SUBMITTED STATEMENT FOR THE RECORD OF

KATHRYN WALDRON

FELLOW, NATIONAL SECURITY AND CYBERSECURITY

R STREET INSTITUTE

KRISTEN NYMAN

SPECIALIST, GOVERNMENT AFFAIRS

R STREET INSTITUTE

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS

HEARING TO

EXAMINE SUPPLY CHAIN SECURITY, GLOBAL COMPETITIVENESS, AND 5G

OCTOBER 31, 2019

DEAR CHAIRMAN JOHNSON, RANKING MEMBER PETERS AND MEMBERS OF THE COMMITTEE:

Thank you for holding this important hearing on supply chain security, global competitiveness and 5G. In today's world, supply chain integrity is a crucial component of American national security. With the promise of reduced latency and increased speeds, the development of 5G will only expand the number of ways we incorporate technology in our daily lives. However, this deeper incorporation of technology in the fabric of our society also presents adversaries with a multitude of new opportunities for malicious activity, potentially creating new security vulnerabilities. When seeking to mitigate these vulnerabilities, policymakers should identify solutions that equitably promote the competitiveness of American companies in the global market. A failure to balance these priorities could harm both the United States' economy and its national security.

Our names are Kathryn Waldron and Kristen Nyman, and we are members of the National Security and Cybersecurity team at the R Street Institute. The R Street Institute is a nonprofit, nonpartisan public policy research organization whose mission is to engage in policy research and outreach to promote free markets and limited, effective government. Our scholars write extensively on the national security threats posed by cybersecurity and emerging technology.

Supply Chain Risks

Supply chain security has become an increasingly important issue over the past decade. Cyber breaches like the 2013 Target hack (via stolen passwords from a HVAC provider in Target's supply chain) have highlighted the need to enact cybersecurity controls at all levels of the supply chain.[1] A 2019 report from cybersecurity company Carbon Black found that half of all malicious cyber activities involve "island hopping," where hackers use a vulnerable point in a company's network to access their entire supply chain.[2] Yet determining which companies present a supply chain risk can be difficult. As our scholars explain in R Street's *R Sheet* on the topic, "Supply chain security is highly context-dependent, and requires a realistic appraisal of threats and vulnerabilities on a case-by-case basis. No federal department or agency is solely responsible for addressing the risk that the federal government faces, and at present, no national body effectively addresses the supply chain risks faced by state and local governments and the private sector."[3]

In the realm of telecommunication, this cybersecurity awareness should be paired with a heightened wariness of Chinese companies like Huawei and ZTE. The growing distrust of Chinese

[1] Brian Krebs, "Target Hackers Broke in Via HVAC Company," *Krebs On Security*, Feb. 5, 2014. https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.
[2] "Global Incident Response Threat Report," Carbon Black, April 2019. https://www.carbonblack.com/global-incident-response-threat-report/april-2019/.
[3] Kathryn Waldron and Paul Rosenzweig, "R Sheet on Supply Chain Security," R Street Institute, May 2, 2019. https://www.rstreet.org/2019/05/02/r-sheet-on-supply-chain-security/.

companies is hardly surprising given these companies' histories of intellectual property theft and alleged violations of American sanctions against Iran and North Korea.[45] Compounding these issues are recent laws that expand the Chinese government's ability to force Chinese companies into providing access to customer information. As the R Street team stated previously, "In light of the country's legal structure, it would be fair to say that Chinese-based companies operating in China may be said to operate purely by the grace—and under the strong influence (if not the clear control)—of the Chinese government."[6]

Policymakers seeking to curtail the Chinese government's access to American systems and information are rightly raising alarm bells about the use of Chinese products by U.S. government employees. But while the 2019 National Defense Authorization Act banned the federal government and its contractors from using Huawei or ZTE technology without a waiver, the small number of global companies engaged in 5G technology has limited the United States' ability to pressure allies to do likewise, thus limiting policymakers' abilities to keep the Chinese companies from building an even greater presence in the global telecommunications network.

An outright ban on bad actors with market shares as pervasive as Huawei's and ZTE's is unstainable in the long term, given the global nature of telecommunications networks. In Latin America, for example, Huawei has become a leading service provider, and the Chinese company has announced plans to create 5G telecommunications infrastructure in Argentina and Mexico as early as 2020.[7] The United States cannot avoid interacting with countries who use Huawei technology. Therefore, at some level, it is impossible to avoid American data interacting with technology from these problematic providers. Instead of avoiding it altogether, the United States should pressure the providers to change their practices. Indeed, Congress would do well to first, reexamine its hardline posture towards these and any other potentially hostile providers, and second, create a market environment that fosters competition to provide viable alternative providers.

Global Competitiveness

Economic gain is inextricably linked with national security, and it is important to achieve both of those objectives simultaneously. Several studies have shown that increased market competition can actually promote cybersecurity as companies seek to use security as a means of

---

[4] Claire Ballentine, "U.S. Lifts Ban That Kept ZTE From Doing Business With American Suppliers," *The New York Times*, July 13, 2018. https://www.nytimes.com/2018/07/13/business/zte-ban-trump.html.

[5] Kate Conger, "Huawei Executive Took Part in Sanctions Fraud, Prosecutors Say," *The New York Times*, Dec. 7, 2018. https://www.nytimes.com/2018/12/07/technology/huawei-meng-wanzhou-fraud.html.

[6] Paul Rosenzweig and Kathryn Waldron, "Broadening the Lens on Supply Chain Security in the Cyber Domain," R Street Institute, April 15, 2019, p. 3. https://www.rstreet.org/2019/04/15/r-street-policy-study-no-170-broadening-the-lens-on-supply-chain-security-in-the-cyber-domain/.

[7] Oliver Stuenkel, "Huawei Heads South," *Foreign Affairs*, May 10, 2019. https://www.foreignaffairs.com/articles/brazil/2019-05-10/huawei-heads-south

setting apart their products and branding. As our R Street colleague Charles Duan writes, "Computer security is a value-added benefit to consumers, so firms in competitive markets are likely to use security improvements to gain an edge over their competitors, and are likely to poke holes in their competitors' products to draw consumers away from them. By contrast, monopolized markets offer less external impetus to test products for flaws, and a monopolist may choose to focus less on security and more on new product features or increased product quality."[8]

Encouraging competition also prevents the creation of a "monoculture." When a single vendor (or a limited few) captures the entire market, there is no diversity of technological infrastructure. This means hackers who exploit one flaw can bring down entire systems with no practical alternative to which victims can switch. As Duan states,

> In the case of 5G or the Internet of Things, a monoculture is an especially concerning possibility. To the extent that systems such as smart city sensors or communication networks are widely deployed in a monoculture fashion, a widespread attack could have devastating consequences, potentially blacking out a region and affecting essential services such as 911. A monoculture that is vulnerable to so-called "rootkits" or "backdoors"—maliciously installed softwares that enable bad actors to commandeer systems—could also enable mass surveillance or spying by private hackers or foreign governments. The presence of systems from multiple vendors would mitigate these possibilities.[9]

Policy Recommendations

Supply Chain Risks Policy Recommendations

A paper published by R Street's National Security and Cybersecurity team earlier this year promotes these steps for addressing supply chain risks:

- "The National Security Council should prioritize the overall issue of supply chain integrity and support the work of the Federal Acquisition Security Council to make sure that it achieves its objectives.
- "The Federal Communications Commission should conduct a series of public hearings between now and the end of 2020 regarding the supply chain threat to the telecommunications infrastructure of the United States and its foreign partners, how best to mitigate those threats and how best to recover from malicious activity directed against such infrastructure.

---

[8] Testimony of Charles Duan, Senate Committee on the Judiciary, "5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation," 116th Congress, May 14, 2019. https://www.rstreet.org/2019/05/23/5g-national-security-concerns-intellectual-property-issues-and-the-impact-on-competition-and-innovation-submitted-statement-of-charles-duan/.

[9] Ibid.

- "The president should request that the U.S.-China Economic and Security Review Commission conduct an evaluation of supply chain risk from all Chinese-owned manufacturers.
- "Congressional leaders should immediately designate one committee in each house of Congress as the lead for conducting oversight of the federal government with respect to supply chain risk management, hold hearings on the topic with input from a broad range of witnesses in the public and private sectors, and propose legislation to address identified gaps in the law. The designated committees should be instructed to complete their work no later than September 2021.
- "Thematically, the U.S. government and other supply chain consumers should broaden their lens to consider supply chain risks in a more holistic manner. To date, the threat definition has been limited mainly to only two countries (Russia and China) and only to companies that appear to be wholly controlled by or connected to a foreign government. However, a more nuanced threat assessment would recognize risks that arise from other countries and also from supply chain providers whose connections to a foreign government are more indirect. This is not to suggest that those risks are absolute but rather to say that a serious risk allocation policy would more broadly assess the scope of threats to supply chain assurance."[10]

Global Competitiveness Policy Recommendations

In terms of promoting emerging technology markets, R Street Technology and Innovation Director Charles Duan recommends the following policies:

- "This Committee should seek to reduce barriers that prevent new firms from entering markets, and avoid efforts to stymie new entrants. Competition promotes better cybersecurity in at least two ways. First, multiple studies show that competition encourages firms to improve their products on multiple vectors, including cybersecurity. Second, competition avoids a situation that security experts call a 'monoculture,' which increases vulnerability to severe cyberattacks.
- "The Committee should look to curtail anticompetitive practices within industries. Given that competition offers benefits to cybersecurity and innovation, this Committee and Congress should focus on promoting competition and removing entry barriers in new technology markets, especially among domestic firms. This focus is especially important because incumbent firms have long advocated, and continue today to advocate for policies that effectively ask the government to pick winners and losers, to create artificial barriers

[10]Paul Rosenzweig and Kathryn Waldron, "Broadening the Lens on Supply Chain Security in the Cyber Domain," R Street Institute, April 15, 2019, pp. 12-13. https://www.rstreet.org/2019/04/15/r-street-policy-study-no-170-broadening-the-lens-on-supply-chain-security-in-the-cyber-domain/.

to entry for newcomer competitors, and to allow for monopolization that diminishes incentives toward product quality and security

- "The Committee should consider the ways in which regulatory barriers to the use of new technologies can have a disproportionate impact on small firms and thus unintentionally entrench incumbents, potentially to the detriment of cybersecurity. This is not to say that any regulatory efforts ought to be avoided per se, but they do need to be considered carefully to the extent that they could present barriers to new entrants or barriers to strong competition. And in particular with regard to cybersecurity, attention must be paid to whether regulatory schemes may interfere with private development of cybersecurity technologies and norms. Industry working groups have long been developing consensus views on cybersecurity practices for 5G and the Internet of Things. Robust industry collaboration on cybersecurity depends on high levels of competition and thus low barriers to entry that foster competition."[11]

We thank the committee for its recognition of the importance of supply chain security in the impending wake of disruptive technologies like 5G. If we can be of any assistance to members of the committee, please feel free to contact us or our colleagues at the R Street Institute.

Kathryn Waldron
Fellow, Cybersecurity and National Security
kwaldron@rstreet.org

Kristen Nyman
Specialist, Government Affairs
knyman@rstreet.org

[11] Charles Duan, "5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation," R Street Institute, May 14, 2019. https://www.rstreet.org/wp-content/uploads/2019/05/testimony-iot-cybersecurity-2.pdf