SECURITY VULNERABILITIES WITHIN OUR COMMUNICATION NETWORKS

FIND IT | FIX IT
FUND IT

REPORT OF THE STAKEHOLDER WORKSHOP
HELD JUNE 27, 2019 AT THE
FEDERAL COMMUNICATIONS COMMISSION

NOVEMBER 21, 2019

Contents

Introduction

U.S. wireless carriers are actively rolling out initial 5G networks around the country. These networks come with the promise of higher speeds, lower latency and the potential to revolutionize both wireless broadband communications and the myriad applications they make possible. This emerging technology will impact all aspects of American life, from health care to financial services to education to public safety. Simply put, the economic and national security interests of the United States will depend heavily on the functionality and integrity of these 5G networks.

At the same time, nations are competing to establish international dominance in setting 5G standards and building country-wide 5G networks. As part of that race to 5G leadership, China is working aggressively to achieve dominance in 5G standard setting and network deployment. It appears that Chinese companies are not pushing this agenda as market-based competitors. Instead, China is using Chinese manufacturers like Huawei and ZTE as instruments in its efforts to achieve 5G dominance. China's actions certainly raise questions about the potential for that country to use future 5G networks constructed by Chinese manufacturers for espionage or cyber-attacks – questions that we must resolve to strengthen our security. But we must also be concerned about today, and the threat posed to current 3G and 4G networks that already have Chinese equipment in them.

On June 27, 2019, I convened a workshop at the FCC to consider security threats that stem from the presence of certain Chinese communications equipment in U.S. networks and from the related services these companies provide. This workshop gathered the views of many stakeholders, particularly in the wireless communications ecosystem, including carriers, trade associations, manufacturers, and academics. Workshop participants shared their perspectives on network security issues and evaluated my proposal that we need to *find* untrustworthy and insecure communications equipment currently located in U.S. communications networks, *fix* the problems posed by this equipment, and help *fund* the process. Find it. Fix it. Fund it.

The workshop began by examining the threats that China and Chinese-manufactured communications equipment pose. It continued with three panels mirroring the Find it, Fix it, Fund it objective. The first panel explored the types of insecure and untrustworthy equipment currently located in U.S communications networks, where it's found, and the scope of the risk it poses. The second panel evaluated the merits of various solutions to fix this problem and featured an active debate on a rip-and-replace strategy versus a monitoring solution. The final panel discussed options for funding a replacement of insecure equipment, highlighting the fact that insecure networks are a national problem in need of a national solution. Many of the carriers who purchased untrustworthy Chinese equipment are small and operate in rural areas, did not break any laws or rules, and frequently lack the financial means to cover the costs of replacement.

A major takeaway from the workshop is that our networks must only contain equipment from trusted sources. When evaluating the security of a piece of communications networking equipment we should not ask "do I trust this piece of equipment" but instead, "do I trust the manufacturer?" Because networking equipment today relies so heavily on software from its manufacturer, no equipment from an untrustworthy manufacturer should be used. Even if the equipment appears secure at first, if a manufacturer must comply with the Chinese national security law by providing "front door" access to the Chinese government via upgrades and patches, then no amount of mitigation will fully address the problem. Other takeaways from the workshop included:

Nature of the Threat

- The impact of 3G and 4G wireless network threats increases closer to the core which manages all data sessions.
- Perimeter security doesn't work when equipment inside a network gets patched and updated by untrustworthy sources outside the network.
- Distributed processing in 5G networks makes the RAN more vulnerable in the event of an attack.
- Variations in Huawei software make it difficult or impossible to know exactly what software is deployed in a given build.
- Huawei software has "front doors" accessible not only by Huawei but by bad actors familiar with exploiting inconsistencies and flaws in Huawei code.
- Huawei systems are typically managed remotely with frequent updates delivered from China. Control over updates and their delivery essentially amounts to control over an entire network.

Find It

- There are two dimensions to finding insecure or untrusted equipment: 1) determining where Huawei, ZTE, or other untrustworthy equipment is located, and 2) determining which exact equipment constitutes a threat (*e.g.* determining whether all or only some core equipment poses a threat).
- Estimates vary, but Huawei equipment only accounts for a small percentage of equipment in U.S. networks – likely in the low single digits.
- While other carriers or their affiliates may have Huawei or ZTE equipment in their networks, it appears to be most prevalent in rural wireless networks. These carriers bought this equipment, often a decade or more ago, because it was far less expensive than other options and because Chinese companies were willing to work with them to create customized networks. These purchases did not violate any rules or laws.

- Options for finding untrusted Chinese-manufactured communications equipment in U.S. networks include: 1) providing financial incentives for carriers to self-identify; and 2) using FCC authority to require carriers to report locations of threatening equipment to the FCC.

Fix It

- Factors to balance in any "fix" include the speed and feasibility of implementation, increased security, cost, and effect on customers. Approaches to "fixing" threats in the network are "rip-and-replace," or monitoring existing equipment.
- In evaluating threats in the network, the most important question is – "can we trust the equipment manufacturer" not "can we trust a specific piece of equipment."
- Monitoring may be an interim step, but it does not meet the long-term security needs of networks in the US, particularly for core elements. And, particularly in densified networks, there may be too much equipment for monitoring to be practical.
- There are valid concerns about network-wide rip-and-replace operations causing disruption. Nokia and Ericsson explained they have facilitated major network swaps without consumer disruption.
- Availability of replacement equipment will be a challenge, especially without an established U.S.-based hardware supplier and with European 5G equipment suppliers typically not doing business on a scale small enough to work for small rural wireless carriers.
- The European manufacturers currently seem willing to create products and financing options geared toward smaller carriers that need to replace Chinese equipment.
- A "rip-and-replace" solution could allow rural carriers currently on a 3G networks to upgrade to a more secure 4G network that could be made 5G compatible via software updates. U.S.-based software companies may be able to participate in this sort of network replacement.

Fund It

- Congress and appropriated funding are going to need to play a funding role.
- Estimated rip-and-replace costs vary from hundreds of millions of dollars to over a billion.
- Estimates of the per-cell site cost range from $70,000 to $130,000.
- Replacement time frame affects costs. Doubling a one- to two-year timeline may cut costs in half.
- Funding could be tied to requirements to maintain good cyber-security practices.

Below, this report further sets out the context in which this problem arises, describes the nature of the threat posed by China and Chinese-manufactured communications equipment, and provides a summary and analysis of the discussion that took place in each of the three panels of the FCC workshop. Moving forward, I expect that further discussion of the issues addressed and takeaways developed at the workshop will shape the debate surrounding the U.S. approach to addressing threats posed by untrusted communications equipment currently located in U.S. communications networks.

The Nature of the Threat

Outdated Reliance on Trust in Communications Networks

In the past, before there were ubiquitous IP networks and competitive communications providers, communications network security was based primarily on trust amongst a small group of “trusted entity” carriers, each trusting the others to adhere to certain security standards. This trust-based network security model worked when there were only a few carriers on the network. However, as communications networks and technology have evolved and new parties have entered the network, this trust-based model has become more nostalgic than practical.[1] Bad actors now have ready access to network credentials that were once limited to trusted entities, a situation that can lead to harm to the network and the use of the network for harmful purposes.

Risks Posed by Untrustworthy Equipment

Workshop participants suggested three general risks posed by untrustworthy communications networks:

- First, these networks may allow bad actors to improperly access data of American citizens. Workshop participants urged policy makers to pay particularly close attention to the consequences of untrustworthy network equipment allowing for improper data access. Participants highlighted the sheer amount of sensitive communications transmitted through our networks, explaining that unfettered access to this information by a potentially hostile actor presents an enormous threat to American security.

- Second, bad actors could use untrustworthy communications equipment to degrade service, including intentionally slowing down service or even disrupting communications systems. This would be particularly catastrophic during a national emergency.

- Finally, equipment can be used as a launch point for cyber-attacks that could compromise or stop network functionality in locations of a bad actor’s choosing. For example, a bad actor could launch attacks from untrustworthy equipment designed to slow or stop communications networks during, or in the aftermath of, a natural disaster.

[1] *See* Jonathan Mayer, Assistant Professor of Computer Science and Public Affairs, Princeton University, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019); *see also* International Telecommunications Union, *International Security in Telecommunications and Information Technology* (2003) at vii, https://www.itu.int/ITU-T/edh/files/security-manual.pdf (describing the risks created by a “multiplicity of new actors” in the communications industry).

Chinese Telecommunications Equipment Manufacturers

When thinking about Huawei and Huawei communications equipment and services as a threat in U.S. communication networks, it is important to consider the context in which Huawei was created and how it has grown into the largest telecommunications equipment maker in the world.[2] As panelist James Lewis, a China expert from the Center for Strategic and International Studies, explained during the workshop, Huawei has grown into that position over the last 20 years in large part due to Chinese government subsidies and preferential treatment in the Chinese market. Notably, Mr. Lewis pointed out that Huawei's chairman has commented that if the Chinese government hadn't blocked foreign suppliers there would not be a Huawei today.[3]

In this context, Huawei can be seen as an instrumentality of the Chinese government to dominate global communications equipment markets and control the global flow of information. China has demonstrated that it will use aggressive and coercive tactics and behavior to ensure that companies like Huawei are allowed into markets around the world.[4] For example, when Australia banned Huawei and ZTE from supplying equipment for its 5G network, China appears to have banned imports of Australian coal into some Chinese ports.[5]

Furthermore, Huawei has been accused of corporate espionage and patent theft on multiple occasions[6] and Huawei's profitability and earnings have been criticized as artificial on

[2] *See* Dan Strumf, et. al, *How Huawei Took Over the World*, Wall St. J. (Dec. 25, 2018), https://www.wsj.com/articles/how-huawei-took-over-the-world-11545735603.

[3] James Lewis, Senior Vice President and Director, Technology Policy Program, Center for Strategic & International Studies, Statement at The Security Threat within our Communications Networks: Find it, Fix it, Fund it, Workshop (June 27, 2019). A recording of the event can viewed online at https://www.fcc.gov/news-events/events/2019/06/security-threat-within-our-communications-networks-find-it-fix-it-fund-it.

[4] *See, e.g.*, Peter Harrell, Elizabeth Rosenberg & Edoardo Saravalle, *China's Use of Coercive Economic Measures*, Center for a New American Security (June 11, 2018), https://www.cnas.org/publications/reports/chinas-use-of-coercive-economic-measures.

[5] Dan Murtaugh & Jason Scott, *Major Chinese Port Bans Australian Coal Imports, Report Says*, Bloomberg (Feb. 20, 2019), https://www.bloomberg.com/news/articles/2019-02-21/glencore-sees-political-issue-in-china-s-australia-coal-delays.

[6] Chuin-Wei Yap, Dan Strumpf, Dustin Volz, Kate O'Keeffe & Aruna Viswanatha, *Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics*,Wall St. J. (May 25, 2019), https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858. *See also* Dep't of Just., Chinese Telecommunications Device Manufacturer and tis U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice (2019), https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade (detailing the Western District of Washington State's 10-count indictment alleging Huawei intentionally conspired and encouraged employees to steal intellectual property from T-Mobile); Dep't of Just., Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud (2019), https://www.justice.gov/usao-edny/pr/chinese-telecommunications-conglomerate-huawei-and-huawei-cfo-wanzhou-meng-charged (explaining the

this basis. These tactics allow Huawei to offer its products and service at artificially low prices around the globe, a practice that threatens the viability of other telecommunications companies and presents a serious economic threat.[7]

Huawei also has a track record of making it difficult for carriers who purchase Huawei to use other types of equipment or change equipment vendors. For example, Huawei equipment is typically not interoperable with other systems, which makes it difficult or impossible for network operators to switch to other manufacturers' equipment or components. This ensures that deployed Huawei equipment remains available for exploitation as a launch point for Chinese cyber-attacks.[8]

Finally, reports of past Chinese espionage have created concerns about the apparent willingness of the Chinese government to use Huawei equipment for espionage purposes.[9] For example, in 2017, Chinese-government supplied Huawei servers at the African Union Headquarters in Ethiopia were found to be transferring sensitive information to servers in Shanghai every night, from midnight to 2 a.m., for five years.[10] This discovery led to accusations of espionage.[11] Reported incidents such as these raise concerns that the Chinese government will engage in similar conduct in the future.

Huawei Equipment's Technical Deficiencies

In addition to potentially being subject to direct exploitation by the Chinese government, Huawei's equipment contains software security vulnerabilities due to coding and development inconsistencies.[12] Essentially, software in Huawei communications equipment can vary from one installation to another as installers customize the code to make it work for each installation. As a result, security updates and patches may not work on all equipment because the "base" code that the patch or update installs over can differ between different pieces of equipment. Accordingly, it

Eastern District of New York's 13-count financial fraud indictment and speaking more broadly about the company's use of deceit to grow its business).

[7] *Id.*

[8] David Shepardson, *AT&T CEO says China's Huawei hinders carriers shifting suppliers for 5G*, Reuters (Mar. 20, 2019), https://www.reuters.com/article/us-att-ceo-huawei-tech/att-ceo-says-chinas-huawei-hinders-carriers-from-shifting-suppliers-for-5g-idUSKCN1R12TX.

[9] Laurens Cerulus, *West accuses Beijing of 'extensive' cyber espionage*, Politico (Dec. 20, 2018), https://www.politico.eu/article/china-cyber-espionage-uk-us-accuses-beijing/.

[10] John Aglionby, Emily Feng, & Yuan Yang, *African Union accuses China of hacking headquarters*, Financial Times (Jan. 29, 2018), https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5.

[11] *Id.*

[12] Lily Hay Newman, *Huawei's Problem Isn't Chinese Backdoors. It's Buggy Software*, Wired (Mar. 28, 2019), https://www.wired.com/story/huawei-threat-isnt-backdoors-its-bugs/.

may be difficult or impossible for Huawei to deploy patches to fix discovered vulnerabilities in its code.

Although Huawei is aware of these vulnerabilities, it has been unwilling to fix them.[13] Earlier this year, the British government recognized long-standing "serious and systematic" security faults, asserting that Huawei had made "no material progress" in remediating the vulnerabilities and calling into question Huawei's cybersecurity practices and engineering competence, as well as its willingness to fix problems.[14] British oversight agencies doubt that they will be able to manage and mitigate the risk presented by Huawei in the long term.[15]

Workshop panelists describing the threat posed by untrustworthy Chinese-manufactured communications in U.S. networks made a compelling case of a serious threat that must be addressed immediately. The Workshop next considered issues related to finding this equipment.

Find It

The first step in removing untrusted equipment from our networks is finding it. While this seems like an obvious statement, the fact of the matter is that it will not be an easy task to identify all untrustworthy Huawei and ZTE equipment deployed in U.S. networks. Workshop participants asserted that Huawei and ZTE equipment is only present in less than 1percent of U.S. cell sites,[16] a total of approximately 40 carrier customers,[17] most of which are in rural areas.[18] Other estimates vary, but Huawei equipment only accounts for a small percentage of equipment in U.S. networks – likely in the low single digits.[19] Cooperation among federal agencies may help develop a more complete and current picture. For example, the U.S. Department of Commerce has in the past worked with federal agencies and the communications

[13] *Id.*

[14] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, *Annual Report 2018, A report to the National Security Adviser of the United Kingdom* (Mar. 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

[15] *Id.*

[16] Dileep Srihari, Senior Policy Counsel and Acting Head of Government Affairs, Telecommunications Industry Association, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[17] *Id.;* Carri Bennet, General Counsel, The Rural Wireless Association, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[18] *Id.*

[19] *See* Katy Stetch Ferek, Trump Administration Extends Rural Telecoms' Ability to Use Huawei Gear, Wall St. J. (Nov. 18, 2019), https://www.wsj.com/articles/trump-administration-extends-rural-telecoms-ability-to-use-huawei-gear-11574098705 ("Huawei hardware makes up less than 1% of equipment used by U.S. telecom networks. . . .").

industry to conduct a comprehensive assessment of the U.S. Information Network Infrastructure.[20] A similar effort today may speed the process of identifying Huawei and ZTE equipment. Even if this equipment represents only a small percentage of our national networks, due to the interconnected nature of networks, insecurities in any location represent threats to the entire network.

One small rural operator using ZTE equipment is Pine Belt Wireless, a small communications company serving parts of West Central Alabama.[21] Pine Belt provides mobile wireless service in locations that are relatively costly to serve, and the company relies on loans and funding from the Department of Agriculture's Rural Utility Service and the FCC's Universal Service Fund (USF).[22] When Pine Belt evaluated equipment for its 4G wireless buildout, ZTE equipment cost 1/3 of the competing offers from other manufacturers. Pine Belt's representative at the workshop said that ZTE's pricing allowed Pine Belt to keep its costs low enough to meet USF buildout requirements.[23] Pine Belt was typical of many other small rural carriers, who selected Chinese equipment because of pressure to keep costs low and because manufacturers like ZTE and Huawei worked with these carriers to customize their networks.[24]

While some carriers who have purchased and installed this equipment have publicly self-identified, others may be reluctant to do so for fear that they will be compelled to remove the equipment but will not receive help in acquiring and installing replacement equipment.

Methods of Identifying Untrustworthy Equipment

During the workshop, several participants suggested utilizing funding as an incentive to encourage carriers who have untrustworthy Chinese telecommunications equipment in their networks to identify themselves. With the proper incentives, this approach could lead to rapid identification of threatening network equipment. However, this approach also presents a "chicken and the egg" problem because it's difficult or impossible to know how much funding will be needed until we know how many carriers have untrustworthy equipment.

And, removing equipment without guaranteed funding means that many small carriers would be unable to continue their operations, and their customers, with no other choices in the market, would have to forfeit wireless access. This scenario is unacceptable. Providing adequate

[20] U.S. Dep't of Commerce, *2012 BIS Study, National Security Assessment: U.S. Information Network Infrastructure* (2012), https://www.bis.doc.gov/index.php/documents/other-areas/643-defense-industrial-base-assessment-telecommunications-industry-infrastructure/file.

[21] John Nettles, President, Pine Belt Wireless, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[22] *Id.*

[23] *Id.*

[24] Cecilia Kang, *Huawei Ban Threatens Wireless Service in Rural Areas* (May 25, 2019), https://www.nytimes.com/2019/05/25/technology/huawei-rural-wireless-service.html.

funding at the outset allows carriers to work with the FCC without fear of losing their ability to provide service.

Another approach to identifying carriers with potentially untrustworthy equipment includes using the FCC's power to inquire into carriers' business practices. The Communications Act gives the FCC the authority to obtain information from carriers necessary to perform its duties.[25] And it is the FCC's duty, under provisions of the Communications Act that direct the FCC to ensure that communications networks are ready to serve the national defense and promote safety of life and property, to know about threats to the security of U.S. communications networks. Additionally, the May 2019 Executive Order directs agencies to take all appropriate actions within their authority to implement the Order. This direction may provide an additional source of authority for the FCC to inquire about the location of untrustworthy communications equipment.[26]

Which Equipment Components Pose Risks

At a high level, the major components of a wireless network are the radio access network, or RAN, at the edge of the network, which consists of radios and antenna that communicate with individual handsets; the backhaul, which carries information between the edge components and the center of the network; and the core, which is computing equipment at the center of the network that processes and routes traffic and makes other decision related to completing calls. Huawei produces equipment for every part of the network.

Workshop participants described the nature of threats within 4G and older networks as increasing as you move from the individual handsets to the RAN and on to the core. The reason is that that handsets and RAN components have little to no "decision making" capacity and are therefore very limited in the amount of damage they could do if corrupted, insecure or untrustworthy. Core components, on the other hand, manage all of the data that passes through the network, including roaming arrangements and the selection of information pathways for delivery to consumers and therefore, present the greatest risks if compromised.[27]

Fix It

The next workshop panel focused on how to "fix" the problems posed by untrustworthy equipment. The best solution to fix the equipment problem depends on what equipment is

[25] *See* 47 U.S.C. § 218.

[26] Executive Order 13873, 84 Fed. Reg. 22689, Executive Order on Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain ("Executive Order 13873").

[27] Jonathan Mayer, Assistant Professor of Computer Science and Public Affairs, Princeton University, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

deemed threatening or untrustworthy, how much of that equipment is in our networks, and where it is located. At the time of the workshop, two main types of solutions were discussed: leaving the untrustworthy equipment in place but monitoring it closely to mitigate threats, or implementing a "rip-and-replace" solution that would completely remove such equipment. Factors to consider when evaluating either option include the speed of implementation, the increased security provided by the solution, the ability for carriers to implement the solution, the impact on customers, and the cost of implementation.

Mitigation

A mitigation solution would be the least costly and quickest to deploy but may have questionable effectiveness.[28] Because vulnerabilities created by this equipment already exist in the network, the speed of a solution's implementation is directly relevant to how effective it is overall. However, mitigation presents certain drawbacks. Concerns about untrustworthy equipment extend beyond faulty software to the reliability of the manufacturer, as explained previously. As several workshop panelists pointed out, because the network security concerns at issue involve a sophisticated foreign adversary, threats embedded in the software are uniquely difficult to detect.[29] Additionally, with a mitigation solution, each software patch or upgrade must undergo examination for security vulnerabilities. The number of upgrades and patches to monitor, multiplied by the number of pieces of equipment at issue, particularly if the networks in questions are densified 5G networks, could easily result in mitigation solutions not being technically feasible because there is simply too much equipment and information to monitor. For example, the British Huawei Cyber Security Evaluation Centre, which has recommended mitigation strategies, doubts their overall, long-term effectiveness because Huawei's software is "defective" and "there remains no end-to-end integrity of the products as delivered by Huawei and limited confidence on Huawei's ability to understand the content of any given build and its ability to perform true root cause analysis of identified issues."[30] Also, while a monitoring and mitigation approach may "see" and contain the damage from an attack, it cannot prevent the attack in the first place.

Ultimately, while a mitigation strategy has some appeal until a rip-and-replace solution can be implemented, it is clear that it does not offer the long-term security required by U.S.

[28] Carri Bennet, General Counsel, The Rural Wireless Association, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[29] James Lewis, Senior Vice President and Director, Technology Policy Program, Center for Strategic & International Studies, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[30] Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, *Annual Report 2018, A report to the National Security Adviser of the United Kingdom* (Mar. 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

networks, particularly for network core elements. There is simply too much information to monitor and too much at stake.

Further, in evaluating threats that certain equipment poses to communications networks, it is important to differentiate between a lack of trust in particular devices, which could potentially be mitigated through monitoring, versus a lack of trust in the equipment supplier. A lack of trust in equipment presents discrete risks on its own, but a lack of trust in the equipment supplier creates broader concerns that a supplier will manipulate insecure elements in a network it designed and constructed. While equipment exhibits vulnerabilities by nature, being able to trust a supplier alleviates worries regarding said supplier's purposeful exploitation of the equipment.[31]

Doubts about the trustworthiness of Chinese telecommunications manufacturers continue to grow. These concerns are amplified by the possibility of the Chinese government exercising its domestic legal authority to order a Chinese manufacturer to use network equipment installed in U.S. networks to conduct espionage or to carry out cyber-attacks.[32]

While Huawei has disputed this reading of Chinese law,[33] American national security officials doubt the ability of Chinese companies to challenge the wishes of the Chinese government.[34] These conditions present a major concern that a "back door," *i.e.* an intentional vulnerability, could be inserted into Chinese-manufactured telecommunications equipment,[35] giving the Chinese government access to sensitive information transmitted over our networks. However, it is possible that such a back door might not be needed to collect this sensitive information. Because the company that builds a network controls the delivery and content of any upgrades and patches, it already has a "front door" into its customers' networks.[36] Chinese telecommunications manufacturers could use, or could be ordered by the Chinese government to

[31] Brian Hendricks, Vice President of Policy and Government Relations, Nokia & Bill Chotiner, Director, Radio Access Network Evolution, Ericsson, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[32] Yuan Yang, *Is Huawei compelled by Chinese law to help with espionage?*, Financial Times (Nov. 18, 2019), https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0.

[33] *See* Huawei May 10, 2019 *Ex Parte*, WC Docket No. 18-89, https://ecfsapi.fcc.gov/file/10510052589900/Huawei%20FCC%20Ex%20Parte%20re%20Chinese%20Law%20(Docket%2018-89).pdf (including a 37-page legal brief interpreting the relevant Chinese law.)

[34] Yuan Yang, *Is Huawei compelled by Chinese law to help with espionage?*, Financial Times (Nov. 18, 2019), https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0.

[35] *The Real Costs of Huawei Technology: a Conversation with James Lewis*, Center for International Studies (May 2019), https://www.csis.org/podcasts/chinapower/real-costs-huawei-technology-conversation-james-lewis.

[36] James Lewis, Senior Vice President and Director, Technology Policy Program, Center for Strategic & International Studies, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

use, this “front door” option to gather sensitive information from or disrupt U.S. communications networks.

Rip-and-Replace

Considering the drawbacks of a mitigation solution, a rip-and-replace solution may be necessary, at least for the most vulnerable network equipment such as the network core. As discussed above, a mitigation solution presents various technical deficiencies that may render it insufficient. The pervasive problem of an untrustworthy supplier only serves to amply those deficiencies. When dealing with an untrustworthy supplier, there can be no assurances that the supplier’s knowledge of the network’s layout and its control over patches and updates will not lead to network attacks.

Rip-and-replace serves as a solution when there is simply too much equipment, including patches and updates, to monitor. In the United States, removing and replacing insecure or untrustworthy equipment with technically reliable equipment manufactured by a trusted supplier eliminates security concerns associated with non-trusted manufacturers certainly presents the most secure solution.

Workshop panelists discussed other factors in executing a large-scale rip-and-replace effort to switch out much or all of the untrustworthy equipment present in a carrier’s network. Both Nokia and Ericsson noted during the workshop that they had facilitated major equipment swaps with no consumer disruptions.[37] However, a rip-and-preplace approach will be costly and presents other challenges. For example, it is unknown when capable equipment and labor[38] will be available, especially during the push for 5G deployment. In addition, poor weather conditions and terrain play distinct roles in reaching some of the most remote areas in the United States. All these issues must be dutifully considered regarding how quickly any rip-and-replace solution could be implemented — one rural carrier stated that it usually takes two years to go from ordering equipment to deploying that equipment.[39]

Fund It

The cost of a solution to the insecure and untrustworthy equipment problem depends largely on many of the issues discussed at earlier workshop panels: how much insecure

[37] Brian Hendricks, Vice President of Policy and Government Relations, Nokia & Bill Chotiner, Director, Radio Access Network Evolution, Ericsson, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[38] *See generally The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019)* (Panel 2: Fix It: How to Ensure that Networks are Secure). There may not be enough qualified installation crews available to carry out equipment swaps in rural areas.

[39] John Nettles, President, Pine Belt Wireless, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

equipment is located in U.S. communications networks? Which specific components present threats? What will the approach be to eliminate the threats?

Whatever the cost, the amount of funding available will directly determine the reach and effectiveness of the designated solution. The Commission's Universal Service program provides funding for specific programs as directed by statute but currently lacks the flexibility and funding level to pay for equipment replacements while carrying out its core missions. Therefore, with estimates of the necessary funding in the billions of dollars, workshop participants agreed that appropriated funding must be an important part of the solution. Currently, both the House and Senate are considering bills that would provide funding for replacing insecure communications networks equipment. The Senate bill would provide $700 million and the House bill would provide $1 billion.[40]

Small rural carriers often work on razor-thin margins to provide service to communities that need connection.[41] Workshop panelists Union Telephone and Pine Belt Wireless operate as family-owned businesses and when they bought Chinese equipment many years ago they were focused on keeping their costs low so they could afford to build out networks for people that otherwise wouldn't be connected.[42] When many carriers, like Union Telephone and Pine Belt Wireless, bought this equipment, doing so seemed like a straight-forward business decision at the time. As one workshop panelist pointed out, five years ago it made sense to use Chinese equipment, but the security risks presented by this equipment have changed the equation.[43]

Estimates of Cost

Estimates for a rip-and-replace solution for rural carriers discussed at the workshop varied drastically, from $150 million to over a billion dollars, a variable mostly dependent on how many cell sites contain equipment that would need to be replaced. The lowest estimate did not include installation costs and was based on an estimated 13 carriers with 1,500 cell sites total, with the cost of $100,000 per site.[44] However, one rural carrier alone estimated its costs to be

[40] *See* United States 5G Leadership Act of 2019, S. 1625, 116th Cong. (2019); Secure and Trusted Communications Networks Act of 2019, H.R. 4459, 116th Cong. (2019).

[41] *See generally* The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019) (Panel 3: Fund It: National Problems Require National Solutions).

[42] John Nettles, President, Pine Belt Wireless and Christopher Reno, Director of Accounting, Union Telephone Company, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[43] James Lewis, Senior Vice President and Director, Technology Policy Program, Center for Strategic & International Studies, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[44] Dileep Srihari, Senior Policy Counsel and Acting Head of Government Affairs, Telecommunications Industry Association, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

$85 million for replacing the equipment in its network. This estimate includes increased costs due to the carrier's very rural service areas, federal lands permitting issues, and a short summer-only construction season.[45] Jeff Johnston, Senior Economist at CoBank, a workshop panelist and lender focused on rural telecom companies, estimated a cost of $70,000 per cell site, including labor, but estimated the total number of affected cell sites in the United States to be between 8,000 to 10,000, bringing the estimated cost of a rip-and-replace solution to $800 million to $1 billion.[46] A rural carrier association estimated costs of $800 million to $1 billion to fund the replacement of its problematic equipment for only 12 to 13 carriers in its association.[47]

As illustrated by this wide range of estimated costs, it likely will be impossible to pinpoint, in advance, the exact cost of a rip-and-replace solution until determinations are made about what equipment is insecure, how much of it is deployed in the United States, and if removal of the equipment is necessary in all, or just some, cases. The FCC will need to, and is well positioned to, work with carriers to determine an accurate estimate of the amount of funding needed.

Methods to Reduce Cost

Multiple panelists emphasized how time could serve as a cost-reduction tool.[48] Because networks are in constant need of upgrades, the longer a replacement effort takes, the more insecure and untrustworthy equipment will organically exit the network.[49] For example, workshop panelists estimate that a four- to five-year rip-and-replace timeline would cost about half as much as a rip-and-replace effort carried out over one to two years.[50] But this decrease in cost comes as a tradeoff—the longer insecure equipment stays in the networks, the higher the security risk.

Auditing Proposals

Any funding mechanism must come with an effective auditing mechanism to ensure that the funds are used efficiently, and for their intended purposes. Additionally, auditing could extend to supported carriers' network security practices to ensure they are doing everything they

[45] *Id.*

[46] Jeff Johnston, Senior Economist, CoBank, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[47] Carri Bennet, General Counsel, The Rural Wireless Association, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[48] Alexi Maltas, Senior Vice President, General Counsel, Competitive Carriers Association and Christopher Reno, Director of Accounting, Union Telephone Company, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[49] *See generally* The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019) (Panel 3: Fund It: National Problems Require National Solutions).

[50] *Id.*

can to comply with best practices and requirements to avoid cyber risks and not create additional security-related expenses. In this sense, auditing could provide an opportunity to ensure that funding recipients are following industry best practices related to cyber-hygiene and cyber security practices.

One common theme heard from rural wireless service providers during the June workshop and in other meetings,[51] is that they have not been able to purchase equipment from major European network suppliers because those suppliers struggle to justify the cost of serving small, rural carriers versus the likely benefits from doing so.[52] Service providers also noted that even when they were able to purchase network equipment from European providers, it would often be prohibitively expensive.

However, during the workshop, equipment manufacturers expressed their commitment to helping create secure networks. Specifically, Nokia committed to facilitating financing for smaller carriers, understanding the sensitive national security nature of this problem and the struggles small carriers face in solving it.[53] Nokia explained that financing terms, rather than raw price, are often what make equipment purchases possible. Nokia's commitment is promising, and hopefully other manufacturers are similarly positioned or will follow suit.

Equipment manufacturers at the June workshop noted that it would be difficult for them to create customized networks for each U.S. wireless service provider with problematic equipment that needed to be replaced. But they also discussed the possibility of working with groups of small wireless providers to create packages that would serve the needs of multiple providers while aggregating equipment orders to a volume that would more closely fit with the manufacturers' current business models.

Legislative Proposals

The bipartisan *United States 5G Leadership Act of 2019*, which was introduced in the Senate in May 2019, would establish the "Supply Chain Security Trust Fund" and allocate $700 million dollars from future spectrum auctions to fund equipment replacements.[54] The Senate

[51] Commissioner Starks addressed the Competitive Carrier Association's 2019 annual conference in Providence, Rhode Island in September 2019. While there, he met with small wireless carriers who have Huawei and ZTE equipment in their networks to hear, first hand, about the conditions they are facing and their concerns with the prospect of ripping and replacing their equipment. Commissioner Starks also addressed the U.S. Chamber of Commerce Rural Engagement Initiative event in October 2019 and met with other small wireless carriers during that event.

[52] Drew Fitzgerald & Stu Woo, *In U.S. Brawl With Huawei, Rural Cable Firms Are an Unlikely Loser*, Wall St. J. (Mar. 27, 2018), https://www.wsj.com/articles/caught-between-two-superpowers-the-small-town-cable-guy-1522152000.

[53] Brian Hendricks, Vice President of Policy and Government Relations, Nokia, Statement at The Security Threat within our Communications Networks: Find It, Fix It, Fund It Workshop (June 27, 2019).

[54] *United States 5G Leadership Act of 2019*, S. 1625, 116th Cong. (2019).

Commerce Committee reported the bill favorably out of committee in July and it now awaits consideration by the full Senate. A similar bill, the *Secure and Trusted Communications Networks Act*, was introduced in the House in September 2019 and would provide $1 billion to replace insecure and untrustworthy equipment.[55] Such legislative actions are critical to ensuring funding for replacement of this equipment.

Conclusion

Emerging 5G technology holds great promise, with the potential to benefit all aspects of America life, from health care to education to public safety. But 5G also puts a spotlight on network vulnerabilities that must be addressed if those benefits are to be fully realized. Thanks to participation of a wide variety of industry experts, this workshop helped to define the nature of threats to our communications networks posed by China and Chinese-manufactured communications equipment. They also point the way forward: finding and replacing untrustworthy equipment is a national problem that requires a national solution. I look forward to working with these stakeholders, leaders in government, and the communications industry as whole toward a comprehensive solution.

[55] *Secure and Trusted Communications Networks Act of 2019*, H.R. 4459, 116th Cong. (2019).

Workshop Agenda

"SECURITY VULNERABILITIES WITHIN OUR COMMUNICATIONS NETWORKS: FIND IT, FIX IT, FUND IT"
STAKEHOLDER WORKSHOP

CONVENED AND MODERATED BY
COMMISSIONER GEOFFREY STARKS

Federal Communications Commission
445 12th Street S.W., Commission Meeting Room, Washington, D.C. 20554

June 27, 2019
9:30 AM – 1:00 PM
A recording of the event can be viewed online at
https://www.fcc.gov/news-events/events/2019/06/security-threat-within-our-communications-networks-find-it-fix-it-fund-it.

Workshop Agenda

9:30 AM **Welcoming Remarks from Commissioner Starks**

"Description of the Threat"
Jim Lewis, Senior Vice President and Director, Technology Policy Program, Center for Strategic & International Studies (CSIS)

Professor Jonathan Mayer, Assistant Professor of Computer Science and Public Affairs, Princeton University

Panel 1
10:00 AM **Find it: The Scope of the Problem**
This panel will focus on how to identify which equipment poses a threat and where it is located.

Panelists:

- **Brian Hendricks**, Vice President of Policy and Government Relations, Nokia
- **Jim Lewis**, CSIS
- **John Nettles**, President, Pine Belt Telephone Company
- **Mike Saperstein**, Vice President, Policy & Advocacy, USTelecom

Panel 2
11:00 AM

Fix It: How to Ensure that Networks are Secure

This panel will consider options for fixing identified security problems, including discussion of what equipment needs to be fixed, whether replacing equipment is the best approach, or whether monitoring or other measures can be part of the solution.

Panelists:

- **Carri Bennet**, General Counsel, The Rural Wireless Association
- **Bill Chotiner**, Director, Radio Access Network Evolution, Ericsson
- **Travis Russell**, Director of Cybersecurity, Oracle Communications
- **Dileep Srihari**, Senior Policy Counsel and Acting Head of Government Affairs, Telecommunications Industry Association (TIA)

Panel 3
12:00 PM

Fund It: National Problems Require National Solutions

This panel will address questions regarding funding, including the amount required for equipment replacement and threat mitigation, potential public and private sources, and what safeguards and other conditions should be attached.

Panelists:

- **Jeff Johnston**, Senior Economist, CoBank
- **Alexi Maltas**, Senior Vice President, General Counsel, Competitive Carriers Association (CCA)
- **Christopher Reno**, Director of Accounting, Union Telephone Company

12:55 PM **Closing Remarks from Commissioner Starks**