Free markets. Real solutions.

R STREET POLICY STUDY NO. 170
April 2019

BROADENING THE LENS ON SUPPLY CHAIN SECURITY IN THE CYBER DOMAIN

By Paul Rosenzweig and Kathryn Waldron

CONTENTS

INTRODUCTION

Supply chain integrity in the public and private sectors is a vital component of American national defense. For years, American policy has recognized the need for supply chain assurance regarding critical components of the national defense base. It forms, for example, the fundamental ground for federal legislation that allows the president to block transactions that involve foreign investment in American companies that are part of our defense industrial base.[1] To be clear, America does not and indeed, should not seek independence in an interconnected world, but we do seek supply chain assurance—the certainty that raw materials and manufactured components that are vital to our national defense and homeland security do not depend too extensively on availability from more-risky, non-American (and more particularly, unfriendly, non-American) sources.

America's concern over supply chain security was born of the Cold War, from a time when our adversaries were ideological and the means of conflict were often overt and kinetic. Today, our adversaries are motivated both by ideology and by mercantilism, and the means of conflict are more often covert and non-kinetic in nature. If and when an unrecognized system flaw is exploited to disable a portion of the American electric grid or to disrupt command-and-control communications during a crisis, the reality of non-kinetic supply chain dependence and risk will be realized, with potentially disastrous consequences for society.

At this juncture, American policy seems to approach the issue of supply chain assurance in a somewhat erratic manner. In some cases, seeing threats, we react with an extreme response—one that, effectively, blacklists companies and often entire nations.[2] In other cases, however, where the integrity of the hardware and software in American systems might be of concern, we respond like the proverbial ostrich, with our heads in the sand, ignoring obvious questions that need to be asked and answered.

Neither approach is optimal. To be sure, some risks are so great that an outright ban may be appropriate. But more often, the incorporation of foreign-made products into American systems should be evaluated through the prism of risk—for example, by considering how great the threat is; how significant the vulnerability; what the consequences of failure may be; and the costs of mitigation. One can readily

1. "The Committee on Foreign Investment in the United States (CFIUS)," U.S. Dept. of the Treasury, accessed April 5, 2019. https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

2. For one recent example, consider the decision to ban Kaspersky anti-virus products from all federal systems. Initially an executive policy, the decision was soon embodied in congressional legislation (H.R. 2810, National Defense Authorization Act for Fiscal Year 2018, 115th Cong.). When Kaspersky challenged the decision in court, the exercise of federal discretion was upheld. (*Kaspersky Lab, Inc. v. United States Department of Homeland Security*, 909 F.3d 446 [D.C. Cir. 2018]). Today, a similar dynamic is playing out with respect to Huawei components (See H.R.5515, John S. McCain National Defense Authorization Act for Fiscal Year 2019, 115th Cong.).

imagine some situations (think of our nuclear deterrent triad) where the slightest risk of compromise is too great. And there are others where the risks of failure are outweighed by the anti-competitive costs of prohibition.

Accordingly, the present study begins by outlining the legal framework within which supply chain issues arise. We then examine six cases (three well-known and three less well-known) where foreign government engagement has raised suspicion as to the integrity of these corporate products and we conclude with a series of policy recommendations for consideration by Congress and the executive branch.

THE ROLE OF THE CFIUS

In general, international trade and foreign direct investment are highly beneficial to the economic growth of all nations involved. For this reason, overly protectionist policies should not be justified in the name of national security when the true motivation stems from the jockeying of domestic special interests. For its part, the United States has traditionally advocated for reducing barriers to trade and benefited accordingly. However, there are times when a particular business deal has a negative impact on American security. In particular, mergers, acquisitions or takeovers involving foreign companies, particularly state-owned ones from nations with whom the United States has strained or hostile relations, can often raise red flags.

The Committee on Foreign Investment in the United States, also known as CFIUS, is the federal inter-agency committee that was created in 1975 to assess the national security implications of business deals that involve foreign entities. It is chaired by the Secretary of the Treasury and includes the Secretaries of Homeland Security, Commerce, Defense, State, Energy and Labor, the Attorney General, the Director of National Intelligence, the U.S. Trade Representative and the Director of the Office of Science and Technology Policy.[3]

The committee primarily gained its modern shape through three statutes: the 1988 Exon-Florio amendment, which grants the President the ability to block any foreign investment deemed a national security threat by the committee; the Foreign Investment and National Security Act of 2007 (FINSA), which increased Congressional oversight of CFIUS; and the Foreign Investment Risk Review Modernization Act Of 2018 (FIRRMA), which expands the scope of transaction types CFIUS has the jurisdiction to review, in addition to other reforms.[4]

Its process is fairly straightforward. If companies believe a business deal might have ramifications for national security, they file a voluntary notification with the CFIUS. Upon receiving such notification, it has 45 days to review the deal. Although the majority of deals are approved in this first period, if security concerns do arise, a second, forty-five day investigation is allowed. During this time, the CFIUS may negotiate with the companies in question to resolve risks. At the end of this second investigation period, CFIUS can recommend that the president disallow the transaction. The president then has fifteen days to decide whether or not to block it. To justify blocking a transaction, the president must have "credible evidence" that the transaction will endanger national security and that current laws are insufficient to mitigate the risk posed.[5]

The CFIUS can also retroactively review deals where no voluntary notification was filed. If a national security risk is discovered, the president can require divestiture or other actions from the parties involved.[6]

Over the past few years, the number of CFIUS notifications has grown tremendously. According to a report from the Government Accountability Office, "the committee reviewed over 50% more transactions in 2016 than in 2011."[7] In 2017, approximately 240 notifications were filed, 40 percent of which were investigated. However, only five transactions have been blocked by presidents since the committee's creation. Two of these were blocked by President Trump. In 2017, he blocked Canyon Bridge Capital Partners from acquiring Lattice Semiconductor. And in 2018, he blocked the Singaporean company Broadcom from taking over Qualcomm.[8]

CASE STUDIES

Central to effective risk management is a clear-eyed understanding of the factual grounds for decision-making rather than a broad-brush, one-size-fits-all categorical risk assessment. And, with respect to supply chain assurance, it is highly context-dependent and requires a realistic appraisal of threats and vulnerabilities on a case-by-case basis.

To that end, in the following sections, we examine six companies whose products could potentially pose a national

3. "Overview of the CFIUS Process," Latham & Watkins LLP, May 5, 2017. https://www.lw.com/thoughtLeadership/overview-CFIUS-process.

4. Jonathan Wakely and Andrew Indorf, "Managing National Security Risk in an Open Economy: Reforming the Committee in Foreign Investment in the United States," *Harvard National Security Journal* 9 (2018). https://harvardnsj.org/wp-content/uploads/sites/13/2018/06/WakelyIndorf_CFIUS_05.28.18.pdf.

5. Jonathan Masters and James McBride, "Foreign Investment and US National Security," Council on Foreign Relations, Aug. 28, 2018. https://www.cfr.org/backgrounder/foreign-investment-and-us-national-security.

6. Ibid.

7. "Committee On Foreign Investment In The United States: Treasury Should Coordinate Assessments of Resources Needed to Address Increased Workload," U.S. Government Accountability Office, Feb. 14, 2018. https://www.gao.gov/products/GAO-18-249.

8. Masters and McBride. https://www.cfr.org/backgrounder/foreign-investment-and-us-national-security.

security risk if they continue to be used by federal and state government employees. It should be noted that our concern is not limited to government systems. Many of the same concerns would apply in the private sector where critical infrastructure is managed. While in some cases the exact threat level remains unclear, the evidence is sufficient to justify each department and agency taking a closer look at the products used in their own supply chain and assessing them for possible vulnerabilities.

When evaluating the risks posed by a specific supplier, we recommend looking at four key factors:

1. The sensitivity of the information in question;
2. The criticality and pervasiveness of the infrastructure at risk;
3. The history and structure of the supplier, including previous instances of cyber espionage and close ties with hostile foreign government entities or figures and;
4. The history and legal structure of the supplier's home country, including the likelihood said supplier could be forced by a hostile foreign government to allow access to data that violates the privacy of Americans.

The first two factors are especially crucial for agencies or state-level government departments with smaller budgets, for whom replacing current products or seeking friendlier suppliers may be prohibitively expensive. The acceptable amount of risk for the Department of Defense's weapons systems (or even its unclassified data holdings) and a city's local subway system will differ widely, just as would the damage caused by hostile hackers in a successful cyberattack upon each.

While supply chain vulnerabilities can, of course, come from any country, the companies of two specific countries deserve close attention—China and Russia—precisely because the legal frameworks within which those companies operate are fraught with national security risks for the United States.

China

In November 2016, the Chinese government passed the Cyber Security Law of the People's Republic of China, also known as the China Internet Security Law. It took effect on June 1, 2017 and forced network operators to cooperate with Chinese government officials investigating crime or security issues and granted government agencies the authority to fully access data or remotely conduct penetration testing. Moreover, cloud service providers that provide service in China are now required to build their programs within Chinese territory and to store data from services targeted at Chinese users in Chinese storage facilities. The law also impacted the use of virtual private networks (commonly called VPNs) and telecommunications firms must now seek approval to provide VPN services in China.

"Critical information infrastructure operators" face the strictest restrictions, although exactly what firms count as such is not precisely defined. These operators are required to store personal information and important data collected and generated in China within mainland China. The law further stipulates that "if transmission of such data out of China is necessary due to business needs, clearance procedures shall be followed according to separate rules formulated by the Cyberspace Administration of China."[9] Indeed, the Cyberspace Administration of China was created to implement and enforce the new law.

Supply chain risks must also be evaluated in light of the recently passed National Intelligence Law, which was enacted June 27, 2017, and expands the Chinese government's authority to monitor both foreign and domestic individuals and organizations. It grants legal authority to "National intelligence work institutions," including both the Ministry of National Security and the Internal Security Bureau of the Ministry of Public Security, to search premises and seize property when conducting defensive espionage. This new law raises concerns about increased surveillance and appears to grant the government access to previously private data. Article 14 of the law requires both organizations and individuals to cooperate with government intelligence institutions upon being asked. Further, those who violate the new intelligence law are subject to detention of up to 15 days, and can be charged with a crime.[10]

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. And, this legal structure bears on the national security vulnerability that attends the use of any Chinese supplier.

Huawei—The most well-known example of a problematic Chinese supplier, currently receiving a great deal of public and governmental attention, is the telecom company Huawei, which is an information and communications technology firm based in Shenzhen, China and is one of the world's largest phone providers.[11] Huawei also sells a wide variety

9. "Understanding China's Cybersecurity Law," Ministry of Foreign Affairs and Trade, and New Zealand Trade and Enterprise, September 2017. https://www.mfat.govt.nz/assets/China/Understanding-Chinas-cybersecurity-law.pdf.

10. Staff, "What you need to know about China's intelligence law that takes effect today," *Quartz*, June 28, 2017. https://qz.com/1016531/what-you-need-to-know-about-chinas-intelligence-law-that-takes-effect-today.

11. "Corporate Information," Huawei Technologies Co., Ltd., 2019. https://www.huawei.com/us/about-huawei/corporate-information.

of other goods. In fact, the U.S. Dept. of Justice recently referred to it as "the world's largest telecommunications equipment manufacturer."[12]

The firm was started in 1987 by Ren Zhengfei, a former engineer for the Chinese People's Liberation Army (PLA).[13] The company recently made headlines when Huawei CFO (and daughter of Huawei's founder), Meng Wanzhou, was arrested in Vancouver to be extradited to the United States after she was accused of helping Huawei violate U.S. sanctions against Iran.[14]

It is often publicly alleged that Huawei is a state-owned enterprise, and is therefore under the control of the Chinese government. Officially, the firm is employee owned, however, only employees who are also Chinese nationals are eligible to own shares. All shares not held by founder Ren Zhengfei are held by a trade union committee affiliated with the Shenzhen Huawei Investment Holding Co., which represents employees who own shares. When an employee leaves Huawei, the shares revert back to the company.[15] Allegations of government control also stem from the fact Ren Zhengfei is a former deputy director of the PLA Information Engineering Academy, which has connections to the 3PLA, the Chinese equivalent of the NSA.[16]

Huawei has frequently been accused of economic espionage and intellectual theft. For example, in 2003, Cisco Systems accused Huawei of illegally using stolen source code and plagiarizing Cisco user manuals. When the Chinese company promised to remove the contested code from the devices in question, Cisco Systems dropped their case.[17] In 2010, Motorola Inc. filed a suit against Huawei, accusing its employees of colluding with Motorola employees and plotting together to steal proprietary technology.[18] And in 2017, T-Mobile won a lawsuit against Huawei wherein the judge awarded T-Mobile $4.8 million in damages from corporate espionage and theft of intellectual property.[19]

This January, two of Huawei's corporate entities, Huawei Device Co., Ltd. and Huawei Device Co. USA, were charged with "theft of trade secrets conspiracy, attempted theft of trade secrets, seven counts of wire fraud, and one count of obstruction of justice" as a result of stealing information from T-Mobile.[20] Since 2012, Huawei had allegedly been trying to steal information regarding T-Mobile phone-testing robot "Tappy" in an effort to replicate the robot themselves. It is alleged that during the FBI's investigation, they found emails dating back to July 2013 that revealed Huawei offered their employees bonuses for stealing information from other companies—the more valuable the secret, the bigger the bonus.[21]

In 2008, Huawei tried to acquire 3Com, a defense contractor and producer of anti-hacking software, but the deal fell through after CFIUS began to scrutinize the possibility of future software vulnerabilities.[22] A few years later, in 2010, Sprint purportedly rejected a possible contract with Huawei after a call from the U.S. Commerce Secretary to its CEO.[23] In 2011, it was Huawei that backed away from another deal, when CFIUS raised concerns about the company proposing to purchase assets from American server producer 3Leaf.[24] In 2018, the six top U.S. intelligence chiefs, including the heads of the FBI, CIA and NSA, told the Senate Intelligence Committee they would not recommend private citizens use products from Huawei.[25] The next month, electronics chain Best Buy declared they would no longer sell Huawei products.[26] That same year, the Federal Communications Com-

12. Office of Public Affairs, "Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged With Financial Fraud," U.S. Dept. of Justice, Jan. 28, 2019. https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged-financial.

13. "The Company that Spooked the World," The Economist, Aug. 4, 2012. https://www.economist.com/briefing/2012/08/04/the-company-that-spooked-the-world.

14. Daisuke Wakabayashi and Alan Rappeport, " Huawei C.F.O. Is Arrested in Canada for Extradition to the U.S.," The New York Times, Dec. 5, 2018. https://www.nytimes.com/2018/12/05/business/huawei-cfo-arrest-canada-extradition.html.

15. Claude Barfield, "Telecoms and the Huawei Conundrum: Chinese Foreign Direct Investment in the United States," *AEI Economic Studies*, November 2011, p. 5. https://www.aei.org/wp-content/uploads/2011/11/-telecoms-and-the-huawei-conundrum-chinese-foreign-direct-investment-in-the-united-states_103528582558.pdf.

16. Tom Gara, "On Questions Of National Security, Is Huawei Innocent Until Proven Guilty?", *The Wall Street Journal*, Oct. 8, 2012. https://blogs.wsj.com/corporate-intelligence/2012/10/08/on-questions-of-national-security-is-huawei-innocent-until-proven-guilty.

17. Scott Thurm, "Huawei Admits Copying Code From Cisco in Router Software," *The Wall Street Journal*, March 24, 2013. https://www.wsj.com/articles/SB10485560675556000.

18. David Barboza, "Motorola Solutions and Huawei Settle Claims Over Intellectual Property," *The New York Times*, April 13, 2011. https://www.nytimes.com/2011/04/14/technology/14huawei.html.

19. Rachel Lerman, "Jury awards T-Mobile $4.8M in trade-secrets case against Huawei," *The Seattle Times*, March 18, 2017. https://www.seattletimes.com/business/technology/july-awards-t-mobile-48m-in-trade-secrets-case-against-huawei.

20. U.S. Dept. of Justice, "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice," Press Release, Jan. 1, 2019. https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade.

21. Ibid.

22. Steven Weisman, "Sale of 3Com to Huawei is derailed by U.S. security concerns," *The New York Times*, Feb. 21, 2008. https://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html.

23. "Committee on Foreign Investment in the United States Rejects Huawei Deal; Third Recent Chinese Transaction Scuttled by National Security Review," Davis Polk & Wardwell LLP, Feb. 28, 2011. https://www.davispolk.com/files/files/Publication/02ccdb0e-0f81-424a-b8c4-084b8b2e4a03/Preview/PublicationAttachment/024bb648-4892-4e9b-8223-0954a0699115/022811_huawei.pdf.

24. Sinead Carew and Jessica Wohl, "Huawei backs away from 3Leaf acquisition," *Reuters*, Feb. 19, 2011. https://www.reuters.com/article/us-huawei-3leaf/huawei-backs-away-from-3leaf-acquisition-idUSTRE71I38920110219.

25. Sara Salinas, "Six top US intelligence chiefs caution against buying Huawei phones," *CNBC*, Feb. 13, 2018. https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html.

26. Edward Baig, "Best Buy to stop selling phones from Huawei; Chinese company has been accused of spying," *USA Today*, March 22, 2018. https://www.usatoday.com/story/tech/talkingtech/2018/03/22/best-buy-stop-selling-phones-huawei-chinese-company-has-been-accused-spying/448914002.

mission proposed a rule that would disqualify companies from using specific government funding to buy Huawei and ZTE products.[27] The 2019 National Defense Authorization Act also bans the federal government and its contractors from using Huawei technology unless a waiver is obtained.[28]

The United States is not the only country's government that has voiced concerns about Huawei. In 2006, for example, Canada denied visa applications for two Huawei Chinese employees, citing concerns about espionage.[29] Moreover, at various points, Huawei deals have been blocked in the United States, Australia, New Zealand and Japan (among others) over national security concerns.[30] More recently, the Polish government arrested Weijing Wang, Huawei's sales director in Poland, on suspicions of spying for the Chinese government. After the arrest, Huawei quickly fired Wang for bringing the company into "disrepute."[31]

Countries differ in opinion about how best to mitigate the Huawei threat. While the United States enacted a ban that has completely removed the company from the government supply chain, the United Kingdom has tried a less radical approach. In 2011, they established the Huawei Cyber Security Evaluation Centre (HCSEC), which was charged with monitoring and evaluating the security risk of Huawei telecommunications products. The Centre's degree of success is uncertain, as its 2018 report revealed that it is unsure that the source code they inspect is identical to the source code Huawei actually uses in their products.[32] The report added that, looking forward, "it is less confident that the [British government's National Cyber Security Centre] and HCSEC can provide long term technical assurance of sufficient scope and quality around Huawei in the UK."[33] Like the United Kingdom, Germany has also hedged about the severity of the threat posed by Huawei. For example, the head of Germany's Federal Office for Information Security (BSI), Arne Schoenbohm, insists that his agency lacks sufficient proof of the company's spying, while German regulators have refused to ban Huawei from Germany's 5G internet infrastructure.[34]

ZTE—Often mentioned alongside Huawei, ZTE is another Chinese telecommunications company that has recently been considered a potential problem for supply chain security. Formerly called Zhongxing Telecommunication Equipment Corporation, ZTE was founded in 1985 as Zhongxing Semiconductor Co., Ltd. by Hou Weigui with funding from China's Ministry of Aerospace Industry.[35] A publicly traded company since 1997, 30.34 percent of ZTE shares are held by Zhongxingxin Telecom Co., Ltd., who is partially owned in turn by companies that are subsidiaries of the China Aerospace Science and Technology Corporation (CASC) and the Chinese Aerospace Science and Industry Corporation (CASIC). Both CASC and CASIC are under the direct jurisdiction of the cabinet-level State-owned Assets Supervision and Administration Commission of the State Council (SASAC).[36]

In 2012, the Permanent Select Committee on Intelligence of the U.S. House of Representatives issued the "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," which stated that "ZTE argued at great length that it could not provide internal documentation or many answers to Committee questions given fear that the company would be in violation of China's state-secrets laws and thus subject ZTE officials to criminal prosecution in China."[37] According to the report, the company includes a Chinese Party Committee as part of its structure. Such a refusal to describe its formal interactions with the Chinese government does not imbue confidence in the company's claims to be privately operated.[38]

27. Ryan Duffy, "American companies protest FCC pressure on Huawei," *Cyberscoop*, July 5, 2018. https://www.cyberscoop.com/american-companies-protest-fcc-pressure-huawei.

28. Jacob Kastrenakes, " Trump signs bill banning government use of Huawei and ZTE tech," *The Verge*, Aug. 13, 2018. https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump.

29. "Canada to bar two Huawei workers over spying fears," *The Straits Times*, May 6, 2016. https://www.straitstimes.com/world/canada-to-bar-two-huawei-workers-over-spying-fears.

30. See, e.g., Maggie Lu-YueYang, "Australia blocks China's Huawei from broadband tender," *Reuters*, March 26, 2012. https://www.reuters.com/article/us-australia-huawei-nbn/australia-blocks-chinas-huawei-from-broadband-tender-idUSBRE82P0GA20120326; "Huawei: NZ bars Chinese firm on national security fears," *BBC*, Nov. 28, 2018. https://www.bbc.com/news/business-46368001; "Japan sets policy that will block Huawei and ZTE from public procurement as of April," *The Japan Times*, Dec. 10, 2018. https://www.japantimes.co.jp/news/2018/12/10/business/japan-sets-policy-will-block-huawei-zte-public-procurement-april/#.XG14IuhKg2w.

31. Raymond Zhong, "Huawei Fires Employee Arrested in Poland on Spying Charges," *The New York Times*, Jan. 12, 2019. https://www.nytimes.com/2019/01/12/world/asia/huawei-wang-weijing-poland.html.

32. Michael Shoebridge, "Chinese Cyber Espionage and the National Security Risks Huawei Poses to 5G Networks," The Macdonald-Laurier Institute, November 2018, p. 5. http://macdonaldlaurier.ca/files/pdf/MLICommentary_Nov2018_Shoebridge_Fweb.pdf.

33. "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board: annual report 2018," Huawei Cyber Security Evaluation Centre Oversight Board, July 19, 2018, p. 18. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.

34. See, e.g., AFP, "'No Evidence' of Huawei Spying, Says German IT Watchdog," *SecurityWeek*, Dec. 17, 2018. https://www.securityweek.com/no-evidence-huawei-spying-says-german-it-watchdog; Mike Watson, "Berlin Needs to Heed Washington on Huawei," *RealClearWorld*, March 15, 2019. https://www.realclearworld.com/articles/2019/03/15/berlin_needs_to_heed_washington_on_huawei_112986.html.

35. Kenji Kawase, "ZTE's less-known roots: Chinese tech company falls from grace," *Nikkei Asian Review*, April 27, 2018. https://asia.nikkei.com/Business/Company-in-focus/ZTE-s-less-known-roots-Chinese-tech-company-falls-from-grace.

36. Ibid.

37. Permanent Select Committee on Intelligence, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," U.S. House of Representatives, Oct. 8, 2012, p. 36. https://intelligence.house.gov/sites/democrats.intelligence.house.gov/files/huawei-zte%20investigative%20report%20(final)_0.pdf.

38. Ibid, pp. 37-40.

Equally serious is the revelation of ZTE's repeated violation of international sanctions. In 2017, it pleaded guilty to violating U.S. sanctions against Iran and North Korea. In recompense, the company was slapped with an $892 million fine, promising to punish any responsible leadership and a seven-year ban that would prevent ZTE from buying components from U.S. suppliers if continued sanctions violations were discovered.[39] However, in 2018, the U.S. Dept. of Commerce accused ZTE of breaking its agreement by refusing to seriously discipline its senior management.[40]

The seven-year ban went into effect in April 2018, but soon proved crippling to both ZTE and several U.S. suppliers, such as Qualcomm, from whom ZTE buys many of its chips and processors.[41] As a result, in June (after President Trump met with Chinese President Xi), the Department of Commerce (DOC) proposed a settlement that lifted the import ban in exchange for an additional $1 billion fine, the replacement of its entire senior management and the establishment of a company compliance department with employees selected by the DOC.[42]

The U.S. Senate made an effort to block the settlement with provisions in the National Defense Authorization Act for Fiscal Year 2019. The House version of the bill declined to block the settlement, but did include a ban on the federal government buying technology from either ZTE or Huawei, or contracting with entities that use equipment from ZTE or Huawei, absent a waiver. The House version of the bill was signed by President Trump and in July 2018, the import ban was lifted.[43]

ZTE also made news last year when researchers discovered a backdoor in one ZTE phone model, sold as the ZTE Score M in the United States, which would allow someone to access the phone remotely without the user's knowledge. The handset model in question was not widely used and upon discovery, the company promised to send out a patch to fix the issue.[44]

To help refurbish its tarnished reputation, ZTE hired a former member of Congress to assess its products to assuage American fears of Chinese spying. In December 2018, former Sen. Joe Lieberman registered as a lobbyist and was brought onboard by the company.[45] In an interview with *Politico*, Lieberman said: "I don't expect at any point, certainly in this phase, to be giving ZTE's point of view. I'm really supposed to be listening and asking questions."[46] Lieberman joins two other former lawmakers, former Minnesota Senator Norm Coleman and former Nebraska Representative Jon Christensen, who have also done lobbying work on behalf of the Chinese company.

Lenovo—In addition to Huawei and ZTE, Lenovo Group Limited is a multifaceted provider of information technology goods and services. It manufactures end-user devices such as laptops, tablets, smartphones, monitors and other accessories. It also makes digital infrastructure equipment, such as servers, for use in data centers. The company provides a range of cloud-based services and networking solutions, as well as technical and business consulting.[47] Even though it manufactures such a wide range of electronic equipment and provides various information technology services, Lenovo has not garnered the attention of the administration, Congress or the public as Huawei and ZTE have.

Lenovo was originally founded as Legend in 1984 by Liu Chuanzhi, and has current headquarters in Hong Kong; Beijing; China; and Morrisville, North Carolina.[48] Like ZTE and Huawei, Lenovo is often classified as a hybrid or mixed-ownership company.[49] In the past, the Chinese Academy of Sciences, the government's national "think tank" regarding research related to the natural sciences, retained a controlling share (65 percent) of Legend Holdings, which is a partial owner of Lenovo. However, in recent years, this number has shrunk. According to company websites, 29.102 percent of Lenovo is currently held by Legend Holdings, which is partially owned (36 percent) in turn by the Chinese Academy of Sciences.[50] The majority share of Lenovo (approximately 64 percent) is publicly owned and traded, with the rest owned

39. Karen Freifeld and Sijia Jiang, "China's ZTE pleads guilty, settles U.S. sanctions case for nearly $900 million," *Reuters*, March 7, 2017. https://www.reuters.com/article/us-usa-china-zte-idUSKBN16E1X1.

40. The CEO who oversaw ZTE during the sanctions violations was "demoted" to chairman of the board, while several other complicit executives received bonuses.

41. Paul Mozer, "All About ZTE, the Chinese Sanctions Breaker That Trump Wants to Help," *The New York Times*, May 14, 2018. https://www.nytimes.com/2018/05/14/business/zte-trump-china.html.

42. 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.

43. Ibid. As noted earlier, the purchase ban is now the subject of litigation by Huawei. See: Aaron Pressman, "Why Chinese Telecom Giant Huawei Is Suing the U.S. Government," *Fortune*, March 7, 2019. http://fortune.com/2019/03/07/huawei-sues-us-government.

44. Dennis Fisher, "ZTE Score M Android Phone Found to Have Backdoor Installed," *Threatpost*, May 18, 2012. https://threatpost.com/report-zte-score-m-android-phone-found-have-backdoor-installed-051812/76584.

45. Kevin Breuninger, "Former Sen. Joe Lieberman joins China's ZTE to ease national security concerns amid lawmakers' distrust," *CNBC*, Dec. 14, 2018. https://www.cnbc.com/2018/12/14/joe-lieberman-zte-to-lead-national-security-assessment-of-products.html.

46. Daniel Lippman and Steven Overly, "China's ZTE taps Joe Lieberman for D.C. damage control," *Politico*, Dec. 13, 2018. https://www.politico.com/story/2018/12/13/zte-china-joe-lieberman-1031383.

47. "Data Center," Lenovo, 2019. https://www.lenovo.com/us/en/data-center.

48. "Company History," Lenovo, 2019. https://www.lenovo.com/us/en/lenovo/company-history.

49. "China's Mixed-ownership Enterprise Model: Can the State Let Go?", *Knowledge@Wharton*, Sept. 26, 2018. https://knowledge.wharton.upenn.edu/article/will-chinas-mixed-ownership-enterprise-model-work.

50. See, e.g., "Shareholding Structure," Lenovo, Dec. 31, 2018. https://investor.lenovo.com/en/ir/shareholding.php; "Articles of Association of Legend Holdings Company," Legend Holdings Corporation, December 2018. http://legendholdings-umb.china-cloudsites.cn/media/1114/%E7%AB%A0%E7%A8%8B_e.pdf.

by current CEO Yang Yuanqing and other company directors.[51] Lenovo is incorporated in Hong Kong and its shares are traded on the Hong Kong Stock exchange.[52]

In 2005, it acquired IBM's Personal Computing Division. The acquisition led some to question the national security implications of using Lenovo and certain IBM products. A letter from then-Representatives Henry Hyde (R-Ill. and then-chair of the House International Relations Committee), Duncan Hunter (R-Calif. and then-chair of the House Armed Services Committee) and Don Manzullo (R-Ill. and then-chair of the House Small Business Committee) stated:

> First, this transaction may transfer advanced U.S. technology and corporate assets to the Chinese government. Second, this transaction may transfer licensable or export-controlled technology to the Chinese government. Finally, this transaction may result in certain U.S. government contracts with or involving (personal computers) being fulfilled or participated in by the Chinese government.[53]

Nevertheless, the acquisition was approved by CFIUS.

In 2006, a planned State Department purchase of 16,000 Lenovo computers raised concerns with two U.S.-China Economic and Security Review Commission members, Larry M. Wortzel and Michael R. Wessel. Created in 2000, the U.S.-China Economic and Security Review Commission was created by Congress to "monitor, investigate, and submit to Congress an annual report on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China, and to provide recommendations, where appropriate, to Congress for legislative and administrative action."[54]

In a letter to then-Representative Frank Wolf (R-Va.), Wessel and Wortzel wrote:

> There is no company or individual in China that is immune to the pressures of the Chinese government when it comes to facilitating the interests of the state. The fact that these computers may be assembled outside of China or that the software is produced in the United States does not eliminate the opportunity for covert means to gain access to some of our nation's most important data.[55]

While other computer security experts doubted the risk posed by Lenovo's acquisition of IBM's personal computing division, the alarm from Wolf, Wessel and Wortzel was sufficient to impact the State Department's decision, and 900 IBM computers originally intended to be integrated into classified networks were used only for unclassified networks.[56]

Similarly, after Lenovo's acquisition of IBM's x86 server business in 2014, the U.S. Navy announced they planned to replace IBM servers for the Aegis Combat System, a weapons tracking and guiding system, with non-Lenovo systems.[57] In 2015, an advertising software by a company called Superfish that came pre-downloaded on Lenovo computers was discovered to track the online movements of the people using the computers. Upon discovery, the Dept. of Homeland Security issued a warning to Lenovo PC users to remove the software.[58] In 2016, a leaked internal memo from the U.S. Air Force reflected security concerns and the consideration of a potential ban of Lenovo products. DOD officials later retracted the memo.[59] Despite concerns, many Lenovo products are currently still being used by the U.S. government in unclassified systems. Astronauts aboard the International Space Station (ISS) use Lenovo's IBM ThinkPad computers exclusively.[60]

In 2013, a report from the *Australian Financial Review* alleged the "Five-Eyes" countries (Australia, the UK, Canada, New Zealand and the United States) had all banned Lenovo products from the sensitive networks at their intelligence departments after British intelligence discovered cyber vulnera-

51. "Shareholding Structure." https://investor.lenovo.com/en/ir/shareholding.php.

52. "Corporate Information," Lenovo, 2019. https://investor.lenovo.com/en/about/corpinfo.php.

53. John G. Spooner, "IBM-Lenovo deal up for extended review," *ZDNET*, Jan. 28, 2005. https://www.zdnet.com/article/ibm-lenovo-deal-up-for-extended-review.

54. "About Us," U.S.-China Economic and Security Review Commission, accessed April 5, 2019. https://www.uscc.gov/about.

55. Grant Gross, "Security experts: U.S. government's Lenovo ban misguided," *Network World*, May 26, 2006. https://www.networkworld.com/article/2312248/security-experts--u-s--government-s-lenovo-ban-misguided.html.

56. Steve Lohr, "State Department Yields on PC's From China," *The New York Times*, May 23, 2006. https://www.nytimes.com/2006/05/23/washington/23lenovo.html?_r=0.

57. Eva Dou, "U.S. Navy Looks to Replace IBM Servers for Security After Lenovo Purchase," *The Wall Street Journal*, May 19, 2015. https://www.wsj.com/articles/u-s-navy-looks-to-replace-ibm-servers-for-security-after-lenovo-purchase-1432047582.

58. Nicole Perlroth, "How Superfish's Security-Compromising Adware Came to Inhabit Lenovo's PCs," *The New York Times*, March 1, 2015. https://www.nytimes.com/2015/03/02/technology/how-superfishs-security-compromising-adware-came-to-inhabit-lenovos-pcs.html.

59. Hayley Tsukayama and Dan Lamothe, "How an email sparked a squabble over Chinese-owned Lenovo's role at Pentagon," *The Washington Post*, April 22, 2016. https://www.washingtonpost.com/business/economy/how-an-email-sparked-a-squabble-over-chinese-owned-lenovos-role-at-pentagon/2016/04/22/b1cd43d8-07ca-11e6-a12f-ea5aed7958dc_story.html.

60. Gavin O'Hara, "ThinkPad and Space: A Match Made in the Heavens," Lenovo, March 21, 2012. http://blog.lenovo.com/en/blog/thinkpad-laptop-nasa-youtube-spacelab.

bilities in Lenovo hardware and firmware.[61] Furthermore, in 2016, the *Washington Free Beacon* reported that a classified internal report by the J-2 intelligence directorate, which supports the Chairman of the Joint Chiefs of Staff, the Secretary of Defense, Joint Staff and Unified Commands and administers intelligence for joint warfighting assessments, warned that Lenovo computers had been caught "beaconing" or secretly communicating with remote devices.[62]

Russia

Not all technologically problematic software and hardware are of Chinese origin. In 2016, Russia passed the so-called "Yarovaya's law," a pair of amendments to previously existing counter-terrorism legislation, which enacted new requirements regarding the collection and storage of data and granted additional authority to certain government agencies. As a result, "organizers of information distribution on the Internet" must allow the Russian Federal Security Service (FSB) to access stored data as requested. Additionally, certain types of data are required to be stored for specific lengths of time and they must be physically stored on servers in Russia.[63]

According to the law, companies who do not comply face significant fines and may be viewed as passively abetting dissent, which is sometimes categorized as "terrorism" in Russia. Compliance is overseen by Russia's Federal Service for Supervision of Communications, Information Technology and Mass Media. Although the new law was passed in 2016, most of the provisions did not go into place until July 2018. However, immediate compliance with the data storage requirements seems unlikely since, according to experts: "The Russian government presently does not have the necessary equipment or software to enable the storage of such information, as required by the new law, and it is unlikely that such capacity will be developed even by 2018."[64]

However, difficulty implementing these storage requirements does not alleviate the national security risk posed by Russian suppliers. As one commentator has noted: "The fact of the matter is that any Russian company in this sector can be utilized by Russia's security services to serve as a strategic tool for the Kremlin."[65] Because Russian law grants the FSB authority to require companies to assist its activities related to information security for the sake of protecting Russian national security, those who use Russian products should not assume their data is, in fact, private.[66]

Kaspersky—Kaspersky Lab, a Russian antivirus company, has frequently come under scrutiny for possible ties to the Kremlin. Created in 1997 by Eugene and Natalya Kaspersky, the company quickly gained market share in 1998, when their antivirus software was the only product able to identify and destroy the CIH computer virus (frequently referred to as the Chernobyl virus).[67]

A visitor to Kaspersky Lab's American website will see the company logo follow by three words: "proven," "transparent" and "independent."[68] The company claims it is innocent of charges that their products spy on customers. But, Kaspersky also has not been reticent about its political connections. Natalya Kaspersky has said, for example, that all private data belongs to the State.[69] In 2007, the company ran an ad campaign in Japan with the campaign "A Specialist in Cryptography from KGB." This slogan is a reference to Eugene Kaspersky's pre-Kaspersky Lab government connections, as he received his degree from the Technical Faculty of the KGB Higher School and worked as a software engineer for the Soviet Ministry of Defense.[70]

To be sure, Kaspersky Lab says it only assists the Russian government and others in the pursuit of cyber criminals. Indeed, it mocks any suggestion that it is tied to the Russian government. Speaking of one of the KGB's successors, the FSB, and the Interior Ministry, the company website jokes that the government's idea of a "virus" was "strictly biological when Kaspersky Lab was founded."[71] While it does collaborate with different government agencies, Kaspersky insists it does not share user data and that "all data is handled

61. The original article has since been removed from the *Australian Financial Review*'s website. However, at the time, a variety of other news sources commented on the report. See, e.g., "Backdoors see Lenovo on Five Eyes blacklist," itnews, July 29, 2013. https://www.itnews.com.au/news/backdoors-see-lenovo-on-five-eyes-blacklist-351584.

62. Bill Gertz, "Military Warns Chinese Computer Gear Poses Cyber Spy Threat," *The Washington Free Beacon*, Oct. 24, 2016. https://freebeacon.com/national-security/military-warns-chinese-computer-gear-poses-cyber-spy-threat.

63. Matthew Newton and Julia Summers, "Russian Data Localization Laws: Enriching 'Security' & the Economy," The Henry M. Jackson School of International Studies, University of Washington, Feb. 28, 2018. https://jsis.washington.edu/news/russian-data-localization-enriching-security-economy.

64. "Overview of the Package of Changes into a Number of Laws of the Russian Federation Designed to Provide for Additional Measures to Counteract Terrorism," The International Center for Not-for-Profit Law, July 21, 2018, p. 2. http://www.icnl.org/research/library/files/Russia/Yarovaya.pdf.

65. Boris Zilberman, "Kaspersky and Beyond: Understanding Russia's Approach to Cyber-Enabled Economic Warfare," Foundation for Defense of Democracies, June 24, 2018, p. 11. https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare.

66. James Andrew Lewis, "Reference Note on Russian Communications Surveillance," Center for Strategic and International Studies, April 18, 2014. https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

67. Boris Zilberman, "Kaspersky and Beyond: Understanding Russia's Approach to Cyber-Enabled Economic Warfare," Foundation for Defense of Democracies, June 24, 2018, pp. 7-8. https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare.

68. "Home," Kaspersky Lab, accessed April 5, 2019. http://usa.kaspersky.com.

69. Zilberman, p. 9. https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare.

70. Ibid.

71. "Three common myths about Kaspersky Lab," Kaspersky Lab, July 23, 2018. https://www.kaspersky.com/blog/kaspersky-lab-mythbusters/23138.

with extreme care, used anonymously, and protected against any kind of leakage."[72]

However, according to a report from the Foundation For Defense of Democracies (FDD):

> When a Russian company, such as Kaspersky Lab, claims independence or says that it does not work with Russian security services, it is relying on its customers not understanding the legal system under which the company operates. The fact of the matter is that any Russian company in this sector can be utilized by Russia's security services to serve as a strategic tool for the Kremlin.[73]

Russian law grants the FSB authority to require companies to assist its activities related to information security for the sake of protecting Russian national security.[74] Accusing the company of transferring user data to private servers where the FSB could access it, the U.S. government banned Kaspersky software from all federal government computers in 2017.[75] It is no surprise then that, when Senator Marco Rubio (R-Fla.) asked the heads of six American intelligence agencies (the CIA, NSA, the Office of the Director of National Intelligence [DNI], the Defense Intelligence Agency [DIA], the NSA and FBI) if they would be comfortable using Kaspersky software on their computers, all six said no.[76]

Speech Technology Center—Also known as SpeechPro in the United States, the Speech Technology Center is a Russian company founded in 1990 that specializes in voice recognition technology. Based out of St. Petersburg, Russia, STC is the "leading developer of voice and multimodal biometric systems, as well as solutions for audio and video recording, processing and analysis."[77] It first developed a national voice recognition database in Mexico in 2010. According to STC, the technology can scan 10,000 voices in five seconds, using fragments of speech to identify individuals with 90 percent accuracy.

However, the company's origins can be traced back to the KGB,[78] which developed voice recognition technology in part at Sharashka Marfino, a prison camp for engineers and scientists, where prisoners were put to work identifying the voices of individuals calling various embassies in Moscow. Before STC's founding, future employees worked in an applied acoustics unit officially under the scientific development center of the Ministry of Communications but that was actually run by the KGB.[79]

As with Kaspersky, the FSB's potential claim to access data held by any Russian company has raised a few alarms. One of STC's major shareholders is the state owned Gazprombank, which was sanctioned by the U.S. Treasury Department in 2014.[80] Gazprombank is owned by Yuri Kovalchuk, a close associate of Russian President Vladimir Putin. However, the STC also has wholly owned subsidiaries in the United States, Germany and Mexico.[81]

STC products are used by banks, law enforcement and security and telecom companies in over 75 countries, including the United States.[82] In 2012, Alexey Khitrov, STC's Strategic Development Director, reported that STC works with a number of U.S. agencies at both the state and federal level.[83] More recently, STC has begun to branch out into facial recognition software. And in 2012, the company declared it had developed the "world's first biometric identification platform, at a nationwide level, that combines voice and face identification capabilities" in Ecuador.[84]

STC counts several countries with questionable histories regarding human rights among their customers (Kazakhstan, Belarus, Thailand and Uzbekistan).[85] But, its founders apparently are not troubled by how their technology is used by clients. For example, in their book, *Red Web: The Struggle Between Russia's Digital Dictators and the New Online*

72. Ibid

73. Zilberman, p. 11. https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare.

74. Lewis. https://www.csis.org/analysis/reference-note-russian-communications-surveillance.

75. Matthew Rosenberg and Ron Nixon, "Kaspersky Lab Antivirus Software Is Ordered Off U.S. Government Computers," *The New York Times*, Sept. 13, 2017. https://www.nytimes.com/2017/09/13/us/politics/kaspersky-lab-antivirus-federal-government.html. As noted earlier, Kaspersky challenged that decision in court, but its challenge was rebuffed.

76. "US intelligence chiefs have doubts about cybersecurity firm over its Russian roots," *The Guardian*, May 11, 2017. https://www.theguardian.com/us-news/2017/may/11/kaspersky-labs-cybersecurity-us-senate-intelligence.

77. "About company," Speech Technology Center, accessed April 5, 2019. https://speechpro.com/company.

78. Zilberman, p. 16. https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare.

79. Andrei Soldatov and Irina Borgan, "Five Russian-Made Technologies Used in the West," *Wired*, May 10, 2013. https://www.wired.com/2013/05/russian-surveillance-technologies.

80. Zilberman, p. 16. https://www.fdd.org/analysis/2018/06/24/kaspersky-and-beyond-understanding-russias-approach-to-cyber-enabled-economic-warfare.

81. Peter Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia," *Access Now*, June 2013, p. 10. https://www.accessnow.org/cms/assets/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf.

82. "About company." https://speechpro.com/company.

83. Ryan Gallagher, "Watch Your Tongue: Law Enforcement Speech Recognition System Stores Millions of Voices," Slate, Sept. 20, 2012. https://slate.com/technology/2012/09/speechpro-voicegrid-nation-voice-recognition-software-for-use-by-law-enforcement.html.

84. Soldatov and Borgan. https://www.wired.com/2013/05/russian-surveillance-technologies.

85. Gallagher. https://slate.com/technology/2012/09/speechpro-voicegrid-nation-voice-recognition-software-for-use-by-law-enforcement.html.

Revolutionaries, Russian journalists Andrei Soldatov and Irina Borogan detail STC founder Koval's attitude toward government surveillance, as quoted from an interview:

> We just come up with the hardware. It's just technology that is developed with law enforcement in mind. Sure, you can use it against the good guys just as easily as you can use it against the bad guys. One way or another, these governments will be able to use surveillance technology, whether we supply it or not [...] If governments listen in on people's conversations, it's not the microphone's fault![86]

"Friendly" Suppliers—Check Point

Finally, any summary of the current state of play would be remiss if it did not also recognize that the source of risk is broader than two adversarial nations. While the threat of an intrusion is likely less from American allies, it is by no means non-existent. A partial case-in-point (one of the few publicly known exemplars) is the Israeli company, Check Point Software Technologies, Ltd.

According to its website, Check Point is a "leading provider of cyber security solutions to corporate enterprises and governments globally."[87] Created in 1993, the company sells a variety of software and hardware products aimed at addressing a variety of IT security threats, including network and data security.

In 2005, Check Point offered to acquire SourceFire Inc., an American security software company that specialized in intrusion prevention software, for approximately $225 million. However, these plans were scuttled after Check Point withdrew from the deal midway through a CFIUS review of the acquisition.[88] Although CFIUS investigations are classified, it had become apparent that the deal would not be approved. SourceFire was a U.S. government contractor and several federal government agencies, including the FBI, DOD and NSA, objected to the source code in their anti-intrusion software being owned by a foreign company.[89]

There were also alleged concerns about the close ties between Check Point executives and the Israeli Defense Force (IDF). Gil Shwed, one of the company's founders, served in Unit 8200, the IDF's signals intelligence unit.[90] Not surprisingly given Israel's mandatory military service, several former Unit 8200 members have gone on to start IT software and/or security companies.

However, in 2007, a year after Check Point withdrew its offer to acquire SourceFire, the Israeli company was awarded a DOD contract as part of the DoD Enterprise Software Initiative (ESI) and GSA SmartBUY Data At Rest (DAR) Blanket Purchase Agreement (BPA).[91] Because of this later willingness to accept Check Point as a DOD contractor, some critics have suggested that the original CFIUS disapproval of the Check Point/SourceFire deal was politically motivated, rather than fact-based.[92]

ONGOING RESPONSES

Although there is still work to be done, Congress has not ignored the risks posed by supply chain vulnerabilities. Last December, for example, President Trump signed into law the SECURE Technology Act. A combination of three previous bipartisan initiatives, the Act addresses a variety of security concerns relating to the cyber realm, including supply chain risks. The new law establishes a Federal Acquisition Security Council, charged to:

> (1) Identify and recommend development of supply chain risk management standards, guidelines, and practices for assessing and developing mitigation strategies to address supply chain risks; and (2) develop a strategic plan for addressing supply chain risks posed by the acquisition of certain technology and equipment.[93]

The new council is required to create criteria to help distinguish the device types that pose supply chain risks. It will include members from Department of Homeland Security, the Department of Defense, the General Services Administration, Office of the Director of National Intelligence, Federal Bureau of Investigation, Office of Management and Budget, and the National Institute of Standards and Technology.

The new law increases agency responsibilities with respect to assessing their own supply chain risks and sets forth

86. Andrei Soldatov and Irina Borgan, "Building the Kremlin's Big Brother," *Foreign Policy*, Sept. 16, 2015. https://foreignpolicy.com/2015/09/16/we-just-come-up-with-the-hardware-russia-red-web-surveillance-technology.

87. "Facts at a Glance," Check Point Technologies LTD, accessed April 5,2019. https://www.checkpoint.com/about-us/facts-a-glance.

88. Robert Lemos, "Check Point calls off Sourcefire buy," *SecurityFocus*, March 24, 2006. https://www.securityfocus.com/news/11382.

89. Ibid.

90. Idan Tendler, "From The Israeli Army Unit 8200 To Silicon Valley," *TechCrunch*, 2015. https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley.

91. "CheckPoint awarded DOD IT security contract," *Homeland Security News Wire*, July 25, 2007. http://www.homelandsecuritynewswire.com/checkpoint-awarded-dod-it-security-contract.

92. Paul F. Roberts, "Collapse of Check Point/Sourcefire deal raises questions," *Info World*, April 3, 2006. https://www.infoworld.com/article/2655229/collapse-of-check-point-sourcefire-deal-raises-questions.html.

93. H.R. 7327, Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the SECURE Technology Act, 115th Cong.

standards for executive agencies. According to Representative Will Hurd (R-Texas):

> Cyber security is national security. Not a day goes by that our critical infrastructure isn't targeted by bad actors from every corner of the Globe. The SECURE Technology Act ensures that our federal agencies can better mitigate the risks to our networks and supply chains.[94]

In addition, there are a variety of currently pending proposals aimed at addressing supply chain issues. The bipartisan-supported S. 29 and its House counterpart H.R. 618, would create an Office of Critical Technologies and Security. The office's purpose would be to:

> [C]oordinate a whole-of-government response to protect critical emerging, foundational, and dual-use technologies and to effectively enlist the support of regulators, the private sector, and other scientific and technical hubs, including academia, to support and assist with such response; and to develop a long-term strategy to achieve and maintain United States technological supremacy with respect to critical emerging, foundational, and dual-use technologies and ensure supply chain integrity and security for such technologies.[95]

S. 29's sponsors, Senator Mark Warner (D-Va.) and Senator Marco Rubio (R-Fla.), both identified concerns regarding Chinese technology as the motivation for their bill. For example, Sen. Rubio explained:

> China continues to conduct a coordinated assault on U.S. intellectual property, U.S. businesses, and our government networks and information with the full backing of the Chinese Communist Party. The United States needs a more coordinated approach to directly counter this critical threat and ensure we better protect U.S. technology. We must continue to do everything possible to prevent foreign theft of our technology, and interference in our networks and critical infrastructure.[96]

Before last year's NDAA effectively banned government use of Huawei and ZTE products, several members of Congress pushed for even harsher sanctions against Chinese companies. For example, the Defending U.S. Government Communications Act (S. 2391/ H.R. 4747) aimed to prohibit federal agencies from "procuring or obtaining, renewing or extending a contract to obtain or procure, or entering into a contract with an entity that uses any equipment, system, or service with telecommunications equipment or services as a substantial or essential component of any system" not just of Huawei and ZTE, but any entity reasonably believed to be owned or controlled by China.[97] The Fiscal Year 2019 NDAA was somewhat more restrained, calling out specific companies. For example, in addition to Huawei and ZTE, the NDAA banned several Chinese video surveillance manufacturers: Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company.[98]

Finally, the proposed Intelligence Authorization Act (introduced in January 2019) acknowledges a key issue when it comes to determining supply chain vulnerabilities: the sharing of sensitive information or lack thereof. Section 306 authorizes the Director of National Intelligence to create a "Supply Chain and Counterintelligence Risk Management Task Force," which would "standardize information sharing between the intelligence community and the acquisition community of the United States Government with respect to the supply chain and counterintelligence risks."[99] Put simply, information sharing is crucial to developing a secure supply chain and if one intelligence agency withholds information about a particular company, less aware agencies in the government may be put at risk.

FUTURE POLICY CONSIDERATIONS

Thus far, this paper has examined several substantive and procedural challenges that make it harder for the United States to fully identify, understand and mitigate supply chain risks in a manner that better protects its national interests. We therefore summarize the key challenges below and provide a few recommendations for improvement.

In the past, the United States has not had a clear set of publicly stated goals with respect to supply chain security, nor has it had a description of how it plans to achieve those goals or how it will assess the outcomes of the mechanisms that it has put in place to do so. Instead, in practice, the approach appears to have been ad hoc, reactive, episodic and uneven, as it has tended to focus on a limited set of risks from only a few companies in a few countries. Publicly available information cited above suggests that the U.S. government's thinking

94. Office of Will Hurd, "Hurd National Security Bill Passes House," Press Release, Dec. 19, 2018. https://hurd.house.gov/media-center/press-releases/hurd-national-security-bill-passes-house.

95. S.29, A bill to establish the Office of Critical Technologies and Security, and for other purposes, 116th Cong.

96. "Warner, Rubio Debut Bill to Boost Supply Chain Security," *MeriTalk*, Jan. 4, 2019. https://www.meritalk.com/articles/warner-rubio-debut-bill-to-boost-supply-chain-security.

97. S.2391, Defending U.S. Government Communications Act, 115th Cong.

98. H.R.5515, John S. McCain National Defense Authorization Act for Fiscal Year 2019, 115th Cong.

99. S.245, Damon Paul Nelson and Matthew Young Pollard Intelligence Authorization Act for Fiscal Years 2018 and 2019, 116th Cong.

about supply chain risk and what to do about it is not as systematic, consistent or focused on the long term as it should be. One result of this state of affairs is that federal departments and agencies cannot know what to protect and why they must do so, nor can they develop clear parameters for prioritizing their protective efforts with limited resources.

The passage of the SECURE Technology Act, and the creation of a new Federal Acquisition Security Council in particular, are an opportunity to change this slipshod approach. But the members of the new council (which has yet to meet for the first time) will have their work cut out for them. Currently, the United States lacks a publicly available and clearly articulated, comprehensive, dynamic, prioritized and holistic assessment of: (1) what public and private sector **assets** it should protect from supply chain risk; (2) the supply chain **threat actors** who pose the greatest risk; (3) the **malicious tactics, techniques and procedures** that such threat actors use or are likely to use to accomplish their objectives; (4) the **vulnerabilities** that exist to U.S. information systems and devices; (5) the most effective and efficient **defensive measures and mitigation strategies** for thwarting adversaries and **recovering** from failed mitigation efforts; and (6) the **metrics and measures** that public and private sector entities should use to accurately assess the supply chain threat and the effectiveness of risk mitigation and recovery efforts put in place to address those threats.

Moreover, the United States does not seem to have a clear organizational structure or the laws, policies, and enforcement and oversight mechanisms to identify and address supply chain risk in the public or private sectors and to hold a range of actors accountable. As reflected in the membership of the Federal Acquisition Security Council, which includes members from a variety of federal agencies, no single federal department or agency is clearly responsible for addressing the risk that the federal government faces, and no national body today effectively addresses the supply chain risks faced by state and local governments and the private sector, including individual consumers. Instead, numerous federal actors— including the Commerce Department, the State Department, the Department of Homeland Security and the FBI—each play partial roles in addressing supply chain risk. This fragmentation of responsibility, reflective of the fragmented nature of risk faced by each agency, makes cross-department communication and cooperation all the more imperative. Currently, the national response by the United States to supply chain risk does not appear to be flexible, nuanced or adaptable. However, if implemented with strong support from the Executive, the SECURE Technology Act will close some of these gaps.

To be effective, the new federal strategy will need to allow for the delivery of reports not just to Congress but to private corporations, nonprofits and the general public. Further, if the U.S. approach to supply chain risk is not transparent, American citizens will be put at risk. Right now, there is no system in place to consistently and reliably disclose the known threats and vulnerabilities posed by foreign manufacturers and service providers to the general public. Instead, many of the U.S. government's concerns are cloaked behind a veil of classification and secrecy. Although the government must protect sensitive sources and methods, it should reevaluate whether it can increase the disclosure of information about supply chain threats and vulnerabilities to the general public.

Similarly, the U.S. federal government lacks a well-ordered and comprehensive set of effective relationships with key external stakeholders. For a variety of reasons, federal agencies do not have the depth or breadth of relationships with sub-federal governmental actors, key private sector entities (such as manufacturers and service providers), and civil society and consumer groups necessary to address fully supply chain risk.

CONCLUSION

Developing a much more complete and coordinated national response to supply chain risk in the United States will take years and likely will involve numerous beneficial actions by a wide range of parties. It is beyond the scope of this paper to provide a complete roadmap for the country to address supply chain risk over the next 10-20 years. However, there are a variety of steps the government can take beyond the establishment of a Federal Acquisition Security Council:

- 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.
- 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 (as the Check Point example suggests) and also from supply chain providers whose connections to a foreign government are more indirect (as in the case of Lenovo). 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.

These modest steps would not solve the problem of supply chain assurance, nor would they completely mitigate any risk from American engagement in the global information technology supply chain. Taken together, however, they would be an effective first step toward a more comprehensive strategy.

ABOUT THE AUTHORS

Paul Rosenzweig is the founder of Red Branch Consulting PLLC, a homeland security consulting company, and a senior fellow at the R Street Institute. He is also a senior advisor to The Chertoff Group. Mr. Rosenzweig formerly served as Deputy Assistant Secretary for Policy in the Department of Homeland Security. He is also a professorial lecturer in Law at George Washington University and a board member of the Journal of National Security Law and Policy.

Kathryn Waldron is a research associate at the R Street Institute and a graduate research fellow at George Mason University.