Science and Technology Innovation Program

Wilson Center

Author
Melissa K. Griffith

5G and Security:

There is More to Worry About than Huawei

November 2019

5G and Security:

There is More to Worry About than Huawei

Given much of the recent coverage surrounding security and the fifth generation (5G) of cellular networks, you would be forgiven for assuming that security concerns are largely limited to China in general and Huawei in particular.

This is not the case.

Equally important are the concerns for United States' security that extend beyond Huawei's role in the development and deployment of 5G technology. Notably, while Huawei amplifies many pre-existing areas of concern, 5G would represent a significant challenge for American national security even if China was not a peer competitor in the market.

As a consequence, it would behoove policy makers, scholars, and industry leaders alike to recognize the breadth and character of national security concerns before advocating for specific policy solutions, especially those tailored largely to the threats posed by a single multinational technology company.

WHY IS 5G IMPORTANT?

5G, the "fifth generation" of mobile network technology, brings with it significant increases to bandwidth and the number of connections while decreasing latency. In plain English, 5G means faster connections and larger capacity than 4G networks allowed. Why do we care about faster connections and larger capacity? As the Eurasia Group highlights, 5G is the backbone upon which "next-generation digital applications that require highly reliable, near-instantaneous access to massive amounts of data" will be built. In short, 5G is a core foundation upon which modern societies – their economies and their militaries alike – will rest. It will be essential to how industries compete and generate value, how people communicate and interact, and how militaries pursue security for their citizenry. 5G is potentially one of the most important networks of the 21st century. It is the very definition of critical infrastructure.

WHAT ARE THE SECURITY CONCERNS?

Security, at its core, is a risk management problem. Solving that problem first requires a clear understanding of the risks. To that end, there are two broad categories of security concerns surrounding the development and deployment of 5G: (1) those that are intrinsic to 5G in general and (2) those shaped by the specific actors developing and deploying 5G in practice.

Security Challenges With or Without Huawei

It has often been said that software is "eating the world." Crucially, software brings with it increasing cybersecurity challenges, namely in the form of vulnerabilities or bugs.

As 5G networks transition telecommunications even further away from hardware to a largely software-based network, the corresponding security challenges are amplified. Software-based security challenges also increase as the complexity of that software increases. As a general rule of thumb, the number of latent defects grows exponentially with every increase in latent complexity. In other words, the more complex a software system, the more flaws. For 5G, the software in question is incredibly complex. And as Bruce Schneier warned us in 1999, "complexity is the worst enemy of security."

The transition to software in 5G has also limited the utility of several prior security methods. One central example is a lack of hardware chokepoints in 5G networks. 5G has moved away from the hub-and-spoke design toward distributed, software-defined digital routing. Now, rather than passing through a series of physical chokepoints, activity will be distributed throughout a web of digital routers across the network. Why does this matter? At the most foundational level, some traditional opportunities for inspection and control have decreased.

All technicalities aside, increasing reliance on software over hardware increases cybersecurity challenges. The more complex the software, the greater the security challenge.

But the story doesn't end there.

The fifth generation of cellular networks also lies at the center of the Internet of Things (IoT) – an ecosystem of connected devices. The explosive growth of IoT devices simultaneously increases both the potential attack surface of 5G networks and introduces specific software vulnerabilities of their own. As leading cybersecurity firms such as Symantec have pointed out on numerous occasions, ""security" is not a word that gets associated with this category of devices."

There are also severe supply chain security risks present in 5G. The latest iteration of telecommunications will rely on commercial company inputs across the stack from the network to the devices operating on that network. Concerningly, the entire life-cycle of development, deployment, operation, and maintenance of network infrastructure, services, and devices will introduce new potential sources of vulnerability and opportunities for malicious activity, intentionally or otherwise.

In short, even before Huawei enters the conversation, there are numerous cybersecurity challenges baked into 5G. Soberingly, as Tom Wheeler and David Simpson emphasized, "[t]o build 5G on top of a weak cybersecurity foundation is to build on sand." With or without Huawei, national security concerns - the reliability, availability, and integrity of 5G networks - must be addressed at this foundational level or we will, in fact, find ourselves building a central critical infrastructure on sand.

How Huawei Intensifies Risk

Security concerns associated with 5G can be amplified depending on who is developing and operating the technology in question. This 'who' of it all, takes on greater significance given China's place as a rising, geopolitical competitor to the U.S. and other like-minded states.

In a recent Lawfare article, cybersecurity experts underlined the importance of who develops and provides 5G: "Whoever provides the technology for 5G networks will be sitting in a position of incredible access and, thus, power. All data sent and received from a mobile device, smart home or even a car will pass through a network built with Huawei devices. These devices will be remotely controlled and updated, leading to exponential vectors of attack." Though China's dominance in 5G remains far from assured, market dominance is a source of power. One merely needs to look at a map of the underwater cables that connect the global internet for that reality to sink in.

That source of power becomes even more concerning when we factor in the domestic political environment in which Chinese companies operate. In comparison to companies like Ericsson, Nokia, and Samsung, Huawei operates in a political environment characterized by a lack of transparency, a different legal system, and greater opportunities for state influence in or coercion of industry players. Some analysts have gone so far as to coin 5G as "the newest battlefield between open societies and authoritarian regimes." Whatever catchphrase you chose to apply here, there are central and consequential differences regarding the relationship between industry and government in China.

On the more technical side, in addition to concerns over intentional vendor-installed backdoors and potential kill switches, Huawei product code is deeply flawed. In other words, its software is buggy. Buggy even in comparison to other market competitors. Huawei firmware has been revealed time and time again to contain critical vulnerabilities, a reality which we would be foolish to overlook. Whether malicious or just plain sloppy, as Jason Healey summarized, "there are countless cavernous holes" available for exploitation.

These cavernous holes have real security consequences. Yet, attempts to rectify them have been met with limited success. Notably, in their fifth annual report to the National Security Adviser of the United Kingdom, the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board could still "only provide limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks can be sufficiently mitigated long-term" (emphasis added). Even in the context of a country with a longstanding relationship with Huawei, risk mitigation efforts continue to fall short. Similar efforts by other countries are not faring better.

Given the known risks and the availability of potential "alternatives," what then is the appeal of Huawei technology? Economic incentives and security incentives driving 5G decisions are not well aligned. First, what Huawei sacrificed in quality, it made up for with the price tag. Second, even as security concerns rise, there are costs associated with carriers switching vendors. While the degree of cost is hotly debated, some experts have argued that "[i]t takes about two years to plan and implement such a technology shift and install the new equipment." Third, Huawei is, in actuality, one of the early leaders in this space. This has manifested in both research and deployment. On the development front, Huawei currently holds the most 5G standard essential patents in the world. Uniquely, regarding deployment within China, Chinese companies have been able to leverage China's massive domestic market and corresponding unrivaled population size as a means for setting global standards. In short, China invested early in development and has moved rapidly ahead with deployment at home and abroad at relatively low cost.

In summary, while Huawei is not the sole source of risk in 5G, its presence as one of the market leaders does, in fact, amplify many existing areas of concern. This risk takes on even greater significance given its position as a potential geopolitical competitor to the U.S. in the near future.

WHAT ARE THE IMPLICATIONS FOR U.S. NATIONAL SECURITY?

The U.S. is facing a domestic environment defined by critical interdependence: 5G will enable activity throughout society including but not limited to finance (e.g. mobile services), urban development and planning (e.g. smart cities), and transportation (e.g. driverless cars). As Meredith Attwell Baker summarized, "5G is the platform for tomorrow's economy."

5G's importance extends beyond the borders of the U.S. as well. As an example, a 2019 Defense Innovation Board report highlighted the critical nature of 5G networks to future U.S. military operations. Notably, even if the U.S. were able to both exclude Chinese technology and increase 5G security and resilience in its own territory, military operations abroad would still be reliant on the security and resilience of networks in place outside U.S. borders.

5G is the very definition of a single point of failure.

Therefore, two core policy questions should take center stage:

1. How can the U.S. not only increase the underlying security of the 5G ecosystem but also operate securely and reliably on inherently insecure networks?

2. How can the U.S. limit the dominance and influence of a rising geopolitical competitor in domestic and global critical infrastructure?

The latter question has animated much of the public discussion of 5G to date. But the former is equally as important, and remains essential to U.S. national security regardless of how successful we are at the latter.

Huawei in particular and China in general will most likely continue to play at least some role in the global 5G ecosystem now and in the future. However, even if the U.S. and like-minded countries manage to maintain telecommunications dominance in 5G and prevent the widespread use of Huawei technology at home and abroad, 5G would still be a deeply insecure critical infrastructure. A priority of U.S. policy makers, academics, and industry players alike must be to address that fundamental fact. As a consequence, any approach to security in 5G, therefore, must be far more nuanced than the 'Huawei or the Highway' articulation of security concerns would suggest. It will require the creation, maintenance, and operation of secure and resilient 5G telecommunications networks and for future generations of telecommunications networks to come.

In 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.

WOODROW WILSON INTERNATIONAL CENTER FOR SCHOLARS

The Woodrow Wilson International Center for Scholars, established by Congress in 1968 and headquartered in Washington, D.C., is a living national memorial to President Wilson. The Center's mission is to commemorate the ideals and concerns of Woodrow Wilson by providing a link between the worlds of ideas and policy, while fostering research, study, discussion, and collaboration among a broad spectrum of individuals concerned with policy and scholarship in national and international affairs. Supported by public and private funds, the Center is a nonpartisan institution engaged in the study of national and world affairs. It establishes and maintains a neutral forum for free, open, and informed dialogue. Conclusions or opinions expressed in Center publications and programs are those of the authors and speakers and do not necessarily reflect the views of the Center staff, fellows, trustees, advisory groups, or any individuals or organizations that provide financial support to the Center.

The Wilson Center

@TheWilsonCenter

@WoodrowWilsonCenter

www.wilsoncenter.org

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

Wilson Center