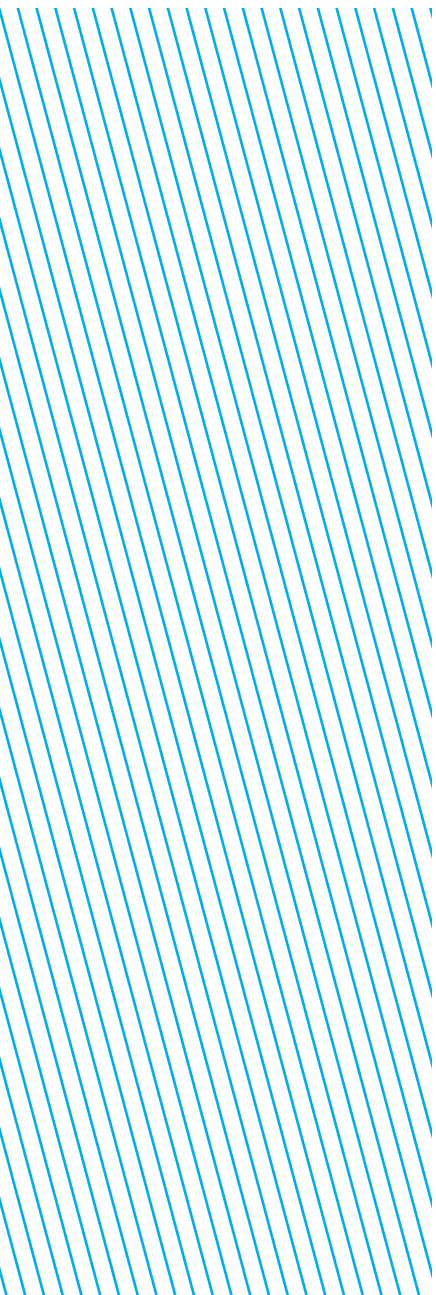

5G a S :

T M W A

H

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

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, nd ourselves building a central critical infrastructure on sand.

How Huawei Intensi es Risk

Security concerns associated with 5G can be ampli ed depending on who is developing and operating the technology in question. This 'who' of it all, takes on greater signi cance 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 in uence in or coercion of industry players. Some analysts have gone so far as to coin 5G as "the newest battle eld 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 awed. In other words, its software is buggy. Buggy even in comparison to other market competitors. Huawei rmware 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 fth 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 suf ciently 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 sacri ced 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 impacted 5G both in standards and deployment. On the development front, Huawei currently holds the most 5G standard essential patents in the world. Uniquely, r9r45og fone of the lm ( )]TJ ET EMC //0 ( )]TJ ET EMC /Span <<

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