommunications technology ecosystem is primarily led by a single company – China-based Huawei. Huawei's impressive rise over the past 15 years was the result of a deliberate strategy aligned with China's vision of economic and technological superiority as an instrument of national power.

Huawei's burgeoning global market share raises a number of significant concerns.

First, Huawei's technology is built on stolen intellectual property (IP). Cyber intrusions, industrial espionage, and employee incentive programs that give bonuses for stolen IP have helped Huawei propel its products to market faster and with less investment than its peers[1,2].

Second, the Chinese Communist Party (CCP) frequently uses its domestically based tech companies to enable global cyber operations. For example, the CCP has leveraged China Telecom's points of presence in North America to manipulate the flow of data over the Internet backbone in order to route sensitive content through Beijing[3].

Third, Beijing's new intelligence law provides Huawei the ability to compel other telecommunications companies to support its national objectives[4].

Fourth, Huawei's products are riddled with easily exploitable security vulnerabilities, a result of poor coding practices forced by too-rapid design and deployment schedules[5].

The United States is actively searching for both policy and technology solutions to this complex problem. 5G is an active front in the growing great power

[1] S. Thurm, "Huawei Admits Copying Code from Cisco in Router Software," Wall Street Journal, March 24, 2003.
[2] "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud," U.S. Department of Justice, EDNY Docket No. 18-CR-457, January 28, 2019.
[3] C. Demchak, Y. Shavitt, "China's Maxim – Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking," Military Cyber Affairs, Vol. 3, (1), October 2018.
[4] R. Emmott, "China's Intelligence Law Looms Over EU 5G Safeguards," Reuters, July 29, 2019.
[5] "Huawei Cyber Security Evaluation Center (HCSEC) Oversight Board: Annual Report", March 2019.

competition between the U.S. and China. These solutions typically fall along three basic lines: slowing down Chinese expansion, accelerating U.S. innovation, and working around this new major player. In the end, any successful national strategy for 5G must leverage and combine multiple strategy dimensions.

Strategy 1: Slow Down China

The first broad strategic approach focuses on slowing down China's global market expansion and the country's instruments for that expansion—companies like Huawei. The U.S. is either in the process of or has already rolled out policies aimed at slowing the adoption of Huawei products globally, targeting Huawei practices that allow it to move quickly, and leveling the international playing field.

The recently signed Executive Order on 5G,[6] along with pending and enacted legislation,[7,8] seeks to implement a range of bans on Huawei equipment. Generally, these bans are intended to prevent the federal government, and those doing business with it, from buying Huawei equipment. They also block U.S. telecommunications companies from deploying Huawei equipment in their core networks and provide funds for carriers to replace existing Huawei equipment in their networks. While Huawei, as well as China-based ZTE, have a 37 percent global market share[9], so far their penetration in the U.S. market is minimal. So while these approaches may help sanitize U.S. infrastructure, they will not have a significant economic impact on Huawei.

Embargos may have more impact on their bottom line. Over the past few years the U.S. Department of Commerce has flirted with embargoing Huawei. Last year, ZTE was the target of proposed sanctions for providing equipment to Iran in violation of international restrictions. That move would have prevented ZTE from buying Qualcomm chips, which are central to its smartphone product line. Ultimately, the sanctions never went into effect. In 2019, Huawei and many of its international affiliates popped up on the Commerce Department's "entity list," preventing them from buying everything from microprocessors to certain apps. While full enactment of the sanctions continues to be postponed as a set of exceptions is finalized, the threat of such action compelled Huawei to begin developing an entirely non-U.S. supply chain for its smartphones. While this move arguably slowed Huawei down in the short term, in the long term it will enable the company to be more resilient with an increasingly China-based supply chain.

As for leveling the playing field, the current strategy among Western nations was laid out at the May 2019 Prague 5G Security Conference. This strategy suggests dictating strict security standards for companies purchasing 5G equipment in order to ensure telecommunications companies assess and effectively manage risk in their supply chain. A key requirement of this proposed security rubric tests whether a company's country of origin has a legal environment that can compel industry to support national military and intelligence operations. So while the low price of Huawei's wares may be very attractive to network operators, its products will fail to comply with these stricter national and international standards for security.

More controversial is a proposal to develop and release an entirely open-source, cost-free 5G implementation. This would be possible; open-source wireless has been growing over the past decade, driven by advances in software-defined radio technology. While free, open-source versions of 2G, 3G, and 4G exist today, they are mostly hobby-grade systems used at

[7] "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," Presidential Executive Order 13873, May 15, 2019.
[8] "John S. McCain National Defense Authorization Act for Fiscal Year 2019", Public Law 115-232, August 13, 2018.
[9] "Defending America's 5G Future Act," S.2118, July 15, 2019.
[10] S. Pongratz, "Key Takeaways – Worldwide Telecom Equipment Market 2018," Dell'Oro Group Telecommunication Infrastructure Research Program, March 4, 2019.

universities or test labs. No scalable, open-source commercial-grade cellular systems exist today. Clearly, developing and releasing such a system would fundamentally change market dynamics. While it would undercut Huawei, it would almost certainly have an existential impact on two European equipment makers: Nokia and Ericsson.

A key concern for using this strategy alone is that it could lead to two Internets. One Internet will extend from China via the Belt and Road initiative; be based on Huawei devices using Huawei's app store; rely on services like Tencent, Alibaba, and Baidu; and be censored by the Great Firewall of China. The other Internet will stitch together the West; be based on vendors like Nokia, Ericsson, and Cisco; rely on services like Google, Facebook, and Amazon; and be governed by primarily U.S. and EU regulations. This Balkanization between technological democracy and autocracy is fundamentally bad for everything from global trade to human rights to developing a shared global culture.

Strategy 2: Speed Up U.S. Production

An altogether different strategic tack is to focus on accelerating U.S. innovation in wireless technologies. Once the world leader in telecom innovation, with cutting edge companies such as the iconic Bell Labs, the pace of U.S. innovation in this area has significantly slowed in recent years. So how can the U.S. jump-start its wireless innovation and build on its strengths in networking infrastructure (e.g. Cisco, Juniper, and Oracle) and Internet platforms (e.g. Facebook, Google, and Amazon)?

The U.S. needs to focus now on what follows 5G. A potentially useful model to follow is the 5G Public Private Partnership (5GPPP). In 2013, the European Union's Horizon2020 program committed 700 million Euro to an industry and university consortium to set requirements and hone technology leading to 5G. This investment attracted 3.5 billion Euro in matching funds from industry sources. The roadmap developed by 5GPPP was used by the United Nation's International Telecommunications Union and standards-setting body for cellular—the Third Generation Partnership Project. It set the stage for the development of standards and ultimately the production and deployment of products.

While it may seem early to start talking about 6G, each generation of mobile technology takes about 20 years to develop: 10 years of research and development, followed by 10 years of requirements, standards, implementation, and deployment. These phases are staggered, as shown in Figure 1. While 5G is being standardized, developed, and deployed, research into 6G is already underway, and with the accelerating pace of each generation, 6G commercial deployments could come as early as 2025. Potential advances in 6G could come from infusing artificial intelligence (AI) into every aspect of the system, from core network orchestration and optimization to using AI to create wireless signaling formats uniquely suited for specific deployment environments. Thus, the U.S.-China technology race in 5G and 6G will more than likely end up being inextricably linked to a similar race underway in AI. The window is closing for the U.S. to launch a major "Beyond 5G" initiative that could serve to catalyze the public and private R&D community to positively impact later versions of 5G and whatever ultimately becomes 6G. Investments of at least $2 billion a year would be needed to effectively tackle this problem with a public-private strategy.

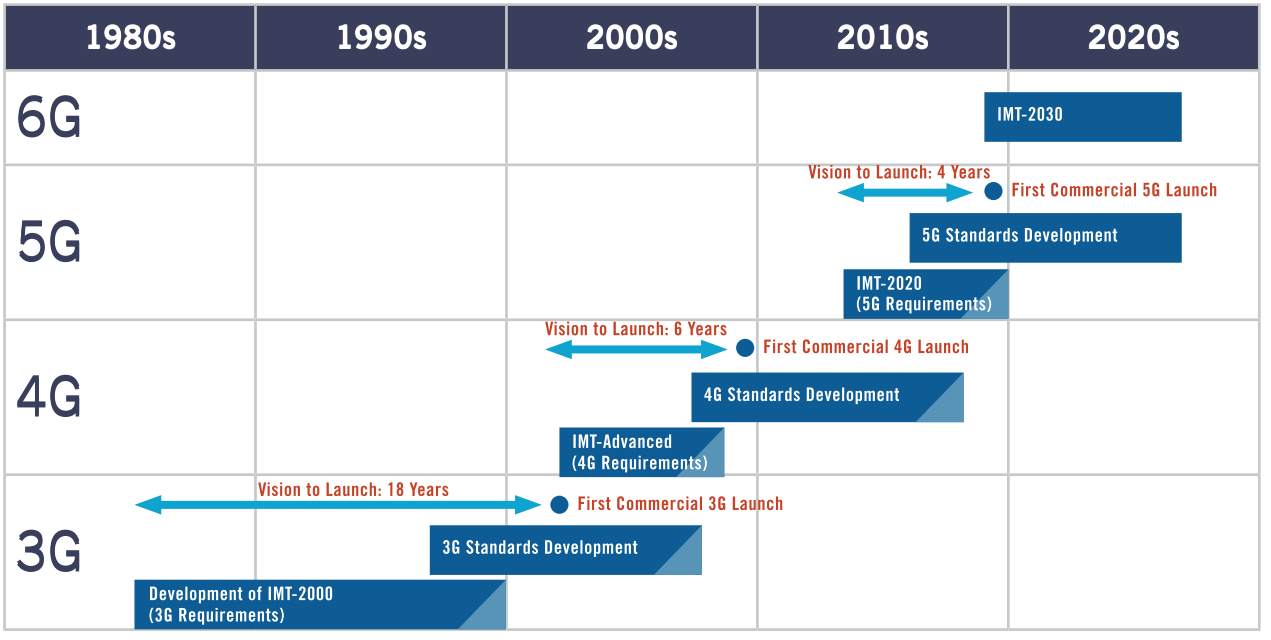

Figure 1. Cellular generations

Meanwhile, much of the economic opportunity with 5G is being driven by its applications in areas like IoT. While the U.S. may not be in a position to lead globally in 5G telecom equipment, there is still the opportunity to lead globally in areas like smart infrastructure (energy, cities, etc.), connected and autonomous vehicles, commercial drone technologies, and connected enterprises. It is in these areas where U.S. companies, with the help of government funding, can maintain and expand their leadership.

Specific aspects of a *Beyond 5G National Investment* Initiative should include:

- Identify an organization in the federal goverment to lead a whole-of-government strategy with an engagement structure that systematically leverages industry groups and trade associations.
- Expand programs within the National Science Foundation to invest in basic research and education programs in advanced telecommunications, with a particular focus on applications of artificial intelligence to wireless communications and networking.
- Launch applied research programs across the government to invest in applications of advanced telecommunications to their respective areas, from energy to transportation to agriculture. These programs should lead to demonstrations of how 5G can be meaningfully applied to their sector, and invest in closing technological, regulatory, and policy gaps to develop secure, reliable, and interoperable sector solutions.
- Develop proof-of-concept implementations of advanced telecommunications standards and make them publicly available to catalyze research, development, and commercialization.

- Create and execute a comprehensive strategy for engagement of standards development organizations (SDOs) across government, industry, and academia.

- Increase the federal R&D tax credit for work in advanced telecommunications, with emphasis on increased support for patent protection costs, SDO engagement, and small business investments.

- Leverage the Small Business Innovation Research (SBIR) and Small Business Technology Transfer (STTR) programs for focused investments in advanced telecommunications and provide supplemental funds for patent protection and SDO engagement, for 5G must leverage and combine multiple strategy dimensions. Ensure that these investments are connected with relevant federal programs have the resources to continue SBIR and STTR projects beyond their first phases.

- Follow through with emerging proposals from the new United States International Development Finance Corporation to invest in Western 5G solutions across the world[11].

Strategy 3: Security in Spite of China

The third broad class of strategies is to accept that Huawei, and other potentially untrusted infrastructure providers, will be a major part of the global telecommunications backbone. Given this assumption, the U.S. will need approaches that ensure security can be maintained even while these companies hold significant global market share. Banishing Huawei from the U.S. market does not necessarily offer safe harbor for domestic data, as demonstrated with China Telecom's ability to influence information routing on the U.S. Internet from its 10 points of presence in North America. Huawei equipment is not needed when China Telecom is a licensed Internet service provider within the U.S. To address this reality, the U.S. needs to get serious about adopting and expanding international norms for security on the Internet backbone. Others already have done so. The Mutually Agreed Norms for Routing Security community, for example, has established norms for routing security for the Internet that, if widely adopted, would prevent malicious route manipulation. The Federal Communications Commission could also reconsider China Telecom's license to operate in the U.S.

Another promising approach is to build secure overlay networks using 5G network slicing technology. One of the fundamental innovations in 5G is that its network infrastructure is entirely virtualized and software defined. This allows the composition of arbitrary networks to satisfy the needs of specific classes of users. Secure network slices can assess the security of the physical hardware over which virtualized infrastructure is implemented and help devices and services assess risk. Additionally, they can sequester important services from the mainline Internet and implement a whole range of static and active defenses against adversaries who are able to find their way into network slices.

At the level of the U.S. military services, zero trust networking (ZTN) is gaining traction. The basic idea is that cloud-based services have no inherent trust of devices. Instead, trust is incrementally built through attestation, multi-factor authentication, authorization, and network context. Based on the extent to which a device is trusted, a variable amount of access to services can be obtained. When ZTN is combined with network slicing, we begin to

[11] Alistair Barr, "U.S. to Tap $60 Billion War Chest in Boon for Huawei Rivals," Bloomberg, December 3, 2019.

have enough tools to quantify the trust level of users, devices, and network infrastructure. From that data, we can assess the level of access that should be granted. This intersection represents a unique opportunity for U.S. investment and commercialization.

Call to Action

Securing 5G is a complex topic, made more difficult by Chinese companies' increasing role in IP, standards, and global supply chain. But it's not impossible. And it's absolutely vital that the U.S. do so. A U.S. National 5G Strategy must be multi-faceted and seek to slow down global adoption of Chinese equipment, invest in and catalyze U.S. innovation beyond 5G technologies, and foster the development of technologies that can isolate critical services and enable variable levels of security.

To date, Congressional and Executive action have focused primarily on slowing China down, the effects of which are short term. While U.S. policy must continue to keep pressure on China to deny it unchecked freedom of navigation in the global marketplace, the U.S. must also make the corresponding domestic investments to be successful in the long run.

About the Author

Charles Clancy is vice president for Intelligence Programs in MITRE's Center for Programs and Technology. In this role, he leads the organization's technical strategy and priorities in support of the intelligence community. He has co-authored more than 250 patents and academic publications, as well as five books. Clancy is an internationally recognized expert on topics at the intersection of wireless, cybersecurity, and artificial intelligence.

Contributing Editors

Greg Grant, Director, The Center for Technology & National Security

James Swartout, Executive Director, The Center for Technology & National Security

About the Center for Technology & National Security

MITRE launched the Center for Technology and National Security (CTNS) to provide national security leaders with the data-driven analysis and technologically informed insights needed to succeed in today's hyper-competitive strategic environment. The Center aims to help policymakers better navigate a dynamic, rapidly evolving technology landscape in order to advance U.S. interests and strengthen national security. As a part of the not-for-profit, non-partisan MITRE Corporation, CTNS is built on the experience and expertise of thousands of our nation's most respected scientific and engineering minds. The Center brings together experts and leading authorities from government, academia, industry, media, and policy institutes to drive informed discussion in this era of unprecedented technological change.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

© 2019 The MITRE Corporation. All Rights Reserved.
Approved for Public Release; Distribution Unlimited. # 19-02806-1

MITRE

MITRE Center for Technology and National Security