Testimony of Dr. Charles Clancy

Bradley Professor of Cybersecurity, Virginia Tech

before the Senate Committee on the Judiciary, Hearing on 5G: The Impact on National Security, Intellectual Property, and Competition

May 14, 2019

Chairman Graham, Ranking Member Feinstein, and Committee Members:

My name is Charles Clancy and I am the Bradley Professor of Cybersecurity in the Department of Electrical and Computer Engineering at Virginia Tech. Over the past nine years at Virginia Tech I have led the Hume Center for National Security and Technology, which conducts advanced research in technology areas in support of defense and intelligence agencies, and prepares students for careers in national security through experiential learning and graduate research. Prior to joining Virginia Tech in 2010, I served as research leader for emerging mobile technologies the National Security Agency.

I am an internationally-recognized expert in wireless security and have held leadership roles within international standards and technology organizations. I have worked extensively with the wireless industry and Federal Communications Commission on topics related to cybersecurity. I am co-author to over 230 peer-reviewed academic publications, to include five books on digital communications; am co-inventor to over 20 patents; and am co-founder of four venture-back startup companies all focused in the wireless and security sectors.

It is my distinct pleasure to address this committee on topics of critical national importance.

5G Wireless

In the past year, 5G wireless technology has become “real”. Carrier deployments, consumer marketing, and the race to be first have brought significant attention to a collection of technologies that have been fifteen years in the making. 5G is significant not only because it will provide better broadband to mobile devices, but also because of its unique ability to enable the Internet of Things (IoT).

Additionally, 5G introduces many new security features, fixing gaps discovered in earlier generations of mobile technologies and creating a toolbox of features that embrace its “software-defined” philosophy to provide agile, extensible, and bespoke security to critical application areas like smart grid and connected cars.

Concerns about China

Technology changes and global economics have altered the telecom equipment supplier landscape going into 5G. Primary 5G equipment vendors are Nokia, Ericsson, Huawei, ZTE, and Samsung.

Chinese telecom company Huawei has skyrocketed from its early position as an imitator, famously being sued by Cisco in 2004 for stealing router source code, to an innovator, spending 1.5x more per year on research and development than Ericsson and Nokia combined. Huawei currently leads globally with a 28% market share[1].

First and foremost, China's primary motives surrounding Huawei and ZTE are economic. China's Belt and Road Initiative, for example, seeks to build transportation connectivity with trading partners, primarily through rail infrastructure and ports. Huawei and ZTE represent the digital version enabling e-commerce. The Chinese Development Bank underwrites these initiatives, providing inexpensive credit to finance major infrastructure investments. Anecdotally this leads to Huawei bids for major telecom projects coming in 40% lower than competitors.

China's economic dominance creates a number of national security concerns.

First, China is investing heavily in surveillance technologies. For example, China is deploying AI-enabled face recognition technologies fueled by 5G connectivity that can track movements of individual people throughout population centers. Huawei and ZTE are exporting these technologies to repressive regimes globally, such has Mongolia, Ethiopia, Zimbabwe, Malaysia, and Ecuador[2].

Second, China has sufficient penetration into the global Internet that it can revector large swaths of the world's Internet backbone traffic, either causing targeted disruption of the Internet, or completely disabling the global Internet. China Telecom uses insecurities in the Internet backbone's routing system, known as BGP, to routinely hijack segments of the Internet. In 2010, China Telecom famously hijacked 15% of the Internet for a total of 18 minutes. There are countless recent targeted attacks, such as hijacking traffic between the Canadian and South Korean governments, traffic between the US and a European bank, and traffic of an American news organization between Europe and Japan[3]. Huawei's global footprint can

[1] Dell'Oro Group, "Key Takeaways – The Telecom Equipment Market 3Q 2018", http://www.delloro.com/delloro-group/key-takeaways-telecom-equipment-market-3q-2018

[2] S. Romaniuk, T. Burgers, "How China's AI Technology Exports Are Seeding Surveillance Societies Globally," The Diplomat, October 18, 2018, https://thediplomat.com/2018/10/how-chinas-ai-technology-exports-are-seeding-surveillance-societies-globally/

[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), 2018, https://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1050&context=mca

give China the ability to expand these attacks in more surgical, less detectible, and less attributable ways by leveraging not only China Telecom points of presence, but points of presence from other operators that include Huawei equipment.

Lastly, Huawei and ZTE equipment could be used to secretly surveil Internet traffic or be used as a launching point to enable a cyber attack on targeted computer systems. Remote access into a Huawei Internet router or 5G base station, for example, could allow targeted collection of data and metadata or be used to execute man-in-the-middle attacks that can inject a virus into a victim computer or defeat the encryption underpinning the web. Additionally, compromised devices can act as a global botnet stitched into the fabric of the Internet itself, able to execute large-scale, distributed denial of service attacks, or serve as a system of waypoints for smuggling intellectual property and state secrets out of sensitive networks.

Smoking Gun

As the US urges allies, partners, and domestic telecom operators to eschew Chinese equipment, many want to see the smoking gun: concrete proof that Huawei has operated on behalf of the Chinese Communist Party (CCP) to hack something somewhere.

As early as 2009, Vodafone identified back doors in Huawei equipment that would give the company remote access into some of its European networks. Vodafone worked with Huawei to close these holes, but it took several years to fully address the problem[4]. However, it is difficult to identify this as a "smoking gun" as during the same time period, many other products were discovered to have similar flaws, including Cisco, Sony, and D-Link[5]. Somewhat hypocritically, the Cisco vulnerability was only discovered because it was part of the CIA Vault 7 leak to WikiLeaks[6].

In 2012, China gifted the African Union a headquarters building in Addis Ababa that included a state-of-the-art telecom system based on Huawei equipment. Five years later it was discovered that every

[4] T. Culpan, "The West Finally Has its Huawei Smoking Gun," Bloomberg, April 30, 2019, https://www.bloomberg.com/opinion/articles/2019-04-30/huawei-backdoors-found-by-vodafone-are-a-smoking-gun

[5] J. Sanders, "Evidence of Backdoors in Huawei Equipment Collapse Under Light Scrutiny," Tech Republic, May 2, 2019, https://www.techrepublic.com/article/evidence-of-backdoors-in-huawei-equipment-collapse-under-light-scrutiny/

[6] B. Vigliarolo, "Think your Cisco switch is secure? Think again: Hundreds are vulnerable to a simple attack," Tech Republic, March 22, 2017, https://www.techrepublic.com/article/think-your-cisco-switch-is-secure-think-again-hundreds-are-vulnerable-to-a-simple-attack/

night network traffic spiked as data from the network was sent back to China[7]. However it is unclear that Huawei uniquely enabled this attack, as the Peoples Liberation Army (PLA) could have put in place advanced persistent threat toolsets without vendor knowledge or cooperation.

Huawei has many documented hijinks around intellectual property theft, such as Huawei's internal policy that provided cash bonuses to employees who steal intellectual property from competitors. This policy led to the physical theft of a robotic testing arm named "Tappy" from a T-Mobile testing lab in Seattle in 2013[8]. While clearly inconsistent with US values and law, they point to Huawei's financial motives.

Like many other vendors, Huawei's race to be first to market means their code has bugs. The most recent report from the Huawei Cyber Security Evaluation Centre Oversight Board in the UK indicates a wide range of security issues with Huawei products[9] stemming from poor software development and engineering procedures. This may make Huawei equipment generally more vulnerable to hackers, regardless of any specific collusion with the CCP.

With this in mind, and putting aside questions of global competition, why should we be uniquely worried about Huawei and ZTE?

First, the CCP has a unique relationship with Huawei and ZTE, from mandatory CCP membership for executives, to laws that could compel Huawei and ZTE to aid the government in matters of national security. Regardless of whether these relationships have affected Huawei and ZTE behavior in the past, they could affect it in the future, and these risks do not exist with other vendors. A well-documented track record of intellectual property theft reinforces a willingness to operate outside international norms.

Second, independent of any direct cooperation or support, proximity, indigenous product ubiquity, and flow of human capital indicates that the PLA probably has a bigger arsenal of cyber weapons that build on top of Huawei and ZTE products than on top of other vendors.

[7] A. Dahir, "China Gifted the African Union a Headquarters Building and then Allegedly Bugged it for State Secrets," *Quartz*, January 30, 2018, https://qz.com/africa/1192493/china-spied-on-african-union-headquarters-for-five-years/

[8] USA v Huawei, "Theft of Trade Secrets Conspiracy," Indictment CR19-010, US District Court, Filed January 16, 2019, https://www.documentcloud.org/documents/5698470-Huawei-Indictment.html

[9] Huawei Cyber Security Evaluation Centre Oversight Board, "Annual Report: A report to the National Security Adviser of the United Kingdom," July 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf

Lastly, while we may not have discovered a malicious back door in products today, a software update pushed to the global install base could add one after-the fact. Additionally, in many parts of the world, Huawei employees actually operate and manage the equipment on behalf of the host telecom company; a back door is not needed if you already have a key to the front door.

Recommendation – Internet Routing Security

The routing fabric of the Internet needs to be resilient to Chinese manipulation, whether executed via China Telecom points of presence or via exploited Huawei and ZTE routers worldwide. Currently the best we can do is monitor the Internet routing tables to identify anomalies and seek to attribute them to bad behavior. However even when detected, this bad behavior has no real consequences. It is generally quantified in terms of failing to meet service level agreements with peering partners, and not in terms of maliciously attempting to hijack segments of the Internet to deny service or surveil traffic. There need to be real accountability for manipulating the fabric of the Internet. Frequency of these attacks is increasing, not only by nation states, but also by criminals looking to steal cryptocurrency[10].

A relatively new organization, Mutually Agreed Norms for Routing Security (MANRS) is one starting point where members work together to filter and validate Internet routing information to prevent hijacks from being as successful. Technical solutions exist to validate the authenticity of routing data, including database cross-validation and digitally signing routing data, but in practice databases are not kept up to date and less than 13% of routes use digital signatures[11]. These technical solutions, combined with agreed-upon and enforced norms, would go a long way to closing these gaps.

Recommendation – Securing US 5G Infrastructure

Much anxiety in the US surrounds whether domestic carriers can deploy secure 5G infrastructure in the face of China's rise to prominence. Currently US carriers have plans that leverage Nokia, Ericsson, and Samsung equipment for core network infrastructure. Some interesting questions remain at the fringes however: Can a hospital or college campus buy Huawei smallcells and deploy them as part of an enterprise 5G network? What about ZTE cell phones? Carrier commitments are only part of the story in a more

[10] A. Siddiqui, "What Happened? The Amazon Route 53 BGP Hijack to Take Over Ethereum Cryptocurrency Wallets," Internet Society Blog, April 27, 2018, https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/

[11] NIST, "Global Prefix/Origin Validation using RPKI," RPKI Monitor, April 18, 2019, https://rpki-monitor.antd.nist.gov/

complex deployment environment. Ultimately it comes down to risk management. What is the criticality of the services delivered over the network, and how should the network be constructed to ensure those services are delivered as expected?

One lens through which to view this issue is 5G network slices. 5G anticipates defining separate network slices for different IoT services, and these slices can have unique security properties. One emerging concept is that the supply chain for the underlying networking, storage, and compute resources being composed to virtually provide services can be taken into consideration. For particularly sensitive network slices only the most trusted hardware could be allowed. Trusted computing standards could give both the network and edge devices the ability to audit virtual configurations to ensure the trust of underlying hardware.

Implementation of techniques such as this would require research, development, implementation, and testing. For critical infrastructure sectors, the associated sector-specific agency would need to weigh in with security best practices and standards for secure slices serving their sectors. Testing would be greatly enabled by establishing a National 5G Security Testbed anchored by NIST, and in partnership with broader government stakeholders, industry, and academia.

Recommendation – US Telecommunications Competitiveness

The United States needs to make investments in research, development, and innovation that will ensure domestic leadership moving forward, particularly focused on 6G. Each generation of wireless technology takes around 15 years from early-stage research to standards and ultimately to deployment. The clock for 6G started a few years ago. If 5G is defined as being "cloud native", by its deployment in the late 2020s, 6G will be "AI native" and possibly "quantum native".

Immediately, basic research sponsors like the National Science Foundation should focus investments not only on applications of 5G but also on core enabling technologies for 6G. Given the opportunity for significant value to the Department of Defense, defense science and technology organizations like DARPA should also be making immediate investments. The connections to other key disruptive technologies like AI and quantum will allow existing, aligned investments in those areas to bolster impact in 6G research.

By 2021, the US should launch a major convening and applied research investment in 6G, similar to the EU's 5G Public Private Partnership (5GPPP). 5GPPP was launched in 2013 and leveraged €700M in public funding against more than €3.5B in private funding. The initiative was fuel that organized Europe in a coherent research direction and developed the use cases for 5G that ultimately informed the standards definition. If the US does not lead the world in a 6GPPP-like initiative, China will.

The intellectual property that is generated by these initiatives must be captured, protected, licensed, and commercialized. In the same way that Bell Labs served as the innovation engine that fueled US telecommunications leadership for half a century, well aligned investments in translational research can create a "telecom Silicon Valley" that will nurture the startups that will become tech powerhouses over the next decade.

Thank you for the opportunity to address the committee today and I look forward to questions.