Silicon Flatirons

KNOW WHAT'S NEXT.

Roundtable Report

Spectrum Vulnerabilities
March 22, 2019
Washington, DC

Chris Laughlin[*]

June 28, 2019

(Version 1.0)

Silicon Flatirons is a center for innovation at the University of Colorado Boulder to serve students, entrepreneurs, policymakers, and professionals at the intersection of law, policy, and technology.

Roundtable Reports capture thoughtful analysis of various issues in law, technology, and entrepreneurship. They are derived from roundtable conversations hosted by Silicon Flatirons that include academia, policymakers, legal professionals, entrepreneurs, and students sharing their knowledge and best practices on specific topics.

Flatirons Reports are published at siliconflatirons.org.

[*] Chris Laughlin is a 2016 graduate of the University of Colorado Law School where he was actively involved in Silicon Flatirons. He is currently an associate in the Communications Practice Group of Kelley Drye & Warren LLP in Washington, DC and remains engaged with Silicon Flatirons through its events and policy discussions. Chris would like to thank Pierre de Vries and Dale Hatfield far their feedback and guidance in drafting this report.

Executive Summary

Wireless systems have become indispensable to government, business, and public life, but the inherent openness of these systems at the RF Layer introduces spectrum vulnerabilities that can be exploited by malicious actors or result in harmful interference. Yet, policymakers and stakeholders have only recently begun to focus on the security of these systems. On March 22, 2019, Silicon Flatirons convened an expert roundtable in Washington, DC to discuss the state of spectrum vulnerabilities, identify ways to increase awareness and understanding of these vulnerabilities, and motivate policymakers and stakeholders to make concerted efforts to address them. The discussion focused on three categories of challenges:

> ***Detecting and Understanding Spectrum Vulnerabilities.*** There are not adequate systems and processes in place to detect and understand what spectrum vulnerabilities exist, according to the participants. Absent this knowledge, vulnerabilities cannot be prioritized to be addressed. The critical factor identified during the discussion is insufficient data sharing among wireless system operators and with the government. To address this, participants coalesced around the idea of data sharing clearinghouses, such as an Information Sharing and Analysis Centers (ISACs). The participants also highlighted the need for increased data collection and analysis, research and testing, government resources, and education of vulnerabilities among policymakers and the public.
>
> ***Identifying and Mitigating Causes of Spectrum Vulnerabilities.*** A general conclusion among the participants was that spectrum vulnerabilities persist because there is a lack of security by design. The commoditization of wireless systems creates incentives for developers to prioritize system performance and speed to market over security and quality assurance testing. This is coupled with increased system complexity, including where several components are combined into one system, obscuring the cause of vulnerabilities. These practices increase the challenge for standard setting bodies, which some said are not doing enough to emphasize security by design. Participants discussed how increased research and testing could facilitate security by design and how system complexity can be used as a mechanism to mitigate vulnerabilities.
>
> ***Classifying and Prioritizing Spectrum Vulnerabilities.*** Classifying the criticality of vulnerabilities is essential to prioritizing and allocating resources to address risks, but there was little agreement among participants on what the classifications should be. Some suggested that vulnerabilities in public safety and national security systems are more critical than those in commercial systems. Others were concerned that low probability, high impact vulnerabilities are not being adequately addressed. Others still highlighted the importance of addressing protocol attacks, which are easy to do, but difficult to detect. Cutting across all of these was a concern shared by the participants that vulnerabilities raising safety-of-life risks should be a top priority.

This roundtable discussion was a starting point. The solutions proposed by the participants are helpful, but more challenges were raised than solutions proposed. The participants agreed that further discussions must take place to assess challenges and to develop more detailed solutions on how to address them. There was consensus that a conference or another roundtable that brings together experts in government, industry, and academia is an appropriate next step.

Contents

Introduction

We rely on spectrum more than ever for essential services and personal communications. The wireless systems that utilize spectrum are indispensable to public safety and national security communications, business and critical infrastructure operations, navigation, socializing, and entertainment. Our reliance on radios is only expected to increase. The most recent projections suggest that there could be more than 27 billion wireless connected devices by 2022 accounting for over 70% of internet traffic.[1] However, policymakers and stakeholders have only recently begun to focus on the security of wireless services, raising concerns that spectrum vulnerabilities are not being adequately addressed with sufficient funding and an acceptable amount of risk.

On March 22, 2019, Silicon Flatirons convened a roundtable discussion entitled "Spectrum Vulnerabilities" in Washington, DC at the offices of Kelly Drye & Warren LLP. The event brought together experts from government, academia, and industry to discuss the state of spectrum vulnerabilities, identify research areas and topics of preliminary consensus, increase awareness and understanding of vulnerabilities, and motivate policymakers, industry, and other stakeholders to make concerted efforts to address them.[2] The participants also considered whether the lack of awareness and severity of vulnerabilities requires further dialogue.

The roundtable was premised on the assumption that RF Layer, or Radio Layer, vulnerabilities, in particular, need greater attention from policymakers and stakeholders.[3] RF Layer vulnerabilities are unavoidable because wireless systems are inherently open: inputs into radio receivers cannot be sealed off and wireless links cannot be completely isolated. Left unaddressed, these vulnerabilities can be exploited by malicious actors or be the source of non-malicious harmful interference, both of which can have high social and economic costs. Certain malicious disruptions that occur at the RF Layer—jamming, spoofing, and sniffing attacks—are inherent to wireless networks. Jamming occurs in wireless receivers and affects the availability and reliability of networks.[4] Spoofing and sniffing occur on the wireless links and can result in corruption of the communications data, forgery of the data, and interception that undermines the privacy and secrecy of communications.[5]

[1] *See Internet of Things Forecast*, Ericsson, https://www.ericsson.com/en/mobility-report/internet-of-things-forecast (last visited June 25, 2019) (noting 29 billion by 2022 with small amounts for phones and computers using wired connections); *Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper*, Cisco (Feb. 27, 2019), https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html.

[2] *See* Appendix A for a list of roundtable participants with their titles and affiliations.

[3] The organizers considered the RF Layer to include both electromagnetic radiation and the PHY layer of the OSI protocol stack.

[4] Jamming disrupts the reception of a desired signal and can occur through brute force, where a stronger signal overpowers the desired signal in the receiver, and through smart jamming techniques, *e.g.*, time correlated, protocol aware, and ability to learn. *See* M. Lichtman, *et al.*, *A communications jamming taxonomy*, 14 IEEE Security & Privacy 1, 47-57 (2016).

[5] Spoofing tricks or deceives radio receivers by transmitting a counterfeit signal in order to produce erroneous results or extract sensitive network and end user information. *Glossary*, ATIS, https://glossary.atis.org/glossary/spoofing/?search=spoof&page_number=&sort=ASC (last visited June 25, 2019). Sniffing captures content and metadata associated with the message being transmitted, and it can be used to learn about the technical characteristics of the target to enable the crafting and launching of tailored jamming and

Disruption can also occur at other layers of the protocol stack. These include natural forms of interference, poor system design, physical attacks on infrastructure, and cybersecurity attacks. Unlike RF Layer attacks, which occur in inherently open portions of wireless systems, cybersecurity attacks constitute unauthorized access into closed portions of systems. The roundtable premise also assumed that cybersecurity risks, which are not unique to wireless systems, are likely addressed adequately in other fora. However, some roundtable participants disagreed with that premise, so there was discussion of those risks as well. Some also noted that software-defined radios and other network developments have obscured the clear division of layers, and as a result, modern spectrum vulnerabilities can cross layers.

This report is broken down into three broad topics: (1) detecting and understanding spectrum vulnerabilities, (2) identifying and mitigating causes of spectrum vulnerabilities, and (3) classifying and prioritizing spectrum vulnerabilities. The discussion followed a modified version of the Chatham House Rule—some participants are quoted and paraphrased in this report, but not by name or affiliation.[6]

Detecting and Understanding Spectrum Vulnerabilities

The roundtable started by asking participants to classify and prioritize spectrum vulnerabilities, but it became quickly apparent that there are not adequate systems and processes in place to allow stakeholders to detect and understand the existence and seriousness of spectrum threats. The consequence, according to one participant, is that if the threats cannot be quantified, they cannot be prioritized, and if they cannot be prioritized, funds cannot be allocated to address them. Participants offered several recommendations that would facilitate the identification and understanding of spectrum vulnerabilities, including increased data collection, data sharing, and research and testing, as well as more and better use of government resources and better education about spectrum vulnerabilities for policymakers and the public.

Data Collection and Analysis

Several participants said that there needs to be greater data collection to be able to identify and address spectrum vulnerabilities. They provided a few reasons why there is insufficient information collection now. As an initial matter, one participant said that many instances of spectrum harm go unreported. In some instances, the user may not even know there is harmful interference that should be reported. For example, when the harmful interference causes equipment degradation, the user might simply believe that the equipment is malfunctioning, not that the user is the victim of intentional or unintentional interference.

Even for users that want to identify if they are the victim of interference, it can be difficult to get visibility into whether they are being attacked. One participant noted that "[commodity hardware] is not designed to enable an engaged defender." At a broader scale, another wondered if part of the problem is that network operators have outsourced expertise about how their networks

spoofing attacks that are more efficient or have greater impact. Bradley Mitchell, *What Is a Network Sniffer?*, https://www.lifewire.com/definition-of-sniffer-817996 (updated May 16, 2019).

[6] Under the Chatham House Rule, participants are free to use and discuss information received, but neither the identity nor the affiliation of any participant may be revealed. This rule was modified so that participants could be quoted and paraphrased with their permission.

function to their vendors. Some participants disagreed. One explained that operators collaborate with their vendors to share and understand information about network services and features. Another, however, noted that while large operators tend to know what is happening in their systems, smaller operators "are the real vulnerability," though "there is a significant interplay between the vendor community and the operators" in all cases.

To address the shortcomings in information gathering, a number of participants suggested that communications equipment could be designed to detect and report potentially harmful interference. One, for example, suggested that there could be a cell phone app that monitors a phone's radio communications for unusual activity that would be reported to the user, but added that there would need to be design modifications in phone specifications to make this feasible. Another offered an analogy to developments in data collection from vehicles. In that context, insurance commissioners were interested in vehicle data to help develop risk models that they could use to set insurance premiums, so the data collection and delivery was being built into the architecture of the cars. A third participant raised artificial intelligence machine learning as a potential solution, saying it could be used to "detect intruders or jammers, not necessarily by demodulating their signals but by observing behavior and trying to look for patterns." That data could then be reported.

Other participants said there are opportunities to understand the scope of spectrum threats with data that is already being collected.[7] One said that 911 data could be insightful as to harmful interference. If the 911 data is being analyzed and calls decrease significantly on a median or a mean basis, then there may be a jammer that is preventing communications. Another said that "there are a fair amount of measurements that are made in radios today" and that "[t]here's certainly a lot of work that can be done . . . to enhance security by just looking at what is being sent out." The challenge is that measurements are very rarely transmitted to network management systems, which typically processes network data. Manufacturers and operators may consider the backhaul for the data transmission to be an unnecessary business expense or the data processing to be a burden on the network management system. The participant was hopeful, however, saying that because networks are generally built as distributed systems, there are many opportunities to insert monitoring software that can get behavioral information or phenomena off the system. Many large operators probably generate enough data within their own network to draw conclusions. The participant was also optimistic that this information could be used to alleviate other concerns, discussed in greater detail below, such as inadequate data sharing (if the software can anonymize the data) and supply chain risks. As to the latter, assessments of system behavior could build a degree of trust in the supply chain, instead of using tight controls on supply sources.

Data Sharing

Even when there are tools to collect and process data, there was broad consensus that there needs to be greater data sharing among wireless system operators and with the government. With sharing, operators would have the information they need to mitigate risks and broader efforts could be implemented to prevent vulnerabilities.

[7] Some participants said that data privacy should be maintained when data is collected and processed.

Participants offered a few reasons data is not being shared. First, there was an understanding that operators might be reticent to share data regarding harmful interference events in general because it might contain confidential or proprietary information or information that could be used to assess liability. Second, information sharing might not occur because there is a lack of reporting tools. One participant noted that the Federal Communications Commission (FCC) has some interference reporting tools, but that there needs to be more effort by federal agencies to capture information.[8] Third, there was some agreement that operators are hesitant to share information with the government after the National Security Agency's massive surveillance program was revealed in 2013. On that point, a participant said that operators do not want to share their vulnerabilities because "they're afraid that they'll get weaponized and shipped out" by the government.

Several solutions were suggested to address data sharing shortcomings. With respect to the sharing of confidential and proprietary information or information that could be used to assess liability, one participant said the data could be anonymized. With regard to whom the data should be shared, a different participant said it could be provided to a system architecture group handling measurements within the 3rd Generation Partnership Project (3GPP).[9] Another suggested that spectrum vulnerabilities could be reported to something similar to the United States Computer Emergency Readiness Team (US-CERT). US-CERT, which is now part of the National Cybersecurity and Communications Integration Center (NCCIC), is a government entity that operates as a global information exchange clearinghouse for computer vulnerabilities, communicating risks to operators so that they can be mitigated.[10]

One participant offered an approach focused on data sharing between operators and across sectors—Information Sharing and Analysis Centers (ISACs). ISACs are sector-based organizations, generally established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation.[11] ISACs collect threat information from their members, then analyze and disseminate actionable threat information to their members and provide members with tools to mitigate risks and enhance resiliency.[12] The participant added that information sharing with ISACs is not necessarily anonymized; however, information is not shared publicly and in many cases is not shared with the government so that members do not have to worry about liability. The existing Communications ISAC is unique, however, in that it is closely tied to the government.[13] The proposer noted that the Communications ISAC is not necessarily the proper ISAC for spectrum vulnerabilities. The ISAC

[8] *Interference Complaints*, FCC, https://www.fcc.gov/reports-research/guides/interference-complaints (last visited June 25, 2019).

[9] 3GPP consists of seven telecommunications standard development organizations which collaborate to produce reports and specifications for 3GPP technologies, such as security and quality of services for cellular telecommunications network technologies. *About 3GPP*, 3GPP, https://www.3gpp.org/about-3gpp (last visited June 25, 2019).

[10] *About Us*, NCCIC, https://www.us-cert.gov/about-us (last visited June 25, 2019). NCCIC says it "bears a significant responsibility to protect the information we receive and to ensure we safeguard privacy, business confidentiality, civil rights, and civil liberties." *Id.*

[11] *About ISACs*, National Council of ISACs, https://www.nationalisacs.org/about-isacs (last visited June 25, 2019).

[12] *Id.*

[13] The Communications ISAC is also known as the Department of Homeland Security (DHS) National Coordinating Center, and it serves as an operational component within the NCCIC. *Member ISACs*, National Council of ISACs, https://www.nationalisacs.org/member-isacs (last visited June 25, 2019).

needed for spectrum vulnerabilities would have little to no government involvement—to alleviate concerns about information sharing with the government—and would be cross-sector, as spectrum vulnerabilities can affect many other industries, such as the healthcare and automotive industries.

Research and Testing

Closely tied to the data collection and data sharing issues is the need for research and testing. Several participants said that researchers are not getting the data they need to conduct testing. One noted a need for a concerted effort—at least within the government—of curating data and making it available to researchers so they can try their research ideas. Another agreed: "[G]etting data is really hard. It took us a year to get some data from a service provider," and that was for a very altruistic test meant to address vulnerabilities during disasters. A third elaborated further, saying "[w]ithout the data, the academics are very much at a loss." That participant went on to explain that data sharing with academics proved critical in addressing cybersecurity risks in the early 2000s. The Defense Advanced Research Projects Agency (DARPA) had conducted research on packet tracing and anomaly detection, and "[e]very paper you saw in a cybersecurity conference ended up relying on the DARPA research results."[14]

If information is not shared with researchers, then researchers need adequate testbeds to get the data themselves. A participant explained that "one of the biggest problems is that we as a user community are beholden to a network after it has been designed, and deployed, and commissioned. There is very little testing before the fact that our researchers can do." In addition, academic researchers "are increasingly limited by what [they] can demonstrate beyond just paper and analysis simulations," in part "because they don't have access to real-life networks that they can experiment with." Closed-form solutions are becoming less viable because of increased system complexity, discussed in greater detail below. Another participant highlighted a different, but related barrier for researchers: expense. The entry-level price for a certain piece of LTE testing equipment is a quarter of a million dollars, and for proper testing, a half-million-dollar piece of equipment is needed—these are too expensive for academic researchers to obtain on their own. The participant said that we might need to develop tools to reduce costs for universities.

A different participant noted that testbeds already exist and are being used by vendors, but that there needs to be "opportunities for academics to get access to those non-real-time networks." According to another participant, the National Science Foundation (NSF) is making strides toward developing testbeds through its Platforms for Advanced Wireless Research (PAWR) program. PAWR is a collaboration between NSF and 28 leading wireless industry companies and associations that is working to develop up to four city-scale research testbeds for wireless testing.[15] To make testing fully successful, however, a participant commented that we need a red-blue team type of test bed and more vertical integration of equipment manufacturers, just as the Chinese have with Huawei, so that there can be end-to-end testing all the way down to the chip level.[16]

[14] *See, e.g.*, W. Timothy Strayer, *et al.*, *Traceback of Single IP Packets Using SPIE*, IEEE Computer Society (2003), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.78.9466&rep=rep1&type=pdf.

[15] Platforms for Advanced Wireless Research, https://advancedwireless.org/ (last visited June 25, 2019).

[16] This refers to red team-blue team simulations, where the red team tests vulnerabilities and the blue team defends against the red team's attack. *See* Doug Drinkwater and Kacy Zurkus, *Red team versus blue team: How to run an*

Government Resources and Authority

A number of participants identified government resources as a potential bottleneck for progress on identifying spectrum vulnerabilities. Indeed, the point made at the outset that spectrum risks cannot be funded if they cannot be identified and quantified was made in the context of allocating limited government resources. The Federal Communications Commission (FCC), for example, has fewer than 200 people in its Enforcement Bureau, split among six divisions, only some of which are able to investigate spectrum issues. The FCC is also limited to policing commercial spectrum—government spectrum is managed by the National Telecommunications Information Administration (NTIA). Moreover, the FCC can only exercise civil authority against those violating the Communications Act—it cannot independently go after criminal actors. While other agencies may have authority to go after criminal actors, they have their own resource limitations.

A participant explained a related problem: how the disbursement of government resources hinders efforts to address spectrum vulnerabilities. The communications industry developed in silos—wired and wireless—and correspondingly, so did government resources meant to address risks with those networks. Yet, these networks are not used in silos, at least not any longer; they are converging. "That presents an enormous policymaking, and really societal governance challenge, because although we have . . . probably dozens of entities in just our federal government that work on some angle of [spectrum and wireless communications] issues, many of them don't even know that the other ones exist," the participant explained.

Education

The participants reached some consensus that there needs to be greater education of spectrum vulnerabilities for policymakers to ensure the risks are adequately addressed. There tends to be inadequate attention paid to identifying and responding to problems until a major outage or other event has already occurred, one participant said. Another asked, "how many members of Congress or cabinet secretaries could explain to you what the difference between 4G and 5G is?," adding that "[w]e need to figure out how we rationalize all of these complexities, and then come up with solutions." A third participant said "it probably will take years to educate lawmakers so that they do what you think is the right thing, and with any luck, don't actually screw it up worse. It's more than just an engineering issue. It's an education issue."

Others noted a need for public education as well. "It's very important for people to understand. Everybody talks about spectrum. Nobody knows what it is," noted one. Some members of the public simply do not know that the equipment they are using might be causing harmful interference or that they might be under the jurisdiction of a federal agency's enforcement authority, a participant explained. Another said that "[o]ne reason that people don't understand this is they don't even have a way to see it," adding that there are some great visualization tools, like Wireshark, that can be used at the middle school and high school level to show students what spectrum is.[17] Relatedly, the first participant described an event at New York University where

effective simulation, CSO (July 26, 2017), https://www.csoonline.com/article/2122440/emergency-preparedness-red-team-versus-blue-team-how-to-run-an-effective-simulation.html.

[17] Wireshark is a network protocol analyzer that can be used to assess network diagnostics. Wireshark, https://www.wireshark.org/.

high school teachers were brought in and educated about spectrum, and then took that information back to their classrooms along with some tools they could use to show students how to find white spaces.

Identifying and Mitigating Causes of Spectrum Vulnerabilities

Apart from detecting and understanding spectrum vulnerabilities, there was extensive discussion about the causes of spectrum vulnerabilities and what tools can be used to mitigate those vulnerabilities. The primary topics of conversation were system design and complexity, supply chain security and diversity, standard setting, adoption of standards, and availability of harmful equipment.

System Design and Complexity

Several participants identified various aspects of system design and complexity as sources of spectrum vulnerabilities, including how the commoditization of equipment creates misaligned incentives for developers, insufficient attention to known vulnerabilities, the magnification of vulnerabilities when system and equipment components are combined, and misperceptions over exactly how much complexity exists in systems. There was cause for some optimism among the participants, however, as several discussed how system complexity can serve to mitigate spectrum vulnerabilities.

A couple of participants noted that equipment commoditization creates misaligned incentives for system developers. One said that for 5G, the priority is placed on high-speed and low-latency at the expense of resiliency. When it comes to Internet of Things (IoT) devices, another noted that "[e]verybody's trying to get their product out on the street and not thinking about what security risk the product might represent."

Regardless of the system, a participant suggested that unintentional design vulnerabilities create a greater risk than back doors intentionally built into the equipment, which are discussed below in relation to supply chain concerns. Some manufacturers are selling low-quality products because they are trying to keep costs low, so they race the product to market with buggy code and no quality assurance testing. Adversaries can simply probe the products to find vulnerabilities—quipped that participant, "Is that a back door? I don't know. It's a bug door."

Relatedly, some participants expressed concern that there is simply not enough attention paid to known vulnerabilities in wireless communications systems. One said that "we spend a lot of energy in making our systems easy to find," which is necessary for users to be able to easily use devices, but that this kind of openness prevents the ability to apply encryption and other protections. Two participants raised the issue of vulnerabilities associated with passive intermodulation (PIM), which can be exploited for much more sophisticated attacks.[18] One of them said that PIM vulnerabilities are "something that a lot of the people designing, building, and operating the systems do not quite understand." A different participant raised another risk, saying that the wireless industry's LTE (aka 4G) specifications offer a software stack directly connected

[18] PIM is when the interaction between different physical elements in a network results in interference. See Lou Frenzel, *Passive Intermodulation (PIM): What You Need To Know*, Electronic Design (Mar. 5, 2013), https://www.electronicdesign.com/wireless/passive-intermodulation-pim-what-you-need-know.

to an input that cannot be controlled and worries that the same will be true for 5G networks because there is not enough effort being made to build secure low-level protocols.

System and equipment design vulnerabilities are magnified when vulnerable components are combined into other equipment and systems. This introduces a level of complexity into the system that obscures the source of the vulnerability, because the vulnerability can be used to affect other parts of the system. One participant explained further: the vulnerable components are being advertised as "peak performance"—lowest latency or maximum throughput, for example—so "they're being bought, and then put into systems by people who don't really understand . . . the underlying issues that could occur . . . and integrat[ed] into systems that have safety-of-life issues." Similarly, another participant expressed concern at the huge increase in the number of devices that are relying on underlying systems that have vulnerabilities. For example, a participant observed, "Today, over half of medical devices that use wireless will use . . . Bluetooth low-energy" in the congested unlicensed spectrum band. From the perspective of a product developer, it is a logical decision, but not one that is made with the goal of preventing vulnerabilities. On a broader scale, another expressed concern about risks to public safety communications and FirstNet, which are consolidating onto commercial networks that may not be sufficiently hardened.

Vulnerabilities may also exist because the level of diversity (and thus resilience) of system designs can be overestimated. One participant provided an anecdote about a 2004 Baltimore tunnel fire that took out all the wired communications in the city. Everyone thought the system was diverse because there were multiple carriers, but all the carriers ran their fiber communication lines through that one tunnel.

While system design and complexity was an identified source of spectrum vulnerabilities, many participants agreed that it could be used to mitigate vulnerabilities. As one put it, "complexity is our friend, as well as our enemy." The participants offered several suggestions that could prove valuable, including:

- **Dynamic Spectrum Operations –** There is a fair amount of frequency diversity in commercial spectrum, so if part of the system is brought down, operators can fall back to other bands.[19]

- **Sensing Capabilities –** Newer technologies are being developed and deployed that are able to detect operations across frequencies and provide information in near-real time that can be used by operators to make choices about whether detected operations pose a threat to intended operations. Sensing capabilities could be coupled with automation to facilitate dynamic spectrum operations.

[19] Subsequent to the roundtable, the White House Office of Science and Technology Policy released a report that highlights research and development priorities for America, which discusses the types of research and development that is needed or under way to facilitate dynamic spectrum operations and sensing capabilities. *See Research and Development Priorities for American Leadership in Wireless Communications*, OSTP (May 2019), https://www.whitehouse.gov/wp-content/uploads/2019/05/Research-and-Development-Priorities-for-American-Leadership-in-Wireless-Communications-Report-May-2019.pdf.

- **Backup Systems –** There should always be a backup system, said one participant who described a project to test whether the GPS on a cellular phone could serve as the backup when the GPS in an autonomous vehicle is being jammed.

- **System Segregation –** Separating the control signal from other components, such as the infotainment system in a connected car, reduces the entry points for malicious actors seeking to cause harm.

- **Terrain Mapping –** There is enough data and processing power now that terrain mapping can be used as an alternative or supplement to GPS.

- **5G Technology Programmability –** Participants identified several opportunities where 5G technology could be programmed to increase security at both the RF Layer and protocol layers, including monitoring, artificial intelligence, network slicing (so users can define their own security and authentication), and enhanced geolocation capability apart from GPS.

- **Spatial Processing Using Multiple Input, Multiple Output (MIMO) –** MIMO is currently being used to enhance performance, but it can also be used as a spatial processor to identify the source of interference, thereby reducing the anonymity of nefarious actors.

Other mitigation mechanisms mentioned by participants were encryption, use of increased timing capabilities to reduce anonymity in system operations, spread spectrum, higher barriers to gain access to networks, and reduced availability of information about how systems operate to increase obscurity to nefarious actors.[20]

Supply Chain Security and Diversity

Supply chain security and diversity was an urgent issue for two participants. The first one described supply chain vulnerabilities as the source of the "true doomsday" scenario, with so many risks that it is overwhelming. This participant (and others) alluded to concerns with telecommunications equipment developed by Huawei, which the Trump Administration recently blacklisted in the U.S. and has sought the same by U.S. allies in the development of 5G networks.[21] There are concerns that the company is building back doors into its technology that the Chinese government can later use for spying.[22] "[Y]ou could have a good radio design, but if there's malware implemented, if there's questions about the code, [or about] who has access to your

[20] Spread-spectrum signals are intentionally made to be a much wider band than the information they are carrying to make them more noise-like, causing them to be harder to detect, intercept, demodulate, and jam. Prabakar Prabakaran, *Tutorial on Spread Spectrum Technology,* EE Times (May 6, 2003), https://www.eetimes.com/document.asp?doc_id=1271899#.

[21] Ian King , Mark Bergen , & Ben Brody, *Top U.S. Tech Companies Begin to Cut Off Vital Huawei Supplies* (May 19, 2019), https://www.bloomberg.com/news/articles/2019-05-19/google-to-end-some-huawei-business-ties-after-trump-crackdown.
Todd Shields & Bill Allison, *Trump Is Losing the Fight to Ban Huawei From Global Networks*, Bloomberg Businessweek (May 9, 2019), https://www.bloomberg.com/news/articles/2019-05-09/trump-is-losing-the-fight-to-ban-huawei-from-global-networks.

[22] *Id.*

network infrastructure from anywhere around the globe," that raises cybersecurity and national security concerns, the second one explained. The first provided this scenario:

> Think about 5-10 years from now, when we're well into the 5G era, and everything is connected, and there are a multiplicity of diverse entities that are being connected in a way that is completely opaque or unknown to most policymakers, to most individuals, to most companies, and it's a web that's as complex as the global Internet itself. It runs everything from connected cars, to insulin pumps, to lights—everything. Everything that's life-sustaining and just general entertainment. A hostile intelligence service [that] has access to how that system functions [can commandeer, sabotage, or surveil the core network].

For example, the actor could gain access to the network and change the channels within radios to cause massive pileup pollution within an LTE network to cause jamming, the second added.

Yet companies, like Huawei, which the same participant suggested is subsidized by the Chinese government, are offering their products for the cheapest price, so that is the equipment that is being deployed despite the risk of vulnerabilities. The problem is then exacerbated because some—particularly smaller—operators will depend on the companies producing the vulnerable products for engineering and software support services. "Now, you've got the fox watching the hen house," this participant said. The first participant explained that the ubiquity of technology from one source is what actually creates the risk, saying that the way an intelligence service would gain leverage over a society is not by incorporating back doors into the network, but simply "by building the network, and thereby knowing the network better than anybody else does, then using that as long-term strategic leverage so that it might do something 5, 10, 20 years later."

Another concern about telecommunications infrastructure is that the number of trusted suppliers is dwindling. "What happens to this country if one of our trusted suppliers gets in more financial trouble, and we're left with a global infrastructure—a global source—that we can't trust?" the second one asked.

Standard Setting

Many participants commented that standard setting is falling short of addressing system design, system complexity, and supply chain issues. They suggested a number of possible reasons, including the complexity, the limited role of the U.S. government in standard setting bodies, and that standards are often being developed after innovations are already on the market.

Some said the complexity of systems, which standards are meant to address, is the reason standards are not working. In essence, according to two participants, standard setting organizations decide on what modes must be supported, and those modes get tested within the system architecture to ensure they meet the standards. However, there are many optional features—which may have vulnerabilities or that introduce vulnerabilities when they are combined with other components—that are not tested or there are not standards developed to account for those features.

Others said that the U.S. government is not playing a strong enough role in standard setting bodies. One participant said, "[T]here is a culture here in the United States that the government does not get involved in standards"—the government wants industry to do it. While another noted that there are several government representatives involved in 3GPP, there seemed to be some consensus that U.S. government representatives tend to be “note takers”—that is, they are not actively contributing to standards development. Another said the cause “is the notion of technology neutrality, because the government doesn’t want to get involved in determining what technologies get implemented in the field.” Consequently, the standards pushed by other governments, such as China, are the ones that get implemented.

Others said there is not enough being done before standards development takes place, tying the issue back to the need for greater research and testing. One participant commented that while 3GPP does great work on standards development, what is needed is a “cycle of innovation, research, implementation,” which needs concerted effort from industry, government, and academia. “[I]f we really want to address these big problems . . . [w]e have to strive to somehow replicate what this wireless world is today and build our research programs around that, rather than the other way around,” where we identify vulnerabilities after the fact. Another participant touched on this as well: “[Y]ou just can’t nominate a standard. You’ve got to have a testbed. You’ve got to show that it works. You’ve got to show it’s the best way to go forward.” A third participant agreed with these sentiments and said we should learn from the Chinese, who were locked out of 3GPP. They developed the FuTURE Forum, described as “a pre-game show for standards, where they bring in companies, and universities, and government researchers together to talk about, what are the problems, and what sort of technology solutions do you have.”[23] That information was then brought to standardization bodies.

Adoption of Standards

Even if the right standards are developed and are effective, the participants struggled with how to ensure that system and equipment developers implement them. One wondered how the government can drive security protocols in the supply chain in a market economy. The only teeth the government has is federal dollars (*i.e.*, procurement and grant money), but there seemed to be general consensus that this is inadequate. As some participants discussed, the population of the U.S. is 330 million people, but the public safety population is roughly 3 million people, or about one percent.[24] The public safety market does not have enough influence to change industry behavior on its own. The challenge is amplified when compared to the global population and the global market for equipment development.

Participants offered a range of solutions to this challenge. One argued that after the proper standards are developed, forceful recommendations would be sufficient. Another said that the FCC or other agencies should implement regulations mandating the adoption of standards. One commenter put a finer point on the need for regulations: if the FCC does not have a rule, it cannot enforce standards, explaining how the agency’s efforts to enforce non-rule-based standards in another context were overturned in court. Another commenter had two suggestions: First, there could be a low-level technical remediation, where before any piece of hardware goes to market, it must undergo testing by a fuzzing suite checking for known protocol vulnerabilities, consistent

[23] *About FuTURE Forum*, FuTURE Mobile Communication Forum, http://www future-forum.org/en/aboutus.asp (last visited June 25, 2019).
[24] *U.S. and World Population Clock*, U.S. Census Bureau, https://www.census.gov/popclock/ (last visited June 25, 2019)

with the standards, and providing an evidence trail of the results.[25] Second, there could be a high-level market remediation, where developers are liable for shipping products that do not comply with standards.

Availability of Harmful Equipment

The risks associated with spectrum vulnerabilities are increasing because there is greater availability of cheap equipment for bad actors. By way of analogy, a participant described how the introduction of personal computers meant anyone could write a computer virus, saying that resulted in a huge proliferation of viruses. Now that we have cheap devices, including software defined radios, it is only a matter of time before somebody decides to build a jammer to interfere with radio communications for fun: "I just believe we're going to be hitting this part of the curve where all of a sudden, once this gets discovered, it's going to take off." A different participant said that jammers are currently available for purchase online, despite them being illegal in the U.S. There was discussion about how it is difficult for the government to police the entry of malicious, as well as non-compliant products into the U.S. because of the aforementioned limited government resources. Another participant gave an anecdote that put a finer point on the risks of malicious equipment availability. The participant described an instance where a $30 international mobile subscriber identity (IMSI) catcher was used to demonstrate how easy it is to capture not only IMSIs, but also other sensitive information from attendees at a conference, and then communicate with those people that they were the victim of an attack.[26]

Classifying and Prioritizing Spectrum Vulnerabilities

Beyond detecting and understanding spectrum vulnerabilities, and identifying and mitigating their causes, the participants discussed how to classify and prioritize these vulnerabilities. Discussion focused on (1) determining how critical particular risks are, then properly allocating resources; and (2) safety-of-life harms from vulnerabilities.

Risk Criticality and Resource Allocation

The participants discussed a few different topics regarding the criticality of risks and resource allocation, including whether commercial network vulnerabilities rise to the same criticality as public safety and national security network vulnerabilities, how to ensure resource allocation to low probability/high impact risks, and challenges associated with addressing protocol attacks.

There was some debate about whether vulnerabilities in commercial networks are as critical as those used for public safety or national security purposes. One participant asserted that

[25] "Fuzz testing (fuzzing) is a quality assurance technique used to discover coding errors and security loopholes in software, operating systems or networks. It involves inputting massive amounts of random data, called fuzz, to the test subject in an attempt to make it crash. If a vulnerability is found, a software tool called a fuzzer can be used to identify potential causes." *Fuzz Testing (Fuzzing)*, Tech Target, https://searchsecurity.techtarget.com/definition/fuzz-testing (last visited June 25, 2019).

[26] An IMSI catcher is "[a] cellular wiretapping device that simulates a cell tower. . . . [I]t logs the phone's International Mobile Subscriber Identity number (IMSI) and functions like a man-in-the-middle attack, relaying voice, text and data traffic between the real cell tower and the target device." *Definition of: IMSI Catcher*, PCMag.com, https://www.pcmag.com/encyclopedia/term/69016/imsi-catcher (May 13, 2019).

LTE and 5G networks do not need to be hardened against jamming because that kind of disruption happens primarily in military contexts and has low consequences when it occurs in commercial contexts. Another participant added, “If you look at it in terms of impact to the whole network, the amount of damage [one] can do by attacking the [RF Layer] typically ends up affecting one cell or maybe a small group of cells.” Such attacks might be significant when they impact public safety communications but are little more than an irritant in commercial contexts. A third participant shared these sentiments, suggesting that the primary vulnerability for commercial networks is congestion, which results in benign interference issues, whereas in military contexts, vulnerabilities can open the door to malicious disruption.

Not all participants agreed that vulnerabilities should not—and do not—matter to commercial actors. One said that substantial disruptions, knocking out communications across four or five city blocks, do happen to commercial networks. When commercial networks are disrupted, operator’s care because it can affect customer satisfaction and revenues, as well as garner unwanted attention from the FCC, the participant explained. Another added, “[I]f you take a large macro cell that’s serving thousands of users, that’s an incredible amount of revenue coming into the operators.”

Other participants were concerned with how to properly allocate resources to risks. One expressed concern that inadequate resources are allocated to risk scenarios that would have a high impact if they were to occur but depend on a series of circumstances happening in concert. Those scenarios may be rare—“black swan events,” a second participant chimed in—but still need to be resourced. The first participant suggested that the problem is exacerbated because, while these risks may never have happened before, they are becoming easier to do and will occur in a matter of time, when the right people are motivated. A third participant said that in the absence of risk probability, we use cost ratios where we assume every attack will be launched and allocate resources based on how much it would cost to launch the attack, how much harm would result, and how much it would cost to fix the harm. Another provided additional considerations: whether the attack is intermittent, how dispersed the attack is, and whether the attack is targeting multiple wireless resources or providers.

Much of the discussion described above is closely tied to the challenges associated with addressing protocol attacks. One participant explained that these types of attacks are such a problem because they are low cost, easy to do, and difficult to detect. Jamming can be detected if something is being radiated, and there are encryption methods for sniffing, but protocol attacks are difficult to detect and measure. Operators tend to follow the protocol without using performance measures to detect whether communications are being transmitted completely and without disruptions. That participant gave an example: “I can put a hopping signal near an LTE, and I can cause it to keep resending the data. Even though the throughput’s high, all systems look like they’re getting signals going through strong. You’re not actually getting any data. That’s not one of the performance measurements that is regularly monitored.”

Safety-of-Life Harms

The participants gave strong indications that the types of vulnerabilities that should be addressed are those that could result in a risk of physical harm to individuals. Nearly all of the examples of harmful outcomes, whether in a commercial, public safety, or military context, involved individual harms. One participant put it bluntly: “Wireless could be the new form of terrorism.” The examples provided by the participants include the following:

- **GPS Spoofing** – One participant said that “GPS is a safety-of-life system. . . . You could conceivably assassinate somebody by GPS spoofing. You could send them a false map and a false signal, and lead them right down the path, either into the hands of a bad person or a situation where they can’t recover from.” This could be exacerbated with autonomous vehicles.

- **Vehicle-to-Vehicle Communications** – A participant described how manufacturers are developing tools for vehicles to transmit intention. With these tools, one vehicle communicates to another that there is intent to change lanes so the other car makes room. The implication was that a communications disruption could be used to cause an accident.

- **Medical Device Automation** – The same participant described insulin pumps that check blood sugar levels and then automatically deliver insulin. Those insulin pumps have already been hacked by hobbyists; a nefarious actor could imitate a signal and deliver a fatal dose. Another participant mentioned recent news about how certain heart defibrillators can be hacked and have their settings changed.

- **Spectral Herding** – Spectral herding involves multiple attacks that exploit vulnerabilities on multiple bands, directly calling into question the value of mitigation through dynamic spectrum operations (noted above), and it can be used in conjunction with physical attacks. A participant said that during the Russia-Ukraine conflict, Russian-supported armed forces jammed Ukrainian military radios, so the Ukrainian military started communicating with commercial phones. The Russia-backed forces then hacked the address books of those phones and texted loved ones to say the soldiers were in harm. Those soldiers messaged other Ukrainian troops to say they were fine, and the Russian-backed soldiers used those communications to locate and attack Ukrainians in the field.

Conclusion

The roundtable participants raised three categories of challenges concerning spectrum vulnerabilities that are both broad and interrelated—they must be addressed together. First, there are not adequate systems and processes in place for stakeholders to detect and understand what spectrum vulnerabilities exist. This is largely due to a lack of data sharing among wireless system operators and with the government, but other factors, including insufficient data collection and analysis, research and testing, and government resources, contribute to this. Second, stakeholders are not seeking out the causes of vulnerabilities, nor trying to mitigate them, even when they can be detected. There was consensus that spectrum vulnerabilities persist in part because wireless system developers are not implementing security by design. This is caused by misaligned incentives and increasing complexity of systems. Third, stakeholders are hindered in their efforts to classify and prioritize resources to address vulnerabilities because they do not have enough insight into the scope and cause of vulnerabilities. However, the highest priority must be placed on those issues that could result in physical harm.

The roundtable participants provided good ideas on how to address some of the challenges identified. For example, to facilitate data sharing, there could be a data sharing clearinghouse, such as an ISAC. Additionally, the participants discussed opportunities to facilitate increased research and testing by academics. There was also insightful discussion about how system complexity can be used as a mechanism to mitigate vulnerabilities.

This roundtable discussion was only a starting point, however. More challenges were raised than solutions proposed. The participants agreed that further discussions must take place to assess challenges and develop more detailed solutions on how to address them. There was consensus that a conference or another roundtable that brings together experts in government, industry, and academia is an appropriate next step.

Participants

Kumar Balachandran, Principal Researcher, Ericsson Research
Stephen Berger, President, Owner, TEM Consulting
William Davenport, Chief of Staff and Senior Legal Advisor, Office of FCC Commissioner Geoffrey Starks
Scott Fox, Chairman, Chief Executive Officer, Global View Partners
Pierre de Vries, Spectrum Policy Initiative Co-director and Executive Fellow, Silicon Flatirons
Monisha Ghosh, Research Professor and Associate Member, The University of Chicago; Program Director, National Science Foundation
Dana Goward, President, Resilient Navigation & Timing Foundation
Keith Gremban, Director, Institute for Telecommunication Sciences, National Telecommunications and Information Administration
Joshua Guyan, Partner, Kelley Drye & Warren LLP
Rosemary Harold, Chief of the Enforcement Bureau at the Federal Communications Commission
Dale Hatfield, Spectrum Policy Initiative Co-director and Executive Fellow, Silicon Flatirons; Adjunct Professor, Technology, Cybersecurity and Policy Program, University of Colorado Boulder
John Hunter, Senior Director, Technology & Engineering Policy, T-Mobile USA, Inc.
Cynthia Irvine, Distinguished Professor of Computer Science, Naval Postgraduate School; Director, Center for Cybersecurity and Cyber Operations
Clete Johnson, Partner, Wilkinson Barker Knauer, LLP
Paul Kolodzy, Principal, Kolodzy Consulting
Sridhar Kowdley, Program Manager, Science and Technology, U.S. Department of Homeland Security
Marc Lichtman, Adjunct Assistant Professor, Department of Computer Science, University of Maryland; Research Engineer, Perspecta Labs
Dan Massey, Director, Professor, Interdisciplinary Telecom Program, University of Colorado Boulder
Melissa Midzor, NASCTN Program Manager, Communications Technology Laboratory (CTL), National Institute of Standards and Technology
Mark Norton, Senior Engineer, Office of CIO, U.S. Department of Defense
Christos Papadopoulos, Professor, Department of Computer Science, Colorado State University
Wayne Phoel, Director of Science & Technology, FinRegLab; Visiting Research Engineer, Institute for Systems Research, University of Maryland
Jeffrey Reed, Willis G. Worcester Professor of the Bradley Department of Electrical and Computer Engineering, Virginia Tech
Eleanor Saitta, Security, Privacy Architecture, and Strategy Consultant
Helen Tang, Portfolio Manager - Wireless Cyber Security, Defense Research and Development Canada (DRDC)
Bryan Tramont, Executive Fellow, Silicon Flatirons Center; Managing Partner, Wilkinson Barker Knauer, LLP
Chip Yorkgitis, Partner, Kelley Drye & Warren LLP